POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Řízení bezpečnosti podniku – teorie, přístupy a praxe

Diplomová práce

Enterprise safety management – Theory, Approaches and Practice

Master thesis

VEDOUCÍ PRÁCE

JUDr. Zdeněk KROPÁČ, Ph.D.

AUTOR PRÁCE

Bc. Jiří KOPRNICKÝ

PRAHA

2024

Čestné prohlášení

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

V Mníšku, dne

Bc. Jiří KOPRNICKÝ

Anotace

Tato diplomová práce se zabývá tématem řízení bezpečnosti podniku – teorií, přístupy a praxí v podnicích, a to konkrétně v oblasti bezpečnostního managementu. Práce zahrnuje obecnou teorii bezpečnostního managementu – oblasti bezpečnosti podniku, dále některé metody a techniky používané při řízení bezpečnosti podniku a pak definicemi různých přístupů (proaktivní, reaktivní, procesní, rizikové, systémové a další). Následující část práce se zabývá praxí, tedy využíváním jednotlivých principů v organizacích a také hodnotí to, jak zaměstnanci nahlíží na implementaci moderních bezpečnostních opatření a jaký je vztah mezi vzděláváním zaměstnanců a bezpečnostními riziky.

Klíčová slova

řízení bezpečnosti podniku, bezpečnostní management, proaktivní a reaktivní přístup, systémový přístup, rizikový přístup, procesní přístup

Annotation

This masters thesis is focused on enterprise safety management – theory, approaches, and practices within businesses, specifically in the field of security management. The work encompasses the general theory of security management – the area of enterprise safety, as well as various methods and techniques used in security management. It also defines different approaches (proactive, reactive, process-oriented, risk-based, and systemic). Second part of the thesis focuses on practical aspects, including the application of individual principles within organizations, and evaluates how employees perceive the implementation of modern security measures and the relationship between employee education and security risks.

Keywords

enterprise safety management, security management, proactive and reactive approach, systematic approach, risk approach, process – oriented approach

Obsah

Úvod

V dnešní době se bezpečnost stává stále důležitějším aspektem podnikání. Bez ohledu na velikost nebo obor podnikání, řízení bezpečnosti podniku hraje klíčovou roli v ochraně zaměstnanců, zákazníků a majetku podniku. Tato práce se zaměřuje na teorii, přístupy a praxi podnikového bezpečnostního managementu, konkrétně na řízení bezpečnosti podniku.

Cílem této práce je hlubší pochopení principů řízení bezpečnosti podniku, různých přístupů k jeho implementaci a jeho praktické aplikace v podnicích. Práce také zdůrazňuje význam efektivního využívání jednotlivých principů pro celkový výkon podniku.

Tato práce je omezena na studium bezpečnostního managementu v kontextu podnikání – řízení bezpečnosti podniku. I když se bezpečnost týká mnoha dalších oblastí, jako je veřejná bezpečnost a osobní bezpečnost, tyto oblasti nebudou do práce zahrnuty.

Práce je strukturována do několika kapitol, které pokrývají širokou škálu témat týkajících se řízení bezpečnosti podniku. Od teorie bezpečnostního managementu, až po praktické přístupy a aplikace v různých odvětvích. Každá kapitola poskytuje podrobný pohled na dané téma a společně tvoří komplexní přehled problematiky bezpečnostního managementu v podnicích.

Cíle práce

Cílem této diplomové práce je vytvořit komplexní příručku na téma „Řízení bezpečnosti podniku – teorie, přístupy a praxe“. Tato příručka bude sloužit jako ucelený průvodce pro hodnocení stávajících bezpečnostních strategií a návrh nových strategií na základě tohoto hodnocení. Příručka bude obsahovat teoretické koncepty, současné přístupy a praktické aplikace v oblasti řízení bezpečnosti podniku, s důrazem na bezpečnostní management.

V rámci práce budou také ověřovány dvě hypotézy:

Hypotéza č. 1: „Implementace nových bezpečnostních přístupů založených na nejnovějších trendech a inovacích v oblasti bezpečnosti podniku povede ke snížení počtu bezpečnostních událostí v organizaci.“

Hypotéza č. 2 „Efektivita stávajících bezpečnostních přístupů v organizaci je přímo úměrná s úrovní vědomí a školení zaměstnanců v oblasti bezpečnosti.“

Metodologie

Tato diplomová práce je strukturována do dvou hlavních částí, které na sebe logicky navazují, a to teoretické a praktické části.

Teoretická část je založena na definici problému, stanovení cílů práce a formulaci hypotéz, které budou ověřeny v průběhu práce. V této části si představíme jednotlivé oblasti bezpečnosti podniku, metody využívané managementem v oblasti řízení bezpečnosti podniku a samozřejmě jednotlivé přístupy.

Praktická část práce analyzuje četnost využití jednotlivých přístupů v organizacích v České republice získané na základě odpovědí získaných z dotazníku odpovědných osob z jednotlivých organizací. V další části se autor zaměří na zodpovězení výše vyřčených hypotéz a na základě analýzy zhodnotí, zda je lze potvrdit, či vyvrátit.

1 Teorie bezpečnostního managementu

První kapitola této práce, nazvaná Teorie bezpečnostního managementu, se bude zabývat především definováním, co vlastně řízení bezpečnosti podniku je. K tomu je tedy potřeba nejprve definovat obecný pojem bezpečnostní management, jehož součástí, specifickým aspektem, je řízení bezpečnosti podniku.

V další části této kapitoly se zaměříme na exkurz do historie, konkrétně na historický vývoj bezpečnostního managementu a plynule přejdeme do současnosti.

Obrázek 1. Znázornění součásti bezpečnostního managementu Zdroj: autor

1.1 Definice a význam bezpečnostního managementu

Definice bezpečnostního managementu se liší v závislosti na zdroji a kontextu. Jedna z definic uvádí, že „*Bezpečnostní management je obor znalostí k působení manažerů za účelem dosahování optimální bezpečnosti organizace“*[1]. Encyklopedie BOZP definuje bezpečnostní management jako efektivní, samo regulující se systém, zajišťující integrované řízení bezpečnosti v podniku, který realizuje vedení podniku na základě stanovených cílů.[2]

Vzhledem k tomu, že řízení bezpečnosti podniku úzce souvisí i s bezpečností a ochranou při práci (BOZP), lze použít i definici podle inženýra Neugebauera a to, že „S*oučasné pojetí BOZP usiluje o omezení všech negativních aspektů*

[1] KOVAŘÍKOVÁ, M. 2015. Prevence ozbrojených útoků na školách jako součást didaktiky mimořádných situací. Lifelong Learning – celoživotní vzdělávání, roč. 5, č. 3, s. 95-112. ISSN 1804-526X. DOI: http://dx.doi.org/10.11118/lifele2015050395

[2] Přispěvatelé Encyklopedie BOZP, *Bezpečnostní management* [online], , c2019, Datum poslední revize 11. 06. 2019, 08:50 UTC, [citováno 23. 10. 2023] <https://ebozp.vubp.cz/wiki/index.php?title=Bezpe%C4%8Dnostn%C3%AD_management&oldid=23175>

souvisejících s prací, včetně stresu, šikany, obtěžování, nerovného zacházení na pracovišti atd. (tzv. ochrana práce)“[3].

Dále lze, podle zahraničních zdrojů, chápat bezpečnostní management jako systém řízení bezpečnosti, a tento systém je definován organizačními procesy, které zajišťují efektivní rozhodování založené na riziku souvisejícím s každodenním podnikáním[4].

V neposlední řadě můžeme použít i definici pro informační bezpečnost, což je komplex opatření, který zahrnuje proces navrhování, schvalování a implementaci softwarových, hardwarových, technických, personálních ochranných opatření spojených s minimalizací možných ztrát, vzniklých v důsledku poškození, zničení nebo zneužití informačních systémů[5].

Z výše uvedených definic lze shrnout, že řízení bezpečnosti podniku je komplexní systém řízení, který se zaměřuje na zajištění bezpečnosti v organizaci. Je to tedy souhrn aktivit a opatření, které slouží k ochraně osob, majetku a životního prostředí před riziky a hrozbami. Cílem tohoto řízení je minimalizovat pravděpodobnost vzniku nežádoucích událostí a jejich dopad na fungování podniku.

1.2 Historie a vývoj bezpečnostního managementu

Tato část se zabývá historií a vývojem bezpečnosti a ochrany zdraví při práci (BOZP) od starověku až po současnost. V této kapitole je stručný popis toho, jak se v různých dobách a kulturách uplatňovaly zásady ochrany života a zdraví při práci, a jak se postupně rozvíjelo zákonodárství a instituce, které měly zajistit lepší pracovní podmínky, sociální zabezpečení a ochranu práv zaměstnanců. V druhé části, která je zaměřena na současný stav bezpečnosti podniku jsou zmíněny aktuální trendy v této oblasti.

---

[3] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[4] 10 THINGS YOU SHOULD KNOW ABOUT SAFETY MANAGEMENT SYSTEMS (SMS). Online. In: The International Civil Aviation Organization. Dostupné z: https://www4.icao.int/demo/SMI/10_things.pdf. [cit. 2024-03-10].

[5] WIKIPEDIE, Přispěvatelé. Informační bezpečnost. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: https://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_bezpe%C4%8Dnost. [cit. 2024-03-10].

1.2.1 Historie bezpečnostního managementu

Ve starověkých civilizacích, jako byly Mezopotámie, Egypt nebo Řím, existovaly určité zásady ochrany života a zdraví při práci, dalo by se říct řízení rizik (nikoli řízení podniku), které byly zakotveny v zákonech, náboženských textech nebo stavebních předpisech. Například Chamurappiho zákoník[6] stanovoval pokuty za zranění dělníků, Pátá kniha Mojžíšova nařizovala zábradlí na střechách, egyptští stavitelé pyramid zajišťovali stravu a zdravotní péči pro dělníky, římští gladiátoři měli nárok na lékařskou pomoc a penzi[7].

Ve středověku a raném novověku se začaly objevovat první zákony a předpisy týkající se hornictví, požární ochrany, nebo cechovní organizace. Například hornický zákon[8] z roku 1500 stanovoval pravidla pro větrání, osvětlení, zabezpečení a zdravotní péči v dolech, požární řád[9] z roku 1571 nařizoval používání ohnivzdorných materiálů a hasicích přístrojů, cechy zajišťovaly sociální zabezpečení a ochranu práv svých členů.

V průběhu průmyslové revoluce a moderní doby se rozvíjelo zákonodárství a instituce, které měly zajistit lepší pracovní podmínky, sociální zabezpečení a ochranu práv zaměstnanců. Příkladem mohou být zákony[10] o pracovní době z roku 1848 a 1919, které omezovaly délku pracovní doby. Zákony o úrazovém a nemocenském pojištění z roku 1884 a 1889 zaváděly povinné pojištění pro zaměstnance, zákazy práce dětí a žen z roku 1878 a 1919 chránily zranitelné skupiny, živnostenský řád z roku 1859 upravoval podmínky pro výkon živností. Všeobecná deklarace lidských práv z roku 1948 proklamovala právo na práci a zákon o bezpečnosti práce z roku 1978 stanovil povinnosti zaměstnavatelů a zaměstnanců v oblasti BOZP. Orgány, které měly dohlížet nad dodržováním

[6] VALA, Jiří. 100 let BOZP 1918 - 2018. 1. vyd. Výzkumný ústav bezpečnosti práce, 2018. 31s.

[7] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[8] Tamtéž

[9] Tamtéž

[10] Tamtéž

těchto předpisů byly živnostenská a tovární inspekce, psychotechnický ústav, výzkumný ústav bezpečnosti práce nebo závodní výbory a komise[11].

1.2.2 Současnost bezpečnostního managementu

Současný vývoj v oblasti řízení bezpečnosti podniku se vyznačuje dynamickým posunem od reaktivního přístupu k proaktivnímu a preventivnímu. Zvyšuje se důraz na komplexní systémy managementu BOZP[12], které integrují různé aspekty bezpečnosti a ochrany. Mezi klíčové trendy se dá zařadit implementace moderních standardů a systémů bezpečnosti, jako je ISO 45 001, který vystřídal stávající standard OHSAS 18 001 a dále zvyšující zájem o integrované systémy managementu, kterými jsou např. ISO 9001 a ISO 14001. Ty propojují dnešní BOZP s kvalitou, ochranou životního prostředí a dalšími oblastmi managementu[13].

Dalším velkým posunem v této oblasti je v dnešní době využívání moderních technologií[14], především pak těch chytrých jako je IoT, nebo-li internet věcí, který se využívá pro monitoring a prevenci rizik. Na základě toho se pak využívá prediktivní analýza dat k identifikaci potenciálních rizik a předcházení incidentům. Díky IoT roste implementace automatizace v oblasti BOZP pomocí automatizovaných auditů a robotických asistenčních systémů.

Kromě používání moderních technologií nelze opomenout i lidský faktor, který stále vykonává většinu práce v podniku a je jeho nezbytnou součástí. V současnosti se zvyšuje důraz na psychologii bezpečnosti a vnímání rizik ze strany zaměstnanců, tedy, aby se sami zaměstnanci aktivně podíleli na bezpečném prostředí a aby byli sami zodpovědní za toto prostředí. Podniky se

[11] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[12] VALA, Jiří. Systémové řízení bezpečnosti a ochrany zdraví v organizacích. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-109-5.

[13] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[14] DVOŘÁKOVÁ, Zuzana; IĽKO, Michael Dezider. Nové technologie v BOZP. Časopis výzkumu a aplikací v profesionální bezpečnosti [online]. 2019, roč. 12, speciální č. Nové trendy v BOZP 2019. Dostupný z: https://www.bozpinfo.cz/josra/nove-technologie-v-bozp. ISSN 1803-3687.

také snaží rozvíjet programy pro zvyšování povědomí o BOZP a motivovat k bezpečnému chování svých zaměstnanců[15].

Jako poslední, co je důležité zmínit jsou normativní a legislativní požadavky[16], které se v čase vyvíjejí, mění a upravují. Stále je zde kladen důraz na bezpečnost lidského faktoru v oblasti BOZP, objevují se ovšem také další důležité oblasti, které je třeba chránit. Podle výše uvedeného, roste využívání moderních technologií a s tím tedy význam kybernetické bezpečnosti a ochrany dat v kontextu řízení bezpečnosti podniku.

2 Oblasti řízení bezpečnosti podniku

Jak bylo zmíněno, řízení bezpečnosti podniku je komplexní činnost, která se věnuje ochraně organizace před různými druhy rizik v rozličných oblastech. Těmito oblastmi jsou fyzická bezpečnost, kybernetická bezpečnost, personální bezpečnost, ekonomická bezpečnost, požární ochrana, enviromentální bezpečnost, ochrana informací a ochrana zdraví při práci. V následujících kapitolách budou stručně shrnuty jednotlivé oblasti.

2.1 Fyzická bezpečnost

Fyzická bezpečnost[17] představuje souhrn technických a organizačních opatření zaměřených na ochranu fyzických aktiv podniku, jako jsou budovy, zařízení, materiály a produkty, před neoprávněným přístupem, poškozením, krádeží nebo zničením. Tímto způsobem zajišťuje fyzická bezpečnost kontinuitu provozu, ochranu majetku a minimalizaci rizik finančních ztrát, poškození reputace a narušení chodu podniku.

[15] Přispěvatelé Encyklopedie BOZP, Psychická bezpečnost práce [online], , c2021, Datum poslední revize 5. 03. 2021, 08:28 UTC, [citováno 4. 03. 2024] <https://ebozp.vubp.cz/wiki/index.php?title=Psychick%C3%A1_bezpe%C4%8Dnost_pr%C3%A1ce&oldid=23933>

[16] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-4.

[17] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

Do systému fyzické bezpečnosti patří:

- Technická ochrana
- Fyzická ochrana
- Režimová opatření

2.1.1 Technická ochrana

Technická ochrana představuje souhrn technických prostředků a systémů[18], které slouží k zajištění fyzické bezpečnosti podniku. Jedná se o komplexní oblast, která zahrnuje širokou škálu technologií a zařízení.

Technická bezpečnost se nejčastěji dělí na:

- Mechanické zábranné systémy
- Elektronické zabezpečovací systémy

Ad. Mechanické zábranné systémy

Mechanické zábranné systémy[19] (MZS) jsou prostředky, které mají za cíl zabránit nebo ztížit vniknutí neoprávněných osob do chráněného objektu nebo prostoru. MZS tedy tvoří fyzickou bariéru, která chrání majetek, techniku, informace a osoby před krádeží, zničením, sabotáží nebo útokem.

Obecné rozdělení MZS je následující:

- Plášťová ochrana – zabraňuje jakémukoliv narušení standardních i nestandardních vstupních jednotek do objektu. Jedná se o zabezpečení vstupu do všech stavebních otvorů v objektu, jako jsou dveře, okna, balkóny, sklepní okna, vikýře apd.;
- Obvodová ochrana – jedná se o prostředky zajišťující bezpečnost na vyhrazeném území a prostor kolem chráněného objektu;

[18] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-808-7500-576.

[19] IVANKA, Ján. Mechanické zábranné systémy. Online. Druhé. Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-427-9. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/18575/Mechanicke_zabranne_systemy-obsah.pdf?sequence=2. [cit. 2024-02-03].

- Předmětová ochrana – zabezpečuje prostory či úschovná místa, kde jsou uloženy peníze, cennosti apod., před zcizením nebo neoprávněnou manipulací;
- Individuální ochrana – přenosné i nepřenosné technické prostředky zmíněné v předchozích bodech;
- Speciální ochrana – chemická ochrana předmětů, cenin apod. Patří sem také ochrana, která je označena jako „ostatní“, do které řadíme plomby, pečetě, hologramy apod.

Ad. Elektronické zabezpečovací systémy[20]

Od roku 2009 se označují jako Poplachové zabezpečovací a tísňové systémy (PZTS), dříve byly označeny jako Elektronické zabezpečovací systémy (EZS). Jak již název vypovídá, jedná se o zabezpečovací systém, který, oproti MZS, aktivně chrání objekt a v případě narušení spustí alarm. Tento systém se skládá z několika prvků[21] a to:

- Ústředna – je základ celého PZTS, je v ní uložena veškerá konfigurace, do ústředny jsou zapojeny ostatní komponenty;
- Ovládací zařízení – jedná se o klávesnici, která ovládá celý systém, mimo to existují i alternativy, jako klíčenky či přístupové terminály;
- Záložní zdroj – myslí se tím akumulátorová baterie obvykle na 12 V, která v případě výpadku poskytuje energii do systému, jak ústředny, tak do periferií;
- Periferie – periferií se rozumí různé přídavné moduly, čidla a systémová příslušenství, která se připojují do ústředny. Mezi nejpoužívanější periferie patří PIR čidla, elektromagnetické kontakty, GSM komunikátory, sirény a další.

[20] HARTL, Jan. Poplachové zabezpečovací a tísňové systémy. Online. Česká zemědělská univerzita v Praze - Technická fakulta. ISBN 978-80-213-2962-1. Dostupné z: https://katedry.czu.cz/storage/258/7579_Poplachove-zabezpecovaci-a-tisnove-systemy.pdf. [cit. 2024-02-03].

[21] AITOM. Elektronické zabezpečovací systémy. Online. Dodáváme zabezpečovací systémy!. Dostupné z: https://www.elkov.cz/sluzby-poradenstvi-a-navrhy-elektronicke-zabezpecovaci-systemy-ezs/. [cit. 2024-03-10].

2.1.2 Fyzická ochrana

Fyzická ochrana[22] představuje souhrn technických a organizačních opatření zaměřených na ochranu fyzických aktiv podniku, jako jsou budovy, zařízení, materiály a produkty, před neoprávněným přístupem, poškozením, krádeží nebo zničením.

Tímto způsobem zajišťuje fyzická ochrana kontinuitu provozu, ochranu majetku a minimalizaci rizik finančních ztrát, poškození reputace a narušení chodu podniku. Většinou je doplněna o technickou ochranu viz předchozí odstavec.

Z výše uvedeného vyplývá, že se tedy jedná o ochranu spočívající v přímém pozorování objektu, který je chráněn, prostřednictvím fyzických osob, například pracovníky ostrahy, policií, nebo bezpečnostní agenturou.

2.1.3 Režimová opatření

Režimová opatření[23] jsou nezbytnou součástí fyzické bezpečnosti podniků, která zahrnuje ochranu majetku, osob a informací před neoprávněným přístupem, zneužitím, poškozením nebo ztrátou. Tato opatření stanovují, kdo, kdy, kde a jak může vstupovat do podniku, používat jeho zařízení a zdroje, manipulovat s citlivými daty a materiály, komunikovat s ostatními subjekty nebo reagovat na mimořádné situace. Režimová opatření by měla být v souladu s platnými právními normami, etickými principy a směrnicemi daného podniku.

Režimová opatření jsou realizována prostřednictvím různých nástrojů a metod. Mezi tyto nástroje a metody může být používání docházkových systémů a vstup pomocí identifikačních karet. Dále to mohou být biometrické systémy a zámky, používání alarmů, kamer, detektorů v podniku. Dalším nástrojem může být pravidelné školení zaměstnanců v oblasti bezpečnosti. V neposlední řadě je také vhodné zapisovat kontroly, školení a další věci do protokolů, což je dalším opatřením. [24]

---

[22] UHLÁŘ, Jan. *Technická ochrana objektů II. Díl: Elektrické zabezpečovací systémy II*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 9788072513130.

[23] Tamtéž

[24] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

2.2 Kybernetická bezpečnost

Kybernetická bezpečnost[25] je jednou z největších výzev moderního světa, která ovlivňuje nejen jednotlivce, ale i podniky a organizace. V kontextu řízení bezpečnosti podniku je kybernetická bezpečnost schopnost chránit informační systémy podniku, jeho interní sítě a data před neoprávněným přístupem, jejich zneužitím nebo zničením. Kybernetická bezpečnost je nezbytná pro zachování důvěry, integrity a konkurenceschopnosti podniku v digitálním prostředí.

Podniky se setkávají s různými typy kybernetických hrozeb[26], které se neustále vyvíjejí a zvyšují svou složitost a sofistikovanost. Mezi nejčastější kybernetické hrozby patří malware, phishing, hacking a sociální inženýrství. Tyto hrozby se snaží infikovat, poškodit, ovládnout nebo ukrást citlivá data z informačních systémů podniků nebo interních sítí. Kybernetické útoky mohou mít vážné dopady na podnik. Může to být například ztráta důvěrných informací a dat, finanční ztráty, poškození reputace nebo porušení legislativních a regulačních požadavků.

Pokud je kybernetická bezpečnost efektivní[27], lze dostatečně zajistit, aby byly informace a data dostupné pouze pro důvěryhodné a oprávněné uživatele a zároveň chráněné před neoprávněnými útočníky. Efektivní kybernetická bezpečnost také snižuje riziko a závažnost kybernetických útoků, zvyšuje schopnost detekovat, reagovat a obnovit se z nich a snižuje náklady na prevenci, ochranu a nápravu. Dobře nastavená kybernetická bezpečnost také udržuje dobrou reputaci podniku, dodržuje legislativní a regulační požadavky a zvyšuje konkurenceschopnost podniku.

Takto efektivně nastavená kybernetická bezpečnost není jednorázovým projektem, ale kontinuálním procesem, který vyžaduje strategické plánování, implementaci, monitorování a zlepšování. Mezi klíčové aspekty takové bezpečnosti patří proaktivní přístup a neustálé sledování hrozeb, spolupráce

[25] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. Online. 1. CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf. [cit. 2024-02-03].

[26] Tamtéž

[27] Tamtéž

vedení a IT oddělení, zapojení všech zaměstnanců a zvyšování jejich povědomí o nových hrozbách pomocí různých školení[28].

Kybernetická bezpečnost je důležitá pro prosperitu podniku v dnešním světě. Podniky by měly investovat do efektivní kybernetické ochrany, aby chránily své informační systémy, sítě a data před kybernetickými hrozbami a využily plný potenciál digitálních technologií. Efektivní kybernetická bezpečnost je nejen nutností, ale i výhodou pro podniky, které chtějí být důvěryhodné, integrované a konkurenceschopné.

2.3 Ekonomická bezpečnost

Ekonomická bezpečnost[29] je stav, kdy je subjekt ekonomické reality schopen uspokojovat své základní potřeby a cíle v současnosti i v budoucnosti, aniž by byl vystaven rizikům a ohrožením, které by mohly výrazně snížit jeho výkonnost, stabilitu nebo rozvoj. Ekonomická bezpečnost je tedy spojena s ochranou a rozvojem ekonomických zdrojů, hodnot a zájmů subjektu.

V kontextu řízení bezpečnosti podniku je ekonomická bezpečnost jedním z klíčových aspektů, které je třeba zohlednit při plánování, provádění a hodnocení bezpečnostních opatření a aktivit. Podnik musí být schopen zajistit svou ekonomickou nezávislost, stabilitu a konkurenceschopnost na trhu, a zároveň minimalizovat dopady potenciálních hrozeb a rizik, které by mohly ohrozit jeho hospodářskou sílu, kvalitu života a rozvojové možnosti.

Ekonomická bezpečnost podniku je ovlivněna mnoha faktory[30], které lze rozdělit na vnější a vnitřní. Mezi vnější faktory patří politické, ekonomické a sociální prostředí, ve kterém podnik působí, a jeho vztahy s ostatními subjekty na domácím i mezinárodním trhu. Mezi vnitřní faktory patří organizační, právní, finanční, technologické a lidské zdroje, kterými podnik disponuje a využívá pro své činnosti. Tyto faktory je třeba průběžně monitorovat, analyzovat a hodnotit, aby

[28] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. Online. 1. CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf. [cit. 2024-02-03].

[29] ŠTĚPÁNOVÁ, Martina. Ekonomická bezpečnost vybraného podniku. Vedoucí Hoke, Eva. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení, 2018. Dostupné také z: http://hdl.handle.net/10563/43062.

[30] Tamtéž

bylo možné identifikovat a eliminovat slabá místa, zlepšovat silné stránky a reagovat na změny a výzvy[31].

Pro kvantifikaci a hodnocení ekonomické bezpečnosti podniku existují různé nástroje a ukazatele. Například podle studie z Charkovské univerzity civilního inženýrství a architektury z roku 2021 lze použít následující ukazatele[32]:

- Integrovaný index úrovně ekonomické bezpečnosti podniku – tento index je syntetická hodnota, která je vytvořena na základě systému indexů rysů (finanční, tržní, intelektuální a personální, technologická, informační, politický a právní). Index je v rozmezí od 0 do 1, kde vyšší hodnota znamená vyšší úroveň ekonomické bezpečnosti.
- Integrovaný index adaptability úrovně ekonomické bezpečnosti podniku – tento index je také syntetická hodnota, která je vytvořena na základě systému indexů rysů (rychlosti, obratnosti, pružnosti). Index je také v rozmezí od 0 do 1, kde vyšší hodnota znamená vyšší úroveň adaptability ekonomické bezpečnosti.
- Matice „ekonomická bezpečnost/adaptabilita“ – tato matice je nástroj pro klasifikaci stavu ekonomické bezpečnosti podniku podle dvou kritérií: úrovně ekonomické bezpečnosti a adaptability systému ekonomické bezpečnosti. Matice je rozdělena na 16 kvadrantů, které odpovídají různým kombinacím hodnot integrovaných indexů.

Tyto ukazatele umožňují porovnávat ekonomickou bezpečnost podniku s jinými podniky a zároveň identifikovat silné a slabé stránky, příležitosti a hrozby, které ovlivňují jeho ekonomickou situaci[33].

[31] KUDLOVÁ, Dagmar. Prostředí v managementu. Online, Učební materiál. Informační systém Masarykovy univerzity: Masarykova univerzita, 2005. Dostupné z: https://is.muni.cz/el/1451/jaro2005/t192/um/Prostredi_managementu.pdf. [cit. 2024-02-03].

[32] SHUMILO, Olha; BABENKO, Vitalina; LIUBOKHYNETS, Larysa; VOLOVELSKA, Iryna a AREFIEVA, Olena. Method of Enterprise Economic Security Evaluation. Online. Studies of Applied Economics. 2021, roč. 39, č. 7. ISSN 1697-5731. Dostupné z: https://doi.org/10.25115/eea.v39i7.4998. [cit. 2024-02-19].

[33] DAŇOVÁ, Monika a Jaroslav GONOS. VYBRANÉ ASPEKTY KVANTIFIKÁCIE EKONOMICKEJ BEZPEČNOSTI [online]. Prešovská univerzita v Prešově: Prešovská univerzita v Prešově, 2016 [cit. 2024-02-03]. ISBN 978-80-555-1619-6. Dostupné z: https://www.pulib.sk/web/pdf/web/viewer.html?file=/web/kniznica/elpub/dokument/Kotulic25/subor/9788055516196.pdf

Z výše uvedených informací vyplývá, že je ekonomická bezpečnost jedním z důležitých aspektů řízení bezpečnosti podniku, který vyžaduje komplexní a systematický přístup, založený na znalosti a porozumění faktorů, které ho ovlivňují, a na schopnosti předvídat a řešit problémy, které by podnik mohly ohrozit. Je také jednou z podmínek pro dosahování dalších cílů a hodnot podniku, jako je spokojenost zákazníků, kvalita produktů a služeb, sociální odpovědnost, environmentální ochrana a další.

2.4 Personální bezpečnost

Na úvod je nutné podotknout, že i když se jedná o personální bezpečnost, nejedná se o bezpečnost vtahující se k ochraně a zdraví zaměstnanců před riziky, ale na ochranu podniku před svými zaměstnanci ve smyslu ztráty citlivých informací, know-how nebo sabotáží.

Zaměstnanci, kteří nemají stejné cíle jako organizace, jsou vždy potenciálním rizikem, jehož dopad je těžko předvídatelný. Nově přijatí zaměstnanci jsou v naprosté většině případů podrobeni důkladnému prověřování, zda neohrožují bezpečnost organizace.

Mezi běžné metody[34] patří reference z minulých zaměstnání, psychologické testy, testy dovedností nebo kontrola trestního rejstříku. V rámci organizace existuje mnoho zranitelných bodů, které mohou noví zaměstnanci využít ve svůj prospěch nebo prospěch jiných. Organizace má zájem pečlivě vybírat zaměstnance, kteří budou zastávat určité pracovní pozice.

Organizace, jakožto celek, má uvnitř mnoho slabých míst, která mohou noví zaměstnanci zneužít ve svůj prospěch nebo prospěch jiných organizací[35]. Z tohoto důvodu by měla mít samotná organizace zájem pečlivě vybírat nové zaměstnance, kteří budou pracovat na určitých pracovních místech.

[34] BRABEC, František, Ivo LÁTAL, Rudolf MUSIL, Ivan PILNÝ, Miloš URBAN a Tomáš VEJLUPEK. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-864-4504-6.

[35] Tamtéž

Mezi nejčastější prohřešky zaměstnanců[36] patří malé majetkové krádeže. Například krádeže kancelářských potřeb, podvádění s palivem do firemních aut nebo vymýšlení fiktivních služebních cest. Horším druhem majetkové škody je krádež firemních aktiv nebo zásob ze skladů, které mohou firmu poškodit mnohem více než krádež kancelářských potřeb.

Jedním z takových příkladů, kdy krádež poškodila firmu, je požár firmy Severochema v Liberci z roku 2017, který zavinil zaměstnanec při stáčení chemikálií do barelu. Ty se následně vznítily a firmě vznikla škoda v řádech desítek milionů.[37] Dalším vážným prohřeškem je vedení nepravdivého účetnictví, kdy dochází k uvádění nesprávných čísel a padělání dokumentů.

Z výše uvedených informací vyplývá, že z hlediska personální bezpečnosti podniku je vhodné, aby byl každý uchazeč řádně prověřen ještě před pohovorem na dané místo. Poté je vhodné, aby pracovník personálního oddělení dobře zhodnotil, zda je uchazeč řádně seznámen se svými povinnostmi a právy v rámci výkonu budoucího povolání.

Samotné prověřování při přijímání nových pracovníků lze rozdělit na následující etapy:

- Před vznikem pracovního poměru

Do této etapy lze zařadit metodu pre-employment background screening[38], což je metoda, kterou se zkoumá profil uchazeče pouze z veřejně dostupných zdrojů ještě před tím, než je s ním uskutečněn pracovní pohovor. Mezi tyto zdroje může patřit například Facebook, LindedIn, osobní blog, web, případně různé veřejné rejstříky, jako je například insolvenční rejstřík.

[36] LÁTAL, Ivo. *Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací*. Praha: Prospektrum, 2001. ISBN 80-717-5091-3.

[37] IDNES. Za požár liberecké Severochemy obvinili dělníka, stáčel načerno chemikálii. MAFRA A. S. IDnes [online]. 2017 [cit. 2024-02-07]. Dostupné z: https://www.idnes.cz/liberec/zpravy/severochema-liberec-pozar-obvineni-policie-cr-hasici.A190321_202010_liberec-zpravy_rko

[38] Pre-employment background screening | Práce a mzda. Hlavní strana | Práce a mzda [online]. Copyright © 2023 Wolters [cit. 07.02.2024]. Dostupné z: https://www.praceamzda.cz/clanky/pre-employment-background-screening#footnote1

- Během pracovního pohovoru[39]

V této etapě se personalista zaměřuje na informace, z první etapy a po vyhodnocení si začne zvát potenciální zaměstnance na pohovor, kde si zjistí více o uchazeči. Ověří se především jeho identita a soulad informací obsažených v životopise se skutečností a jeho trestní minulost.

K ověření těchto informací se používá mnoho metod, mezi které patří například pohovory, dotazníky, testování uchazečů, zkoumání referencí, lékařské prohlídky.

Na základě těchto postupů se vybere jeden uchazeč, se kterým se podepíše pracovní smlouva, smluvní ujednání o právech a povinnostech zaměstnance během pracovního poměru a po skončení pracovního poměru a další potřebné dokumenty před nástupem na novou pozici.

- Po ukončení pracovního poměru[40]

V případě ukončení pracovního poměru mohou nastat jistá rizika, především v možném úniku citlivých dat a know-how, které dotyčný odcházející zaměstnanec nabyl v době působení ve firmě.

Je proto vhodné, jak již bylo uvedeno v předchozím bodě o podpisu smluvního ujednání, jak se chovat v případě ukončení pracovního poměru. Zde je nutné poučit odcházejícího zaměstnance, jak se chovat a co by neměl vyzradit. To je provedeno záznamem o poučení s podpisem zaměstnance.

2.5 Ochrana zdraví při práci

Dle názvu této podkapitoly je jasné, že se tato oblast bezpečnosti věnuje ochraně zdraví při práci a riziky s prací spojenými. V praxi se můžeme také setkat se zkratkou BOZP.

BOZP je multidisciplinární obor[41], jehož úkolem je vytvářet systémy norem, které ochraňují zaměstnance, nebo také žáky či studenty na odborných stážích

[39] KUČÁKOVÁ, Adriana. Systémová bezpečnost organizace. Bakalářská práce. Praha: Policejní akademie České Republiky v Praze, 2023.

[40] Tamtéž

[41] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

a dále i osoby, které pracují na živnostenský list, nebo zaměstnavatele, kteří jsou fyzickými osobami a sami také vykonávají práci (například praktický lékař, notář aj.), před negativními následky života v pracovním prostředí.

Současná koncepce[42] BOZP se snaží eliminovat všechny negativní faktory spojené s prací, včetně stresu, šikany, obtěžování, diskriminace na pracovišti atd. (tzv. ochrana práce). Nejde jen o normy pro ochranu proti vzniku pracovního úrazu, ale i proti poškození, která se neprojeví hned, ale mohou se objevit i po několika letech. Jako příklad lze uvést práci s počítačem, kdy se poškození zdraví může projevit až po mnoha letech (nemoc z povolání – „nemoci šlach, šlachových pochev, tíhových váčků nebo úponů svalů nebo kloubů končetin z dlouhého nadměrného jednostranného přetěžování“).

BOZP se neskládá jen ze dvou základních oblastí – bezpečnosti práce a ochrany zdraví při práci, ale i z mnoha dalších menších[43], ale nezbytných oblastí, které tvoří tzv. sociální ochranu:

- vztahy na pracovišti
- estetická úprava pracovišť
- vliv práce na soukromý život zaměstnanců
- zřízení, údržba a zlepšení zařízení pro zaměstnance

Vzhledem k tomu, že je BOZP multidisciplinárním oborem, je nutné si uvědomit, že se s ní pojí více oblastí, které musí řešit. Jako příklad lze zmínit ochranu při práci s vyhrazenými technickými zařízeními (VTZ), kterými jsou elektrická, plynová, tlaková a zdvihací VTZ. Každé, z těchto VTZ, má své vlastní předpisy a normy. Hlavním právním předpisem v této oblasti je zákon č. 250/2021 Sb., Zákon o bezpečnosti práce v souvislosti s provozem vyhrazených technických zařízení[44].

[42] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[43] Tamtéž

[44] Zákon č. 250/2021 Sb.

S tímto předpisem však v oblasti BOZP souvisí mnoho dalších, a to například:

- nařízení vlády 194/2022 o požadavcích na odbornou způsobilost k výkonu činnosti na elektrických zařízeních a na odbornou způsobilost v elektrotechnice[45]
- zákon 262/2006 Sb., Zákoník práce[46]
- zákon č. 309/2006 Sb., zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci[47]
- další zákony, nařízení a vyhlášky s touto oblastí spojené

Obecně lze tedy konstatovat, že oblast BOZP se zaměřuje na[48]:

- Ochranu zdraví zaměstnanců: tím, že předchází pracovním úrazům a nemocem z povolání.
- Ochranu zaměstnavatele: a to tím, že minimalizuje ekonomické dopady vyplývající ze snížení zdraví zaměstnanců, jako je snížení produktivity práce, náhrady mzdy v době nemoci, nebo snížení konkurenceschopnosti firmy.

2.6 Požární ochrana

Pojem požární ochrana lze definovat[49] jako soubor podmínek a opatření, které zajišťují ochranu osob a majetku před požáry a umožňují poskytování pomoci v případě živelních pohrom a jiných mimořádných událostech. Požární ochrana se zakládá na stanovení povinností a pravomocí různých subjektů, jako jsou ministerstva, správní úřady, právnické a fyzické osoby, orgány státní správy a samosprávy a jednotky požární ochrany, které spolupracují na prevenci, řešení a nápravě požárních situací.

Na základě výše uvedených informací a dle zákona č. 133/1985 Sb., o požární ochraně je zřejmé, že každý zaměstnavatel, tedy i firmy, musí zajistit určité podmínky požární ochrany (PO) na pracovišti, které jsou uvedeny ve

[45] Nařízení vlády č. 194/2022 Sb.
[46] Zákon č. 262/2006 Sb.
[47] Zákon č. 309/2006 Sb.
[48] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.
[49] Zákon č. 133/1985 Sb.

vyhlášce č. 246/2001 Sb., o požární prevenci. Tyto podmínky[50] se pak liší na základě toho, do jaké požární kategorie spadá daný podnik.

Dělení je následující[51]:

- bez zvýšeného požárního nebezpečí
- se zvýšeným požárním nebezpečím
- s vysokým požárním nebezpečím

Určit kategorii, do které spadá činnost, je velice důležité, neboť to ovlivňuje, jakého odborníka na PO si musí zaměstnavatel zajistit[52]. Podle toho se rozhodne, zda mu stačí mít mezi zaměstnanci preventistu PO, nebo zda potřebuje technika PO nebo odborně způsobilou osobu (OZO) v PO. Prvním krokem je tedy stanovit stupeň požárního nebezpečí a zařadit činnost do kategorie se zvýšeným nebo vysokým požárním nebezpečím. Pokud činnost nepředstavuje ani jeden z těchto stupňů, patří do kategorie bez zvýšeného požárního nebezpečí. To ale neznamená, že se nemusí provést zařazení do kategorie, protože jinak by se mohlo předpokládat, že činnost je v nejnižší kategorii a že stačí splnit jen úkoly pro ni. Zařazení do správné kategorie může udělat jen technik PO nebo OZO v PO, protože to vyžaduje nejen odborné znalosti z oblasti požární ochrany, ale také to stanovuje vyhláška o požární prevenci.

Požární ochrana se nejvíce prolíná s oblastí BOZP, a to především v otázkách VTZ, kdy je nutné dodržovat pravidelné kontroly a revize[53] z důvodu rizika vznícení zařízení při poruše, dále v otázkách evakuace, školení PO, požárním evakuačním plánu a další.

Shrneme-li výhody požární ochrany, můžeme vypsat následující benefity firmy v dobře zavedené požární ochraně:

- Ochrana životů a zdraví osob v podniku
- Minimalizace materiálních škod a přímých finančních ztrát podniku

[50] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.
[51] Tamtéž
[52] Tamtéž
[53] Nařízení vlády č. 190/2022 Sb.

- Umožnění plynulého pokračování v provozu
- Dodržování legislativních a regulačních požadavků

2.7 Enviromentální bezpečnost

Enviromentální bezpečnost podniku[54] je schopnost podniku chránit životní prostředí před negativními dopady své hospodářské činnosti. To zahrnuje dodržování norem a požadavků vztahujících se k životnímu prostředí, snižování spotřeby přírodních zdrojů a emisí škodlivých látek, rozvoj environmentálních inovací a zelené výroby, zavádění systémů environmentálního managementu a auditu, plánování a monitorování environmentálních aspektů podnikání.

Enviromentální bezpečnost je, stejně jako PO, úzce spojena s BOZP a vzájemně se ovlivňují. Jako příklad[55] lze uvést použité osobní ochranné pomůcky, léky po expiraci nebo použité chemické prostředky po úklidu. V těchto případech s tímto odpadem musí firma naložit tak, aby to bylo bezpečné a neohrozila životní prostředí v okolí viz první odstavec. Proto je součástí enviromentální bezpečnosti i odpadové hospodářství, které by tyto problémy mělo řešit.

V případě, že by nebyla firma dostatečně zabezpečená v enviromentální oblasti a nedodržovala legislativní předpisy, by se tedy mohlo stát, že pokud dojde k nějakému narušení životního prostředí, může být postihnuta jak finančními sankcemi, tak v tom nejhorším případě uzavřením provozu[56]. Z toho plyne i ztráta zisku, který firma mohla mít, pokud by vše dodržovala.

Jako jeden z příkladů z poslední doby[57] lze uvést pokutu 1 000 000 Kč, kterou dostal podnik Maso Brejcha s.r.o. od České inspekce životního prostředí. *„Podnik*

[54] ABANINA, E N, Yu S SERGEENKO, O V DEVYATOV, O YU GANYUKHINA a Yu M NIKITENKO. The Structure of Training Program and Advanced Training of Enterprise Managers in Order to Ensure Environmental Safety. IOP Conference Series: Materials Science and Engineering [online]. 2019, 2019-09-01, 582(1) [cit. 2024-02-07]. ISSN 1757-8981. Dostupné z: doi:10.1088/1757-899X/582/1/012032

[55] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[56] Zákon č. 17/1992 Sb.

[57] Inspektoři Čižp uložili masokombinátu pokutu přes milion korun za spáchání několika správních deliktů.” Čižp, online, https://www.cizp.cz/aktuality/inspektori-cizp-ulozili-masokombinatu-pokutu-pres-milion-korun-za-spachani-nekolika.

nakládal s povrchovými vodami v rozporu s povolením, vypouštěl odpadní vody do vod podzemních bez povolení, odebíral povrchové vody bez povolení. Neohlásil také neprodleně havárii znečištění povrchových vod levostranného přítoku Ceciny a následně též povrchových vod ve vodním toku Cecina, kterou způsobil vypouštěním odpadních vod z ČOV".

2.8 Ochrana informací

Poslední oblast, kterou je nutné zmínit je oblast ochrany informací – informační bezpečnost podniku[58]. V této éře rostoucích digitálních technologií a jejich stále větší složitosti je řízení informační bezpečnosti pro organizaci kritickým a náročným úkolem. Naštěstí existují řešení a normy, které poskytují strukturovaný, nákladově efektivní a systematický způsob, jak zavádět, provozovat, monitorovat, přezkoumávat, udržovat a zlepšovat informační bezpečnost prostřednictvím zavedení systému řízení informační bezpečnosti (ISMS). Takovým řešením je norma ISO 27001.

Informační bezpečnost[59] je pro každou organizaci v současnosti nezbytná. ISMS je množina pravidel a opatření, která zajistí, že informace budou správné a úplné (princip integrity), dostupné pro ty, kdo je opravdu potřebují (princip dostupnosti) a chráněné před neoprávněným přístupem (princip důvěrnosti). ISMS je účinný dokumentovaný systém pro řízení a správu informačních aktiv, který má za cíl zabránit jejich možné ztrátě nebo poškození tím, že definuje aktiva, která je třeba ochránit, vybírá a řídí potenciální rizika informační bezpečnosti, implementuje opatření s požadovanou úrovní záruk a provádí jejich kontrolu. ISMS může být aplikován na organizační jednotku firmy, informační systém nebo jeho část, nebo může pokrývat celou organizaci. ISMS je systém, který nejen zabezpečuje informace organizace proti ztrátě nebo zneužití, ale také chrání členy vedení a zaměstnance před neúmyslnými porušeními zákonů ČR.

Ochrana informací a její řízení jsou stále v centru zájmu všech manažerů, kteří se v rámci své práce setkávají s daty, zpracovanými pomocí informačních

[58] TA-SEEN, Junaid. ISO 27001: Information Security Management Systems. Online. In: . Dostupné z: https://doi.org/10.13140/RG.2.2.36267.52005. [cit. 2024-02-11].

[59] NOVÁK, Luděk a POŽÁR, Josef. Systém řízení informační bezpečnosti. Online. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf. [cit. 2024-02-11].

a komunikačních technologií. Informační bezpečnost je spojená s rozloženou (individuální) zodpovědností a je velmi důležitá pro zajištění činností jakékoli organizace. Největším ohrožením pro ochranu informací[60] je člověk, který způsobí většinu bezpečnostních incidentů. Každý si musí uvědomit, že se nedá bezpečnost informací zajistit stoprocentně, ale mělo by se udělat vše pro to, aby se bezpečnost zajistila na přijatelné úrovni za ekonomicky oprávněné náklady. A právě zde hraje klíčovou roli řízení rizik, které je nezbytným základem každého ISMS.

3 Standardy a regulace v oblasti řízení bezpečnosti podniku

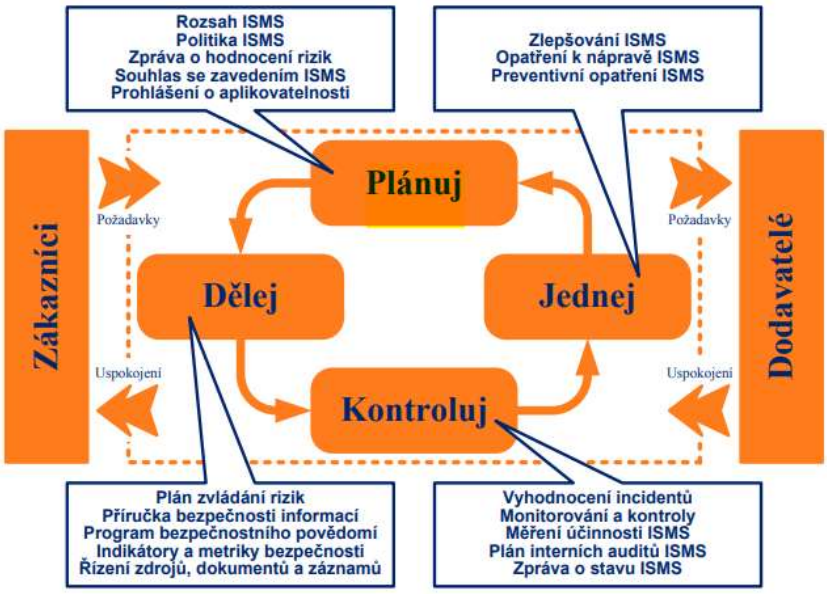
V předchozí kapitole byly v jednotlivých oblastech bezpečnosti podniku zmíněny některé standardy a právní normy. Tato kapitola má za cíl si tyto standardy a právní regulaci stručně popsat.

3.1 Mezinárodní standardy

V této kapitole si popíšeme jednotlivé standardy, které mají nějaký vztah k řízení bezpečnosti podniku. Mezi tyto standardy patří ISO 45001, ISO 27001, ISO 9001, ISO 14001 a ISO 31000. Vzhledem k tomu, že v následujících podkapitolách si o každém z těchto standardů napíšeme konkrétní body, o čem jsou, je vhodné zmínit, jaké mají společné znaky. Jedná se především o přístup, který mají všechny standardy společný. Tímto přístupem je tzv. *Systémový přístup*, který je popsán v kapitole 5.3.

Další společnou vlastností všech standardů je tzv. cyklus PDCA (Plan – Do-Check – Act) a je základem všech systémů managementu dle ISO norem[61].

[60] NOVÁK, Luděk a POŽÁR, Josef. Systém řízení informační bezpečnosti. Online. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf. [cit. 2024-02-11].
[61] Tamtéž



Obrázek 2. PDCA Model pro řízení bezpečnosti informací

Jednotlivé kroky PDCA jsou:

- Plánování – Stanovení cílů a definování kroků k jejich dosažení.
- Dělej – Implementace naplánovaných aktivit
- Kontroluj – Monitorování a měření výkonnosti systému
- Jednej – Analýza výsledků a implementace nápravných a preventivních opatření

Posledním společným bodem je dokumentace, ve které jsou evidovány veškeré změny související se zaváděním standardu.

3.1.1 ISO 45001 Systém managementu bezpečnosti a ochrany zdraví při práci

Mezinárodní norma ISO 45001:2018 stanovuje požadavky na systém řízení bezpečnosti a ochrany zdraví při práci (BOZP). Norma poskytuje rámec pro organizace, jak řídit rizika a zlepšovat výkon BOZP. Norma obsahuje kritéria pro politiku BOZP, cíle, plánování, provádění, provoz, auditování a přezkum[62].

[62] CONSTANTINE, Alister. ISO 45001:2018 OCCUPATIONAL HEALTH & SAFETY IMPLEMENTATION GUIDE [online]. In: . 1. NQA, 2018, s. 35 [cit. 2024-02-11]. Dostupné z: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-45001-Implementation-Guide.pdf

Klíčovými prvky této normy[63] jsou:

- Závazek vedení na zlepšování bezpečnosti
- Účast zaměstnanců
- Identifikaci nebezpečí a hodnocení rizik
- Dodržování právních a jiných požadavků dané země
- Plánování nouzových situací
- Vyšetřování incidentů
- Neustálé zlepšování

Norma ISO 45001 využívá metodologii Plan-Do-Check-Act (PDCA) pro systematické řízení rizik BOZP. Platí pro organizace všech velikostí a lze ji integrovat s jinými normami ISO pro systémy řízení[64].

Výhody zavedení této normy[65] jsou:

- Poskytnutí mezinárodně uznávaného rámce pro řízení rizik BOZP. Umožňuje organizacím systematicky posuzovat nebezpečí a implementovat opatření pro jejich kontrolu, což vede ke snížení pracovních úrazů, nemocí a incidentů.
- Přijetí normy ukazuje zaměstnancům a externím organizacím, že je organizace zavázána k ochraně zdraví, bezpečnosti a pohodě pracovníků.
- Norma vyžaduje dodržování právních a jiných požadavků na BOZP, čímž zajišťuje právní soulad. Také podporuje proaktivní řízení rizik, což může snížit výdaje za pracovní úrazy.
- Tím, že vyžaduje protokoly pro přípravu a reakci na nouzové situace, norma ISO 45001 posiluje organizační odolnost proti bezpečnostním hrozbám a krizím.
- Díky PDCA se může systém BOZP neustále zlepšovat a vyvíjet, čímž se zvyšuje jeho dlouhodobý výkon.

[63] ISO 45001:2018

[64] TILHON, Jiří; SKŘEHOT, Petr a VALA, Jiří. Komentované vydání ČSN ISO 45001: systémy managementu bezpečnosti a ochrany zdraví při práci: požadavky s návodem k použití. Praha: Česká společnost pro jakost, [2018?]. ISBN 978-80-02-02840-6.

[65] ISO 45001:2018

3.1.2 ISO 27001 Systém managementu informační bezpečnosti

Mezinárodní norma ISO/IEC 27001:2022 stanovuje požadavky na systém řízení informační bezpečnosti (ISMS). Norma poskytuje rámec pro organizace, jak řídit rizika spojená s bezpečností informací, kybernetickou bezpečností a ochranou soukromí. Norma obsahuje kritéria pro politiku informační bezpečnosti, cíle, plánování, provádění, monitorování, revizi a zlepšování ISMS[66].

Klíčovými prvky této normy[67] jsou:

- Závazek vedení k podpoře informační bezpečnosti
- Zapojení zainteresovaných stran
- Identifikace nebezpečí a hodnocení rizik
- Dodržování právních a jiných požadavků na informační bezpečnost
- Plánování a reakce na incidenty a nouzové situace
- Vyšetřování a řešení nekonformit
- Neustálé zlepšování

Norma ISO/IEC 27001 využívá také metodologii Plan-Do-Check-Act (PDCA) pro systematické řízení rizik informační bezpečnosti. Platí pro organizace všech velikostí a lze ji integrovat s jinými normami ISO pro systémy řízení[68].

Výhody zavedení této normy[69] jsou:

- Poskytnutí mezinárodně uznávaného rámce pro řízení rizik informační bezpečnosti. Umožňuje organizacím systematicky posuzovat nebezpečí a implementovat opatření pro jejich kontrolu, což vede ke snížení počtu a dopadu bezpečnostních incidentů.
- Přijetí normy ukazuje zainteresovaným stranám, že je organizace zavázána k ochraně informací, kybernetické bezpečnosti a soukromí.

[66] NOVÁK, Luděk a POŽÁR, Josef. Systém řízení informační bezpečnosti. Online. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf. [cit. 2024-02-11].
[67] ISO/IEC 27001:2022
[68] NOVÁK, Luděk a POŽÁR, Josef. Systém řízení informační bezpečnosti. Online. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf. [cit. 2024-02-11].
[69] TA-SEEN, Junaid. ISO 27001: Information Security Management Systems. Online. In: . Dostupné z: https://doi.org/10.13140/RG.2.2.36267.52005. [cit. 2024-02-11].

- Norma vyžaduje dodržování právních a jiných požadavků na informační bezpečnost, čímž zajišťuje právní soulad. Také podporuje proaktivní řízení rizik, což může snížit náklady na nápravu a sankce.
- Tím, že vyžaduje protokoly pro přípravu a reakci na incidenty a nouzové situace, norma ISO/IEC 27001 posiluje organizační odolnost proti bezpečnostním hrozbám a krizím.
- Díky PDCA se může ISMS neustále zlepšovat a vyvíjet, čímž se zvyšuje jeho dlouhodobý výkon.

3.1.3 ISO 9001 Systém managementu kvality

Mezinárodní norma ISO 9001:2015 stanovuje požadavky na systém managementu kvality (QMS). Norma poskytuje organizacím rámec pro efektivní řízení a zlepšování kvality produktů a služeb. Obsahuje kritéria pro tvorbu politiky kvality, stanovování cílů, plánování, implementaci, monitorování, měření, analýzu a neustálé zlepšování QMS[70].

Klíčové prvky normy[71] ISO 9001:2015 zahrnují:

- Zaměření na zákazníka
- Zapojení vedení a všech zaměstnanců
- Procesní přístup k managementu
- Systém pro hodnocení a zlepšování
- Důraz na prevenci vad
- Neustálé zlepšování

Norma ISO 9001:2015 je univerzální a lze ji aplikovat na organizace všech typů a velikostí v jakémkoli odvětví. Tato norma je důležitá především z ekonomického bezpečnostního hlediska. Pokud by výrobek daného podniku nebyl dostatečně kvalitní, podnik by ztratil klientelu, a tedy i ekonomický zisk.

[70] Hillnhagen, Simon & Mütze, Alexander & Nyhuis, Peter & Schmidt, Matthias. (2024). Influence of ISO 9001 on the configuration of production planning and control. Procedia CIRP. 120. 10.1016/j.procir.2023.09.165.

[71] ISO 9001:2015

Výhody zavedení normy[72] ISO 9001:2015:

- Zlepšení spokojenosti zákazníků
- Zvýšení efektivity a produktivity
- Snížení nákladů
- Zvýšení konkurenceschopnosti
- Lepší přístup na trh
- Zlepšení image a reputace podniku

3.1.4 ISO 14001 Systém enviromentálního managementu

Mezinárodní norma ISO 14001:2015 stanovuje požadavky na systém environmentálního managementu (EMS). Norma poskytuje organizacím rámec pro efektivní řízení environmentálních aspektů a dopadů jejich činností. Obsahuje kritéria pro tvorbu environmentální politiky, stanovování cílů, plánování, implementaci, monitorování, měření, analýzu a neustálé zlepšování EMS[73].

Klíčové prvky této normy[74] zahrnují:

- Závazek vedení k ochraně životního prostředí
- Dodržování platných environmentálních právních a jiných požadavků
- Prevence znečišťování
- Neustálé zlepšování environmentálního výkonu
- Operační kontrolu a zvládání environmentálních aspektů
- Připravenost a reakci na mimořádné situace
- Komunikaci s relevantními zainteresovanými stranami

Stejně jako ostatní normy, tak i tato je univerzální a lze ji použít na jakýkoliv podnik. Z hlediska bezpečnosti podniku se jedná především o enviromentální bezpečnost viz kapitola Enviromentální bezpečnost.

[72] Hillnhagen, Simon & Mütze, Alexander & Nyhuis, Peter & Schmidt, Matthias. (2024). Influence of ISO 9001 on the configuration of production planning and control. Procedia CIRP. 120. 10.1016/j.procir.2023.09.165.
[73] ISO 14001:2015
[74] Tamtéž

Výhody zavedení normy[75]:

- Snížení environmentálních dopadů a rizik
- Zvýšení efektivity a produktivity
- Snížení nákladů
- Zlepšení image a reputace
- Lepší přístup na trh – v dnešní době se více hledí na otázky recyklace, upcyklace apd.
- Zlepšení motivace a zapojení zaměstnanců do procesů

3.1.5 ISO 31000 Systém řízení rizik

Mezinárodní norma ISO 31000:2018[76] stanovuje principy a obecné pokyny pro řízení rizik. Norma poskytuje organizacím rámec pro efektivní identifikaci, hodnocení a řízení rizik v jakémkoli kontextu. Obsahuje kritéria pro tvorbu politiky řízení rizik, stanovování cílů, plánování, implementaci, monitorování, měření, analýzu a neustálé zlepšování systému řízení rizik.

Klíčové prvky normy[77] ISO 31000:2018 zahrnují:

- Integrovaný přístup k řízení rizik
- Zapojení vedení a všech zaměstnanců
- Systematická identifikace a hodnocení rizik
- Plánování a implementace opatření na ošetření rizik
- Monitorování a přezkum řídících mechanismů
- Neustálé zlepšování systému řízení rizik

Opět univerzální norma, kterou lze aplikovat na jakýkoliv podnik. Jak již z názvu normy vyplývá, jedná se o normu zaměřenou na rizika v podniku. Díky aplikaci lze snížit tato rizika na minimum, a tedy chránit podnik ve všech oblastech bezpečnosti viz předchozí kapitoly.

[75] Hidayati, Ruti & SODIKIN, SODIKIN. (2023). Benefit analysis of the implementation of Environmental Management System (EMS) ISO 14001:2015 in a tyres industry. Indonesian Journal of Applied Environmental Studies. 4. 77-84. 10.33751/injast.v4i2.8897.

[76] ISO 31000:2018

[77] Tamtéž

Výhody zavedení normy[78] ISO 31000:2018:

- Zlepšení informovanosti o rizicích a jejich dopadu
- Zvýšení efektivity a produktivity
- Snížení nákladů
- Lepší dodržování právních a jiných požadavků
- Zvýšení odolnosti organizace

3.2 Právní a ostatní regulace řízení bezpečnosti podniku

Kromě mezinárodních standardů v oblasti řízení bezpečnosti podniku existují také jisté právní regulace, které jsou povinné pro podniky v dané zemi. Právní regulace v oblasti řízení bezpečnosti podniku je často specifická pro danou zemi – jiné zákony platí v České republice, jiné v Belgii, Německu apd. V souvislosti s bezpečností podniku v České republice je především regulována oblast zaměřená na BOZP a PO a související právní předpisy a enviromentální bezpečnost se souvisejícími právními předpisy.

3.2.1 Právní řád Evropské unie

I když bylo zmíněno, že každý stát má specifické právní předpisy, tak státy v Evropské unii se musí řídit v případě rozporu primárné Evropským právem. Toto právo se dělí[79] na primární právo a sekundární právo. Primární právo je tvořeno smlouvami a právními akty, které vymezují ústavní rámec EU. Sekundární právo je tvořeno nařízeními a směrnicemi, které jsou v dnešní době hlavním zdrojem práva EU.

Pro oblast bezpečnosti[80] jsou hlavním zdrojem nařízení a směrnice evropských společenství. Nařízení ES jsou obecně závazné předpisy, které platí pro členské státy EU. Mezi takové nařízení, vztahující se na oblast bezpečnosti lze uvést například Nařízení Evropského parlamentu a Rady (ES) č. 1272/2008 o klasifikaci,

[78] Bochkovskyi, A.. (2020). Improvement of risk management principles in occupational health and safety. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 94-104. 10.33271/nvngu/2020-4/094.

[79] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[80] Tamtéž

označování a balení látek a směsí (CLP) nebo Nařízení Evropského parlamentu a Rady (EU) 2023/1230 o strojních zařízeních.

3.2.2 Právní řád České republiky

Prameny práva v ČR jsou právní předpisy, mezinárodní smlouvy a specifická rozhodnutí Ústavního soudu. Dále zde existují vyhlášky a nařízení, což jsou podzákonné formy, které neobsahují stanovení povinností, pokud k tomu nejsou zmocněny zákonem. Předpisy mají různou právní sílu od Ústavního zákona, až právě po nařízení vlády a vyhlášky.[81]

Stejně jako v předchozí kapitole, i pro oblast bezpečnosti jsou v České republice specifické zákony, nařízení a vyhlášky. Vzhledem k tomu, že existuje mnoho oblastí bezpečnosti, zmíníme v této kapitole jen několik předpisů a vyhlášek pro představu:

- Zákon č. 262/2006 Sb. Zákon zákoník práce – stanovuje obecné požadavky na zajištění bezpečnosti práce a ochrany zdraví při práci
- Zákon č. 133/1985 Sb., o požární ochraně – stanovuje požadavky na zajištění požární ochrany v objektech a při činnostech
- Zákon č. 22/1997 Sb., o technických požadavcích na výrobky – stanovuje požadavky na bezpečnost výrobků uváděných na trh
- Nařízení vlády č. 375/2004 Sb., kterým se stanoví podmínky ochrany zdraví při práci – upřesňuje požadavky na zajištění bezpečnosti práce v konkrétních oblastech
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví – stanovuje požadavky na ochranu zdraví při práci

3.2.3 Normy ČSN

České technické normy (ČSN) lze zařadit do ostatní regulace řízení bezpečnosti[82]. Tyto normy nejsou, podle Zákona č. 22/1997 Sb. o technických požadavcích na výrobky, obecně závazné, ale jsou platné. Technické normy

[81] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[82] Tamtéž

obsahují odborné rady a jejich uplatňování je obvykle dobrovolné. Nicméně je často prospěšné řídit se podle pravidel dané normy. Zvláštní právní postavení mají harmonizované normy a specifikované technické normy, které se používají pro hodnocení shody určitých výrobků.

Konkrétní pravidlo české technické normy, nebo i celá norma, může být určeno povinným (tedy právně vynutitelným) na základě několika právních dokumentů[83], resp. činností, a to zákonem, dohodou mezi dvěma nebo více stranami, rozhodnutím úřadu na základě oprávnění daného zákonem, vnitřním nařízením subjektu, resp. na příkaz nadřízeného. Vždy platí, že pravidlo normy je povinné jen pro subjekty, na které se vztahuje odpovídající požadavek dokumentu, který určil pravidlo povinným.

Odkazy pro ČSN[84] v českých právních předpisech se mohou provést různými způsoby:

- Výlučně – definování jediného možného způsobu, jak splnit příslušné ustanovení právního předpisu
- Indikativně – použití ustanovení normy je jedním z možných způsobů naplnění požadavku právního předpisu
- Odkaz na normovou hodnotu – v úvodu předpisu je definováno, co je považováno za normovou hodnotu
- Interními předpisy – ve firmě s odvoláním na konkrétní ČSN

4 Metody a techniky řízení bezpečnosti podniku

Čtvrtá kapitola této práce, nazvaná Metody a techniky řízení bezpečnosti podniku, se zaměřuje na různé metody a techniky, které se v tomto procesu používají.

4.1 Metody

V této podkapitole se autor zaměří na metody používané v řízení bezpečnosti podniku. Tyto metody můžeme rozdělit do tří základních kategorií: metody

[83] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.
[84] Tamtéž

zaměřené na identifikaci rizik, metody zaměřené na hodnocení rizik a metody zaměřené na ošetření rizik. Každá z těchto kategorií obsahuje několik konkrétních metod, které budou v jednotlivých podkapitolách podrobněji popsány.

4.1.1 Metody zaměřené na identifikaci rizik:

Identifikace rizik je prvním a základním krokem v procesu řízení bezpečnosti podniku. Cílem je zjistit, jaká rizika mohou ohrozit bezpečnost podniku, jaké jsou jejich zdroje, jejich příčiny a projevy. Identifikace rizik umožňuje podniku lépe pochopit své slabé a silné stránky, příležitosti a hrozby, a připravit se na možné scénáře a situace. Níže jsou vypsány některé metody, které se používají pro identifikaci rizik, jako jsou například:

- Analýza rizik[85] – systematický proces identifikace, hodnocení a ošetření rizik, která mohou ohrozit bezpečnost podniku. Analýza rizik se skládá z několika fází, jako je definice rozsahu a cílů analýzy, sběr a analýza dat, identifikace rizik, hodnocení rizik, ošetření rizik, dokumentace a komunikace výsledků, monitorování a revize analýzy[86]. Pro Analýzu rizik se používají různé metody, jako jsou například FTA – strom poruch, ETA – strom událostí, metoda HAZOP, SWOT a další.
- Brainstorming[87] – skupinová technika pro generování co nejvíce nápadů na potenciální rizika. Spočívá v tom, že se skupina lidí sejde a volně sdílí své myšlenky, otázky a obavy týkající se bezpečnosti podniku. Cílem je podnítit kreativitu, diverzitu a originalitu nápadů, aniž by je kritizovalo nebo hodnotilo. Brainstorming pomáhá podniku objevit nová a nečekaná rizika, která by jinak mohla zůstat nepovšimnuta.

[85] Metody a způsoby hodnocení rizik na pracovišti. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/. [cit. 2024-02-18].

[86] Analýza a řízení rizik BOZP. Identifikace, hodnocení a management ve firmách a jiných organizacích. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/analyza-rizik-bozp-rizeni-hodnoceni-identifikace-management/. [cit. 2024-02-18].

[87] WIKIPEDIE, Přispěvatelé. Brainstorming. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: https://cs.wikipedia.org/wiki/Brainstorming. [cit. 2024-02-18].

- Dotazníkové šetření[88] – získávání informací o rizicích od zaměstnanců a dalších zainteresovaných stran. Spočívá v tom, že se vytvoří a rozešle dotazník, který obsahuje otázky týkající se bezpečnosti podniku. Dotazník může být buď uzavřený, kdy se nabízí pevně dané odpovědi, nebo otevřený, kdy se nechává prostor pro vlastní komentáře. Dotazníkové šetření pomáhá podniku získat cenné zpětné vazby, názory a postřehy od lidí, kteří jsou zapojeni do činnosti podniku nebo jsou jimi ovlivněni.
- Kontrolní seznam[89] – je soubor otázek, které se týkají typických nebezpečí a zdrojů nehod. Je vytvořen podle předpisů a norem, a slouží k posouzení bezpečnosti systému. Kontrolní seznam musí být aktuální a vytvořený odborníky. Každá otázka má možnost ano – ne. Kontrolní seznam má výhodu snadného použití, ale má nevýhodu mechanického přístupu a omezenosti zkušenostmi. Kontrolní seznam se používá pro identifikaci nebezpečí v jakékoliv fázi života systému.
- Metoda What-If[90] – je metoda, která se používá k identifikaci nebezpečí a rizik v procesu pomocí otázek a odpovědí. Pracovní tým odborníků se ptá, co se stane, když se něco změní nebo pokazí v procesu, a hledá možné následky a opatření. Metoda je intuitivní, rychlá a efektivní, ale méně systematická a závislá na zkušenostech týmu. Metoda se hodí pro jednoduché nebo známé procesy, pro složitější procesy je lepší použít jinou metodu. Metoda vyžaduje dobrou znalost procesu, kvalitní tým a tvořivou atmosféru.

4.1.2 Metody zaměřené na hodnocení rizik:

Hodnocení rizik je druhým krokem v procesu řízení bezpečnosti podniku. Cílem je kvantifikovat nebo kvalifikovat rizika, která byla identifikována v předchozím kroku, a určit jejich prioritu, přijatelnost a potřebu ošetření. Hodnocení rizik

[88] WIKIPEDIE, Přispěvatelé. Dotazníkové šetření. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: https://cs.wikipedia.org/wiki/Dotazn%C3%ADkov%C3%A9_%C5%A1et%C5%99en%C3%AD. [cit. 2024-02-18].

[89] HÁJKOVÁ, Martina. Identifikace nebezpečí a hodnocení rizik - metody. Online. BOZPinfo.cz. Dostupné z: https://www.bozpinfo.cz/identifikace-nebezpeci-hodnoceni-rizik-metody. [cit. 2024-02-18].

[90] Tamtéž

umožňuje podniku porovnat rizika mezi sebou, stanovit kritéria pro jejich řízení, a rozhodnout, jaké opatření je třeba podniknout. Existuje několik metod[91], které se používají pro hodnocení rizik, jako jsou například:

- Semi-kvantitativní metody[92] – spočívají v tom, že se používají předem definované stupnice, tabulky nebo matice, které přiřazují rizikům číselné hodnoty podle toho, jak často se mohou vyskytnout a jak velké škody mohou způsobit. Tyto hodnoty se pak sčítají nebo násobí, aby se získalo celkové skóre rizika, které slouží k jeho uspořádání a kategorizaci.
- Kvantitativní metody[93] – spočívají v tom, že se používají matematické, statistické nebo simulační techniky, které umožňují odhadnout pravděpodobnost a důsledky rizik na základě dostupných dat, expertních úsudků nebo scénářů. Tyto hodnoty se pak používají k výpočtu ukazatelů, jako jsou například očekávaná ztráta, variační koeficient, hodnota v riziku, nebo křivka přežití, které slouží k měření a srovnávání rizik. Mezi některé kvantitativní metody patří metody ETA, FTA, HAZOP, QRA.
- Kvalitativní metody[94] – spočívají v tom, že se používají otevřené, nestrukturované nebo polouzavřené otázky, rozhovory, pozorování, a další zdroje dat. Tato data se pak analyzují pomocí induktivní, abduktivní nebo interpretativní logiky, které umožňují vytvářet hypotézy nebo teorie, které slouží k objasnění a porozumění zkoumaným jevům. Mezi kvalitativní metody patří pozorování, nejhorší případ, bezpečnostní prohlídky a další.

4.1.3 Metody zaměřené na ošetření rizik:

Ošetření rizik je třetím krokem v procesu řízení bezpečnosti podniku. Cílem je snížit nebo eliminovat rizika, která byla identifikována a hodnocena v předchozích

[91]Metody a způsoby hodnocení rizik na pracovišti. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/. [cit. 2024-02-18].

[92] Polokvantitativní metoda – parametr "pravděpodobnost ohrožení". Online. Parametr "pravděpodobnost ohrožení" | BOZPinfo.cz. Dostupné z: https://www.bozpinfo.cz/polokvantitativni-metoda-parametr-pravdepodobnost-ohrozeni. [cit. 2024-02-18].

[93] JIŘINKA. Současný charakter vykonávané.. Online. Znalostní systém prevence rizik v BOZP. Dostupné z: https://zsbozp.vubp.cz/metody-hodnoceni-rizik. [cit. 2024-02-18].

[94] Polokvantitativní metoda – parametr "pravděpodobnost ohrožení". Online. Parametr "pravděpodobnost ohrožení" | BOZPinfo.cz. Dostupné z: https://www.bozpinfo.cz/polokvantitativni-metoda-parametr-pravdepodobnost-ohrozeni. [cit. 2024-02-18].

krocích, a zajistit, že zbylá rizika jsou na přijatelné úrovni. Ošetření rizik umožňuje podniku zlepšit svou bezpečnostní situaci, snížit náklady a ztráty spojené s bezpečnostními problémy, a dodržovat legislativní a normativní požadavky na bezpečnost. Existuje několik metod, které se používají pro ošetření rizik, jako jsou například:

- Eliminace[95] – úplné odstranění rizika. Eliminace je nejúčinnější a nejžádanější metoda ošetření rizik, protože znamená, že riziko již neexistuje a nemůže způsobit žádné škody. Eliminace se používá pro rizika s vysokou pravděpodobností a závažností, která nelze snížit jinými způsoby. Eliminace může zahrnovat například změnu procesu, produktu nebo služby, odstranění nebezpečného materiálu nebo zařízení, zrušení činnosti nebo funkce, aj.
- Prevence[96] – snížení pravděpodobnosti výskytu rizika. Prevence je druhou nejúčinnější a nejžádanější metodou ošetření rizik, protože znamená, že riziko se stává méně pravděpodobným a tím i méně nebezpečným. Prevence se používá pro rizika s vysokou nebo střední pravděpodobností, která nelze eliminovat. Prevence může zahrnovat například zavedení preventivních opatření, kontrol, norem, procedur, školení, osvěty, motivace, aj.
- Zmírnění[97] – snížení závažnosti dopadů rizika. Zmírnění je třetí nejúčinnější a nejžádanější metodou ošetření rizik, protože znamená, že riziko má menší následky a tím i menší škody. Zmírnění se používá pro rizika s vysokou nebo střední závažností, kterou nelze eliminovat nebo jí zabránit. Zmírnění může zahrnovat například zavedení zmírňujících opatření, náhrad, rezerv, pojištění, nápravy, obnovy, aj.
- Přenos[98] – přenesení rizika na jinou stranu (např. pojištěním). Přenos je čtvrtou nejúčinnější a nejžádanější metodou ošetření rizik, protože znamená, že riziko je sdíleno nebo převzato jinou stranou, která je schopna

[95] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-8750-019-4.
[96] Tamtéž
[97] Tamtéž
[98] Tamtéž

lépe ho zvládnout nebo snášet. Přenos se používá pro rizika s nízkou nebo střední pravděpodobností a závažností, která nelze eliminovat, zabránit nebo zmírnit. Přenos může zahrnovat například uzavření smlouvy, dohody, koncese, partnerství, outsourcingu, pojištění, garance, aj.

- Akceptace[99] – souhlas s existencí a ponecháním rizika. Akceptace rizika je nejméně účinná a nejméně žádaná metoda ošetření rizik, protože znamená, že riziko není řešeno ani snižováno, ale pouze tolerováno. Akceptace rizika se používá pro rizika s nízkou pravděpodobností a závažností, která nelze odstranit nebo předcházet, nebo jejichž řešení by bylo příliš nákladné nebo nepraktické. Akceptace rizika může zahrnovat například přijetí rizika jako součásti podnikání, pojištění proti riziku, vytvoření rezervy na riziko, nebo ignorování rizika.

4.2 Techniky

Tato kapitola je zaměřena na techniky používané v řízení bezpečnosti podniku. Tyto techniky můžeme opět rozdělit do tří základních kategorií: techniky zaměřené na prevenci, techniky zaměřené na ochranu a techniky zaměřené na monitorování a zlepšování. Každá z těchto kategorií obsahuje několik konkrétních technik, které budou v této kapitole podrobněji popsány.

4.2.1 Techniky zaměřené na prevenci

Prevence je jednou z nejdůležitějších a nejefektivnějších strategií v řízení bezpečnosti podniku. Cílem je zabránit vzniku nebo výskytu rizik, která by mohla ohrozit bezpečnost podniku, jeho zaměstnanců, zákazníků, dodavatelů, majetku nebo životního prostředí. Prevence se opírá o principy proaktivního, preventivního a participativního přístupu k bezpečnosti. Níže jsou uvedené některé techniky, které se používají pro prevenci rizik:

[99] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-8750-019-4.

- Školení zaměstnanců[100] – školení zaměstnanců by mělo být nedílnou součástí strategie firmy, která chce předcházet rizikům vzniklých lidským přičiněním. Školení obecně jsou způsoby, jak zvyšovat znalosti a dovednosti zaměstnanců, a také zlepšit jejich postoj vůči firmě a motivovat je k bezpečnému chování na pracovišti, dodržování bezpečnostních pravidel a postupů, a naučit je, jak reagovat na bezpečnostní situace. Školení mohou probíhat jak teoreticky, tak prakticky, mohou být individuální nebo skupinové, povinné nebo dobrovolné, periodické nebo jednorázové, a mohou se týkat různých témat, jako jsou například základy bezpečnosti u VTZ, řízení vysokozdvižných vozíků, evakuace při požáru, používání OOPP, první pomoc, práce ve výškách a další.
- Implementace standardů[101] – implementace a dodržování bezpečnostních standardů relevantních pro daný obor a typ podniku by mělo být stěžejní pro management každého podniku. Bezpečnostní standardy jsou soubory pravidel, norem, požadavků, kritérií, metod, postupů a dalších dokumentů, které stanovují, jak má být zajištěna bezpečnost podniku, jeho činností, procesů, produktů, služeb, zařízení, materiálů, a dalších prvků. Bezpečnostní standardy jsou dobrovolné. Jsou buď národního nebo mezinárodního charakteru, a mohou se týkat různých aspektů bezpečnosti, jako jsou například BOZP, fyzická bezpečnost, personální bezpečnost a další viz předchozí kapitoly zaměřené na oblasti bezpečnosti a standardy.
- Pravidelná údržba[102] – pravidelná údržba a kontrola strojů a zařízení pro zajištění jejich bezpečného provozu je nezbytná pro eliminaci rizik na pracovišti. Pravidelná údržba a kontrola jsou činnosti, které spočívají v tom, že se provádějí pravidelné prohlídky, dělají se zkoušky, provádí se měření. Dále se provádí čištění, mazání, opravy, kalibrování, a další úkony, které

[100] NEUGEBAUER, Tomáš. Školení bezpečnosti práce, požární ochrany a motivační školení k prevenci rizik. 2. vydání. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-957-2.

[101] Viz předchozí kapitoly

[102] JIŘINKA. Bezpečnost práce v údržbě a opravárenství. Online. Znalostní systém prevence rizik v BOZP. Dostupné z: https://zsbozp.vubp.cz/bezpecnost-prace-v-udrzbe-a-opravarenstvi. [cit. 2024-02-18].

mají za cíl udržovat stroje a zařízení v dobrém technickém stavu, zabránit jejich opotřebení, předejít závadám a poruchám, a zlepšovat jejich výkonnost, spolehlivost a životnost. Pravidelná údržba a kontrola se nejčastěji provádí podle plánu, nebo návodu od výrobce. V případě, že se jedná o jiné technické zařízení, je zde i nutnost provádět kontrolu např. podle norem – ČSN 33 1600 ED.2 – Revize a kontroly elektrických spotřebičů během používání.

4.2.2 Techniky zaměřené na ochranu

Ochrana je další ze strategií v řízení bezpečnosti podniku. Jejím cílem je chránit podnik a jeho zaměstnance, majetek nebo životní prostředí před riziky, která by mohla ohrozit jejich bezpečnost, a zmírnit jejich dopady, pokud se rizika projeví. Ochrana se opírá o principy reaktivního přístupu k bezpečnosti. Zde jsou některé techniky, které se používají pro ochranu před riziky, jako jsou například:

- Krizové plány a postupy[103] – nouzové plány a postupy jsou dokumenty, které popisují, jak má podnik reagovat na různé typy mimořádných událostí, jako jsou například požáry, úniky nebezpečných látek, sabotáž a další potenciální rizika. Nouzové plány a postupy obsahují informace o zodpovědných osobách, jejich rolích a úkolech, o hlavních komunikačních kanálech, o zdrojích a prostředcích, o evakuační trasách a místech shromáždění. Dále obsahují informace o zásadách a pravidlech, a dalších aspektech, které mají za cíl zajistit bezpečnost a ochranu lidí, majetku a životního prostředí v případě vzniku nežádoucí události.
- Požární ochrana[104] – implementace protipožárních opatření a systémů pro minimalizaci rizik vzniku a šíření požáru je v nutná a musí se provést podle zákona o požární ochraně[105]. Požární ochrana je soubor činností, které spočívají v tom, že se provádějí preventivní opatření, které mají za cíl snížit nebo odstranit škody způsobené požárem. Požární ochrana zahrnuje

[103] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce. 2. vydání. Wolters Kluwer, 8/2016n. l., 380 s. ISBN 978-80-7552-107-1

[104] Jaké jsou povinnosti na úseku zajištění požární ochrany? Zde je základní přehled. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/jake-jsou-povinnosti-na-useku-zajisteni-pozarni-ochrany/. [cit. 2024-02-18].

[105] Zákon č. 133/1985 Sb.Zákon České národní rady o požární ochraně

například instalaci a údržbu hasicích přístrojů, hasících hydrantů, protipožárních dveří, únikových tras a dokumentace požární ochrany, která zahrnuje například požární řád, požární poplachové směrnice, požární evakuační plán a další.

- Ochranné osobní pracovní prostředky[106] – poskytování a používání ochranných osobních pracovních prostředků (OOPP) pro ochranu zdraví a životů zaměstnanců jsou zařízení, pomůcky, oděvy, obuv, rukavice, brýle a další věci, které slouží k ochraně zaměstnanců před riziky, která mohou ohrozit jejich zdraví a životy při práci. OOPP musí být vhodně vybrány podle účelu pracovního zařazení. Musí být poskytnuty odpovědným pracovníkem, a hlavně musí být používány daným zaměstnancem na dané pracovní pozici.
- Bezpečnostní signály a značení[107] – zaměstnavatel je povinen zajistit bezpečnostní značení a signály na místech, kde se provádějí činnosti, které mohou ohrozit zdraví. Tyto značky a signály mají za cíl poskytnout informace nebo pokyny týkající se ochrany zdraví při práci. Bezpečnostní značení a signály mohou být například vizuální, akustické nebo světelné.

4.2.3 Techniky zaměřené na monitorování a zlepšení

Monitorování a zlepšení jsou posledními strategiemi v řízení bezpečnosti podniku. Cílem je sledovat a vyhodnocovat úroveň bezpečnosti podniku, jeho rizika, incidenty, nehody, poruchy, náklady, výkony a další ukazatele, a na základě získaných informací provádět nápravná a preventivní opatření, která mají za cíl zvýšit bezpečnost a efektivitu podniku. Monitorování a zlepšování se opírají o principy zpětné vazby, kontroly, měření, hodnocení, analýzy, řešení problémů, inovace a neustálého zlepšování. Existuje několik technik, které se používají pro monitorování a zlepšování bezpečnosti podniku, jako jsou například:

[106] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce. 2. vydání. Wolters Kluwer, 8/2016n. l., 380 s. ISBN 978-80-7552-107-1

[107] Tamtéž

- Audity[108] – pravidelné audity a kontroly jsou způsoby, jak lze ověřit, zda podnik plní své bezpečnostní cíle, politiku, plány, postupy, návody, normy, zákony a další požadavky, které se týkají bezpečnosti podniku. Audity a kontroly mohou být jak interní, tak i externí. Mohou být plánované nebo neplánované a mohou se týkat různých oblastí, jako například BOZP, fyzická bezpečnost, personální bezpečnost, ekonomická bezpečnost, a další.
- Monitoring[109] – sledování a vyhodnocování bezpečnostních rizik a incidentů je způsob, jak sbírat, zaznamenávat, analyzovat a interpretovat data o bezpečnostních rizicích a incidentech, které se vyskytují v podniku. Monitorování pomáhá podniku identifikovat a řešit bezpečnostní problémy, a zároveň poskytuje zpětnou vazbu o účinnosti již aplikovaných bezpečnostních opatření.
- Vyšetřování incidentů[110] – provádění důkladných vyšetřování incidentů a přijímání nápravných opatření je způsob, jak zjistit, co se stalo, proč se to stalo, jaké byly důsledky, a co se dá udělat, aby se to neopakovalo. Vyšetřování incidentů zahrnuje sběr a analýzu důkazů, výslech zaměstnanců, stanovení příčin, navrhování a provádění nápravných a preventivních opatření, a dokumentování výsledků.

5 Přístupy

V páté kapitole se autor zaměří na jednotlivé přístupy k řízení bezpečnosti podniku. Nejprve představí dva základní přístupy: proaktivní a reaktivní. Proaktivní přístup se zaměřuje na prevenci incidentů a zahrnuje analýzu rizik, plánování

[108] Audit bezpečnosti práce (BOZP). Příprava, postupy a tipy pro realizaci. Online. Couldn't find publisher. Dostupné z: https://www.bozp.cz/aktuality/audit-bezpecnosti-prace/. [cit. 2024-02-18].

[109] Amanipour, Soheil & Klaus, Hubert. (2024). Security Auditing and Monitoring: Incident response and management.

[110] DASHÖFER, Verlag. Význam procesu vyšetřování incidentů. Online. Články na témata bezpečnost práce, Legislativa a komentáře, Poradna BOZP, Ochrana zdraví při práci, Prevence rizik, Technicko-bezpečnostní rozbory činností, Školení a vzdělávání BOZP, Vzorová dokumentace BOZP. Dostupné z: https://www.bozpprofi.cz/33/vyznam-procesu-vysetrovani-incidentu-uniqueidgOkE4NvrWuOKaQDKuox_Z6AjhnlZCh84lJR9Hs5aM2Y/. [cit. 2024-02-19].

a neustálé zlepšování. Reaktivní přístup se zaměřuje na řešení incidentů po jejich vzniku. V praxi se obvykle používá kombinace obou přístupů.

V další části kapitoly se bude věnovat dalším specifickým přístupům k řízení bezpečnosti, jako je rizikový přístup, systémový přístup, procesní přístup, přístup založený na chování zaměstnanců, principy High-Reliability Organizations (HRO), Inherent Safety Design (ISD) a Human Factors Engineering (HFE).

5.1 Proaktivní a reaktivní přístup

Proaktivní a reaktivní přístup k bezpečnostnímu managementu představují dva základní přístupy, které řídí, jak by měla organizace reagovat na bezpečnost a jak by se měla snažit předcházet budoucím incidentům.

5.1.1 Reaktivní přístup

Reaktivní přístup k řízení bezpečnosti[111] se zaměřuje na řešení bezpečnostních incidentů po jejich vzniku. Tento přístup se snaží minimalizovat škody a zabránit opakování incidentů v budoucnu.

Základní vlastnosti tohoto přístupu jsou:

- Řešení incidentů – zaměřuje se pouze na to, co se stalo a řeší, jak incidenty napravit
- Nedostatek prevence – nesoustředí se na prevenci
- Učení se z chyb – tento přístup se učí z chyb a snaží se je neopakovat
- Nízké náklady – je levnější, než proaktivní přístup

Z vlastností uvedených výše vyplývá, že velkou nevýhodou tohoto přístupu bude nákladnost při řešení incidentů a přerušení produkce ve výrobě a tím i další ekonomická ztráta. V případě úrazu se pak bude jednat o další výdaje za léčení a také to bude vrhat špatné světlo na podnik.

[111]Rasmussen, L. B. (2010). From reactive to proactive approach of interactive leadership. In The Ambivalent Character of Participation: New Tendencies in Worker Participation in Europe (1. ed., Vol. 20, pp. 585-612). Peter Lang.

Mezi reaktivní opatření se dá zařadit[112] vyšetřování incidentů, zálohování dat, nápravná opatření a další.

Vzhledem k výše uvedeným informacím lze usuzovat, že se tento přístup hodí spíše pro malé podniky s nízkým rizikem, nebo podniky s omezenými finančními zdroji, které si nemohou dovolit proaktivní přístup. V některých případech[113] může být naopak prevence obtížná, nebo nemožná a jediné řešení je využití reaktivního přístupu.

5.1.2 Proaktivní přístup

Proaktivní přístup k řízení bezpečnosti[114] se zaměřuje na prevenci bezpečnostních incidentů před jejich vznikem. Tento přístup se snaží identifikovat a eliminovat rizika, čímž se minimalizuje pravděpodobnost a dopad incidentů.

Hlavní vlastnosti tohoto přístupu jsou:

- Prevence – snaha předcházet incidentům
- Analýza rizik – identifikace a eliminace rizik
- Plánování – plánování a příprava v případě vzniku incidentu
- Zlepšování – neustále zlepšování bezpečnostních procesů a systémů

Z vlastností výše vyplývá, že díky proaktivnímu přístupu je lepší zabránit bezpečnostním incidentům předem, než je řešit po jejich vzniku. Tento přístup přináší podnikům řadu výhod[115], jako jsou nižší náklady a vyšší produktivita. Proaktivní přístup snižuje náklady na opravy, pokuty, odškodnění a náhrady, které jsou spojeny s bezpečnostními incidenty. Proaktivní přístup k řízení bezpečnosti je tedy efektivní a výhodný způsob, jak zajistit bezpečnost zaměstnanců, zákazníků, dodavatelů a veřejnosti.

---

[112] The Difference Between Reactive and Proactive Health. Online. Dostupné z: https://www.evotix.com/resources/blog/the-difference-between-reactive-and-proactive-health-safety-management. [cit. 2024-02-19].

[113] Rasmussen, L. B. (2010). From reactive to proactive approach of interactive leadership. In The Ambivalent Character of Participation: New Tendencies in Worker Participation in Europe (1. ed., Vol. 20, pp. 585-612). Peter Lang.

[114] Tamtéž

[115] The Difference Between Reactive and Proactive Health. Online. Dostupné z: https://www.evotix.com/resources/blog/the-difference-between-reactive-and-proactive-health-safety-management. [cit. 2024-02-19].

Mezi proaktivní opatření patří[116] audity, inspekce, monitorování, školení zaměstnanců a další.

Proaktivní přístup je tedy finančně náročnější, oproti reaktivnímu a z toho důvodu je vhodný spíše pro podniky s vysokým rizikem incidentů, pro podniky s cennými aktivy, které je nutné chránit anebo pro podniky, které chtějí minimalizovat škody při nějakém incidentu.

5.1.3 Shrnutí

Z výše uvedeného vyplývá, že proaktivní přístup je považována za důležitější a měl by být prioritou v rámci řízení bezpečnosti podniku, jelikož může pomoci předcházet incidentům. Je však náročnější na čas a zdroje. Naopak reaktivní přístup poskytuje zpětnou vazbu a umožňuje organizaci reagovat na události, které se již staly. To může ale vést i k reakci na nová rizika.

V praxi mnoho organizací používá kombinaci obou těchto přístupů. Důležité je, aby si organizace vytvořila rovnováhu mezi proaktivním a reaktivním přístupem tak, aby bylo dosaženo optimální úrovně bezpečnosti. Z následujících podkapitol, ve kterých budou zmíněny další používané přístupy bude patrné, že základem je proaktivní a reaktivní přístup.

5.2 Rizikový přístup

Rizikový přístup[117] je založen na systematickém a preventivním přístupu k identifikaci, hodnocení a řízení rizik. Jinými slovy, je to způsob, jak organizace identifikují potenciální nebezpečí a hrozby a podnikají kroky k jejich eliminaci nebo snížení pravděpodobnosti jejich výskytu. Z této definice se dá vyvodit, že se jedná především o proaktivní přístup, který využívá analýzu rizik.

[116] Proactive Vs Reactive Health And Safety Management. Online. HASpod. Dostupné z: https://www.haspod.com/blog/management/proactive-reactive-health-safety-management. [cit. 2024-02-19].

[117] What Is Proactive Risk Management? Online. RiskOptics. Dostupné z: https://reciprocity.com/resources/what-is-proactive-risk-management/. [cit. 2024-02-21].

5.2.1 Proces řízení rizik

Součástí rizikového přístupu je vytvoření tzv. Plánu řízení rizik. To znamená definovat si jednotlivé kroky[118], které podniky musí podniknout k identifikaci, hodnocení a řízení rizik. Tento proces je složen z těchto kroků:

- Identifikace rizik – to znamená aktivní hledání potenciálních rizik na pracovišti, v pracovních procesech a činnostech. K identifikaci těchto rizik lze použít různé metody, jako jsou hodnocení rizik, bezpečnostní audity a zpětná vazba od zaměstnanců.
- Hodnocení rizik – po identifikaci rizik by měla následovat jejich analýza a hodnocení. Hodnotí se jejich pravděpodobnost a potenciální závažnost následků. To pomáhá určit závažnost rizik, podle jejich možného dopadu a efektivně alokovat zdroje pro snižování těchto rizik.
- Řízení rizik – na základě hodnocení rizik se provádějí různá opatření k omezení identifikovaných rizik. Tato opatření mohou zahrnovat technická opatření (např. ochranné kryty strojů), bezpečné pracovní postupy, osobní ochranné prostředky, vzdělávací programy a administrativní opatření.
- Monitorování a hodnocení – po zavedení opatření se sleduje a průběžně hodnotí jejich účinnost. To zahrnuje sledování údajů o incidentech, skoro nehodách[119] a ukazatelů bezpečnostního výkonu k identifikaci oblastí pro zlepšení a přizpůsobení opatření podle potřeby.

5.2.2 Shrnutí

Zavedení rizikového přístupu může přinést organizacím několik významných výhod. Jednou z nich je snížení rizika a tím souvisejících nehod a zranění. To je dosaženo proaktivním identifikováním a řešením potenciálních nebezpečí. Tím se výrazně snižuje pravděpodobnost nehod. Další výhodou je zvýšení operační efektivity, která spočívá v identifikaci potenciálních narušení způsobených

[118] OLSON, David L. a WU, Desheng Dash. Enterprise Risk Management Models. Online. Springer Texts in Business and Economics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017. ISBN 978-3-662-53784-8. Dostupné z: https://doi.org/10.1007/978-3-662-53785-5. [cit. 2024-02-21].

[119] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

bezpečnostními incidenty. To umožňuje přijímat preventivní opatření a zajistit hladší provoz provozu. Prevence nehod[120] nejen snižuje nebezpečnost práce, ale také vede k úsporám nákladů spojených s lékařskými výdaji, ztrátou produktivity a výpadkem provozu způsobeným incidenty.

Proaktivní řízení rizik[121] také napomáhá lepšímu rozhodování tím, že poskytuje systematický rámec pro hodnocení a snižování rizik. To pomáhá informovaně rozhodovat managementu o investicích do bezpečnosti a alokaci zdrojů. Navíc proaktivní řízení rizik přispívá ke zlepšení dodržování předpisů. Zavedením těchto postupů organizace prokazují dodržování předpisů a vyhýbají se možným pokutám.

5.3 Systémový přístup

Systémový přístup je založen[122] na myšlence, že bezpečnost je součástí celkového systému podniku a měla by se řešit proaktivně, nikoli operativně či reaktivně. Tento přístup se zaměřuje na vytváření a poskytování praktických instrukcí pro procedurální a organizační postupy.

5.3.1 Zavedení systému

Základními kroky systémového přístupu[123] jsou:

- Zavedení systému – Prvním krokem by mělo být zavedení, vytvoření, nějakého systému, který chceme aplikovat v rámci řízení bezpečnosti. Systém by měl odrážet postoj managementu k bezpečnosti podniku, ať už v rámci BOZP, nebo jakékoliv další oblasti bezpečnosti. Zde lze využít jakýkoliv standard viz kapitola zaměřená na mezinárodní standardy v oblasti bezpečnosti. Mělo by to být plánováno na strategické úrovni.

[120] HUNZIKER, Stefan. Enterprise Risk Management. Online. Wiesbaden: Springer Fachmedien Wiesbaden, 2021. ISBN 978-3-658-33522-9. Dostupné z: https://doi.org/10.1007/978-3-658-33523-6. [cit. 2024-02-21].

[121] Tamtéž

[122] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[123] Tamtéž

- Integrace systému – to znamená, že by se tento systém měl promítnout do všech aspektů podniku. V této části lze využít cyklus PDCA, na kterém jsou postaveny všechny ISO standardy viz kapitola 3.1.
- Sledování a hodnocení systému – to zahrnuje pravidelné kontroly a revize systému, aby se zajistilo, že je stále účinný a že se rizika průběžně hodnotí a ošetřují. I to je součástí všech ISO standardů.

5.3.2 Safety Management Systems (SMS)

Je důležité zmínit, v souvislosti se systémovým přístupem, že existuje specifický přístup pro bezpečnost podniku – **Systém řízení bezpečnosti**[124]. Ten byl záměrně vytvořen, jak již z názvu vyplývá, na řízení bezpečnosti podniku.

Při zavádění systému se tedy počítá s tím, že se bude primárně jednat o systém zaměřený na bezpečnost podniku, nikoliv na systém jakosti podle ISO 9001 apd.

5.3.3 Shrnutí

Systémový přístup k řízení bezpečnosti podniku tedy představuje holistický způsob, jak začlenit bezpečnost do celkového fungování organizace. Tento přístup umožňuje organizacím lépe rozumět svým rizikům, efektivněji je řešit a neustále zlepšovat své bezpečnostní systémy.

K zavedení systémového přístupu lze využít mezinárodní standardy pro různé oblasti bezpečnosti, kterých je nespočet. Mezi ty nejznámější patří ISO 45001 a ISO 9001.

5.4 Procesní přístup

Procesní přístup řízení spočívá v tom[125], že se zaměřuje na identifikaci, pochopení a systematické řízení procesů, které probíhají v rámci organizace. Proces je definován jako soubor vzájemně propojených aktivit, které transformují vstupy na výstupy a přispívají tak k dosažení cílů organizace. Základní myšlenka

[124] SNYDER, Paul a ULLRICH, Gary. Practical Safety Management Systems. Online. 2. Newcastle, Wahsington: Aviation Supplies & Academics, 2019. ISBN 978-1-61954-887-9. Dostupné z: https://asa2fly.com/practical-safety-management-systems-softcover/. [cit. 2024-02-22].

[125] DUDEK, Martin. Procesní přístup. Online. Kvalita jednoduše - Zaměřeno na management kvality. Dostupné z: https://kvalita-jednoduse.cz/procesni-pristup/. [cit. 2024-02-22].

procesního přístupu spočívá v tom, že organizace se vnímá jako systém vzájemně propojených procesů, nikoliv jako soubor izolovaných oddělení a funkcí. Tento přístup zdůrazňuje důležitost efektivního fungování procesů a jejich vzájemného propojení.

5.4.1 Zavedení procesního přístupu

Zavedení procesního přístupu do řízení bezpečnosti podniku[126] je komplexní a trvalý proces, který vyžaduje aktivní zapojení vedení organizace i všech jejích zaměstnanců. Základními kroky implementace jsou:

- Identifikace klíčových procesů – důležitá část, kdy je potřeba definovat, které procesy jsou pro dosažení cílů organizace nejdůležitější, to se dá provést vytvořením tzv. mapy procesů.
- Definování odpovědných osob za jednotlivé procesy – každý proces by měl mít odpovědnou osobu, která bude zodpovědná za jeho fungování a zlepšování.
- Dokumentace procesů – důležitou součástí zavádění je popis jednotlivých procesů krok za krokem, aby bylo jasné, jak fungují, jaké mají mezi sebou vazby a kdo je za co zodpovědný.
- Analýza procesů – dalším důležitým krokem je sledovat, jak procesy fungují, a identifikovat oblasti, které je nutné zlepšit.
- Identifikace a implementace příležitostí ke zlepšení – na základě analýzy výkonnosti procesů je nutné identifikovat a implementovat opatření pro jejich zlepšení.
- Kontrola – procesy se neustále mění, a proto je nutné je pravidelně monitorovat a aktualizovat.

5.4.2 Shrnutí

Důležité je, aby se vedení při popisu procesů zaměřilo na důležité činnosti a popsalo je stručně a jasně, jelikož se tím budou muset orientovat i zaměstnanci

[126] DUDEK, Martin. Procesní přístup. Online. Kvalita jednoduše - Zaměřeno na management kvality. Dostupné z: https://kvalita-jednoduse.cz/procesni-pristup/. [cit. 2024-02-22].

na nižších manažerských pozicích, kteří se budou podílet na vytváření procesních map a karet procesů.

Díky tomu může být procesní přístup efektivním nástrojem[127], který může organizacím pomoci dosáhnout jejich cílů i mimo bezpečnost podniku. Je však důležité, aby byl implementován správně a aby se na něm aktivně podíleli všichni zaměstnanci.

5.5 Přístup založený na chování zaměstnanců

Tzv. Behavior – based safety (BBS) je proaktivní přístup[128], který se zaměřuje na pochopení a ovlivňování chování zaměstnanců, které může vést k nehodám a vzniku rizik. Na rozdíl od tradičních bezpečnostních programů, které primárně zdůrazňují pravidla, postupy a technická opatření, BBS uznává, že lidské chování je významným faktorem při pracovních incidentech. Jeho cílem je vytvořit takovou firemní kulturu, kde bude každý zodpovědný za svou vlastní bezpečnost a bezpečnost ostatních.

5.5.1 Aplikace BBS

Při aplikaci tohoto přístupu se využívá[129] těchto sedm klíčových principů:

- Zaměření se na chování – prvním z principů je zaměření se na chování zaměstnanců, co dělají a analyzovat jejich chování a snažit se toto chování změnit.
- Vyhledávání externích faktorů – druhý princip je zaměřen na externí faktory, jelikož se člověk chová tak, jak se chová i díky prostředí, ve kterém pracuje, je důležité analyzovat a identifikovat okolní prostředí. Může se jednat o benevolentní bezpečnostní systém firmy, kdy zaměstnanci zbytečně riskují, nebo špatný management firmy a tím demotivaci zaměstnanců konat tak, jak by měli.

[127] Procesní přístup v ISO 9001:2015. Online. Česká společnost pro jakost. Dostupné z: https://www.csq.cz/fileadmin/user_upload/ISO9001_2015_Guidance_on_the_Process_Approach_CZ.pdf. [cit. 2024-02-22].

[128] Behavior Based Safety. Online. SafetyCulture. Dostupné z: https://safetyculture.com/topics/behavior-based-safety/. [cit. 2024-02-22].

[129] GELLER, E. Scott. Behavior-Based Safety and Occupational Risk Management. Online. Behavior Modification. 2005, roč. 29, č. 3, s. 539-561. ISSN 0145-4455. Dostupné z: https://doi.org/10.1177/0145445504273287. [cit. 2024-02-22].

- Řídit a motivovat – tento princip naráží na skutečnost, že jsou lidé řízeni tzv. aktivátory (signály z vnějšího světa – zvonění telefonu). Tyto aktivátory jsou však pouze tak silné, jako jsou jejich možné následky – příjemný, nebo nepříjemný. Tyto následky jsou subjektivní a každý jedinec je vnímá jinak. Tento princip se označuje také jako ABC – activator (aktivátor), behavior (chování), C – consequence (následky).
- Pozitivní motivace následků – princip se opírá o to, že by se měl podnik zaměřit na pozitivní hodnocení, nikoli negativní. Tím se myslí například míra úrazů daného podniku. To zaměstnance demotivuje a bojí se, aby se jim nic nestalo. Místo toho by se měl zaměřit na to, jakých cílů dosáhnout a tím motivovat zaměstnance k jejich dosažení.
- Aplikace vědeckých metod – chování zaměstnanců lze objektivně pozorovat a měřit před a po zahájení pracovního procesu, k tomu je vhodné použít vědecké metody, které nám poskytnou zpětnou vazbu pro zlepšení. Tyto metody by měly být vhodné pro vedoucí zaměstnance a neměly by být příliš složité. Jednou z takových metod je DO IT – define (definuj), observe (pozoruj), intervene (zasáhni), test (otestuj).
- Použití teorie pro integraci informací, ne pro omezení možností – tento princip říká, že teorie by neměla být používána k omezování možností výzkumu, ale k začleňování informací získaných ze systematických pozorování chování. Místo toho, aby se výzkum řídil určitou teorií, měl by být otevřený všem výsledkům a upravovat postupy podle dat. Tím se může vyvinout výzkumně podložená teorie o tom, jaký druh intervence je nejúčinnější v určitých situacích.
- Navrhovat zásahy s ohledem na vnitřní pocity a postoje – princip, který by měl brát v úvahu, jak zásahy na zlepšení bezpečnostního chování ovlivňují psychologické stavy nebo vnímání lidí, jako je pocit svobody, důvěry nebo sounáležitosti. Zásahy by měly být navrženy tak, aby podporovaly pozitivní pocity a postoje, nikoli negativní nebo defenzivní reakce, které by mohly způsobit odpor nebo sabotáž. Zásahy by měly být hodnoceny nejen podle jejich dopadu na chování, ale také podle jejich dopadu na pocity a postoje, které lze zjistit prostřednictvím rozhovorů nebo dotazníků.

5.5.2 Shrnutí

Oproti výše zmíněným přístupům, které jsou zaměřeny převážně na příkazech a kontrole nebo vynucování bezpečnosti, je tento přístup založen primárně na chování zaměstnanců a počítá s nimi, jako se zdrojem rizika a s tím také pracuje. Pro aplikaci se používají výše zmíněné principy, které mohou zaměstnanci i zaměstnavatelé aplikovat a zvýšit tím bezpečnost podniku a samotných zaměstnanců.

5.6 Další přístupy

5.6.1 High-Reliability Organizations (HRO)

Přístup tzv. vysoce spolehlivá organizace[130] (HRO) zahrnuje organizace, které se zabývají činnostmi s vysokým rizikem, jako je letecká doprava, jaderná energetika nebo zdravotnictví, a přitom dosahují velmi nízké míry havárií a nehod. Tyto organizace se odlišují od ostatních tím, že mají specifické vlastnosti a praktiky, které jim umožňují efektivně zvládat rizika a předcházet nehodám.

HRO sdílí pět klíčových bodů[131], které jsou základem jejich spolehlivosti:

- Předvídání – znamená, že HRO aktivně vyhledávají a identifikují potenciální rizika a hrozby, a to i ty, které se zdají být nepravděpodobné nebo vzdálené.
- Odolnost – to znamená, že HRO jsou odolné vůči neočekávaným událostem a dokážou se rychle adaptovat na měnící se situaci.
- Učení se – tento bod naznačuje, že se HRO neustále učí z chyb a událostí, a to i těch nepatrných, a tyto poznatky aktivně využívají k prevenci budoucích incidentů.
- Flexibilita – tou se rozumí, že HRO jsou flexibilní a dokážou se rychle přizpůsobit novým informacím a měnícím se okolnostem.

[130] Veazie S, Peterson K, Bourne D. Evidence Brief: Implementation of High Reliability Organization Principles. Department of Veterans Affairs (US), Washington (DC); 2019. PMID: 31233295.

[131] Tamtéž

- Integrace – posledním bodem je integrace, tedy to, že se HRO vyznačují silnou firemní kulturou a sdílenými hodnotami, které podporují spolupráci a koordinaci mezi všemi členy organizace.

HRO se také řídí pěti základními principy[132], které jsou aplikací jejich charakteristik v praxi:

- První princip, který HRO využívá je předvídání. To znamená, že HRO věnují značné úsilí identifikaci a analýze potenciálních rizik. Využívají k tomu různé metody, jako je analýza minulých událostí, brainstorming a expertní posudky.
- Druhým principem je zabránění chybám, což znamená, že HRO se snaží předcházet chybám a incidentům hned na počátku. Toho dosahují prostřednictvím důkladného plánování, standardizace procesů a důkladného školení zaměstnanců.
- Třetím principem je robustnost, což znamená, že HRO se snaží budovat robustní systémy a procesy, které jsou odolné vůči neočekávaným událostem. To zahrnuje implementaci redundancí, zavádění bezpečnostních bariér a budování kultury odolnosti.
- Čtvrtým principem je učení se z chyb, což znamená, že HRO se neustále učí z chyb a incidentů. To zahrnuje důkladné vyšetřování událostí, identifikaci základních příčin a implementaci nápravných opatření.
- Pátým principem je adaptace a flexibilita, což znamená, že HRO se dokážou rychle adaptovat na měnící se situaci a reagovat na neočekávané události. Toho dosahují prostřednictvím decentralizovaného rozhodování, otevřené komunikace a silné kultury učení se.

Z výše popsaných principů a bodů lze dovodit, že HRO lze aplikovat v široké škále organizací, a to jak v soukromém, tak ve veřejném sektoru. Implementace těchto principů může vést k významnému zlepšení bezpečnosti a spolehlivosti organizace.

[132] Veazie S, Peterson K, Bourne D. Evidence Brief: Implementation of High Reliability Organization Principles. Department of Veterans Affairs (US), Washington (DC); 2019. PMID: 31233295.

5.6.2 Inherent Safety Design (ISD)

Inherent Safety Design[133] (ISD), volně přeložen do češtiny jako vlastní bezpečnostní plán, je proaktivní procesní přístup, který klade důraz na prevenci vzniku nebezpečí, místo toho, aby se spoléhal na dodatečné bezpečnostní systémy k jejich zmírnění.

ISD se opírá o pět[134] základních principů:

- Eliminace
- Náhrada
- Minimalizace
- Zmírnění
- Zjednodušení

ISD lze aplikovat[135] v různých oblastech především chemického průmyslu a procesního zpracovávání, jako jsou návrhy procesů, návrhy zařízení, výběr materiálů, provoz a údržba, skladování a manipulace s materiály.

Implementace ISD může přinést řadu výhod, jako je snížení rizika havárií, zvýšení bezpečnosti pracovníků, ochrana životního prostředí, snížení provozních nákladů a zvýšení produktivity.

5.6.3 Human Factors Engineering (HFE)

Ve volném překladu se jedná o inženýrství lidského faktoru[136]. Z názvu vyplývá, že se tento přístup zaměřuje na lidské tělo. V tomto smyslu lze tedy použít i slovo ergonomie. Z tohoto popisu lze dovodit, že se přístup HFE používá spíše jako doplnění ostatních přístupů.

HFE – ergonomie – se uplatňuje především v rámci BOZP a v interakci lidského těla se systémy a technologiemi, které jsou v podniku. Snaží se předcházet

[133] INHERENTLY SAFER DESIGN: THE FUNDAMENTALS. Online.Dostupné z: https://www.aiche.org/sites/default/files/cep/20120140-1.pdf. [cit. 2024-02-28].

[134] IChemE Safety Centre Guidance. Online. The Institution of Chemical Engineers. Dostupné z: https://www.icheme.org/media/14917/mb-0024_20-applying-process-safety-during-concept-select-phase-of-a-project-guidance.pdf. [cit. 2024-02-28].

[135] Tamtéž

[136]Human Factors Engineering. Online. Human Factors 101. Dostupné z: https://humanfactors101.com/topics/human-factors-engineering/. [cit. 2024-02-28].

rizikům a nehodám spojených[137] s manipulací břemen, únavou, stresem. Na základě těchto nežádoucích rizik se tento přístup snaží navrhnout taková pracoviště, aby se těmto rizikům předcházelo.

Mezi taková opatření[138] může patřit například:

- Omezení zvedání břemen
- Uspořádání pracoviště
- Osvětlením
- Eliminací hluku

Pokud se HFF implementuje správně, může se zamezit nebo snížit počet rizik na pracovišti, zvýšit výkonnost zaměstnanců, snížit náklady v souvislosti s nižší nehodovostí.

6 Přístupy v praxi

V této kapitole autor zaměřuje na samotné využívání jednotlivých přístupů v praxi. V první části uvede několik příkladů, kde se jaký přístup používá nejčastěji. Informace v této kapitole jsou získány jak z obecně dostupných zdrojů, jako je internet, tak ze zdrojů literatury a vědeckých článků, které byly použity v předchozích kapitolách zaměřených na popis jednotlivý přístupů.

Ve druhé části kapitoly se autor zaměří na vyhodnocení dotazníku, který byl rozeslán odpovědným osobám v oblasti bezpečnosti podniku v různých odvětvích.

Poslední část kapitoly se bude autor zabývat komparací mezi teoretickým a praktickým využitím jednotlivých přístupů na základě informací z první a druhé části této kapitoly.

6.1 Přístupy podle odvětví

V předchozí kapitole autor popsal, v čem spočívají jednotlivé přístupy. V této kapitole se zaměří na jejich využití v praxi. Vzhledem k informacím z předchozích přístupů se dá dovodit, že reaktivní a proaktivní přístup se odráží ve všech

[137] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.
[138] Tamtéž

ostatních přístupech a dá se tedy na základě těchto zjištění předpokládat, že jsou zcela univerzální a v podstatě základním stavebním kamenem, bez kterého by ostatní přístupy nemohly fungovat.

V praxi se lze nejčastěji setkat s těmito druhy přístupů především v oblasti krizového managementu[139] a IT bezpečnosti[140], kdy se i přes předem připravené scénáře a plány musí situace řešit reaktivně.

Na základě informací získaných při psaní předchozí kapitoly také vyplývá to, že v oblasti průmyslu se nejčastěji využívá systémový přístup. Ověřit to lze jednoduše tak, že většina velkých podniků má na svých veřejných webových stránkách certifikaci podle ISO, která se nejčastěji používá právě v systémovém přístupu a u velkých firem je to dnes nezbytností. Mezi tyto certifikace nejčastěji patří certifikace v oblasti BOZP – ISO 45001 a pak také oblasti řízení kvality – ISO 9001 a v neposlední řadě ISO 14001 – enviromentální management.

Jako příklad lze uvést tři největší české firmy:

- Škoda auto[141] – vlastní certifikáty ISO 9001, 14001, 45001, 50001 a 27001
- ČEZ[142] – vlastní opět certifikáty ISO 9001, 14001, 45001, 50001 a 27001
- AGROFERT[143] – stejná certifikace jako výše

6.2 Přístupy podle dotazníku

Na základě informací zjištěných z veřejných zdrojů se autor pokusil oslovit zhruba stovku firem a OZO v oblasti prevence rizik, aby si ověřil zjištěné údaje z teorie. Oslovení proběhlo jednoduchým dotazníkovým šetřením, vytvořeným pomocí Google formuláře, se dvěma otázkami.

[139] NEUGEBAUER, Tomáš. Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

[140]. Www.systemonline.cz. Online. Dostupné z: https://www.systemonline.cz/it-security/preventivni-vs.-reaktivni-pristup-k-bezpecnostnim-hrozbam.htm. [cit. 2024-02-28].

[141] Politika a certifikace společnosti. Online. Škoda Auto a.s. Dostupné z: https://www.skoda-auto.cz/o-spolecnosti/politika-certifikace. [cit. 2024-03-06].

[142] FG FORREST, a.s. Certifikace. Online. ČEZ Energetické služby. Dostupné z: http://www.cez.cz/cs/o-spolecnosti/certifikace. [cit. 2024-03-06].

[143]Certifikáty. Online. Agrofert. Dostupné z: https://www.agrofert.cz/. [cit. 2024-03-06].

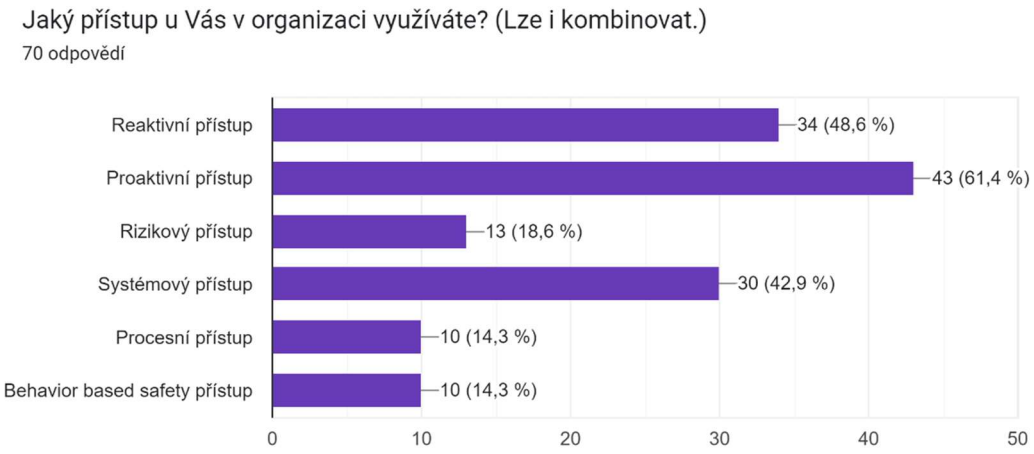
- První otázka byla zaměřená na odvětví, ve kterém dotázaní pracují:

Obrázek 3. Graf odvětví Zdroj: autor

Z grafu je zřejmé, že nejvíce dotázaných pracuje ve výrobním průmyslu, jak textilním, automobilovém tak dalších typech průmyslu 42,9 % (30 dotázaných). Následují je respondenti z bezpečnostních sborů 27,1 % (19 dotázaných). Třetí, nezanedbatelnou skupinou respondentů, je z oblasti veřejné správy a úřadů 11,4 % (8 dotázaných). Další z oblastí, které byly zahrnuty do průzkumu a bylo by vhodné je zmínit jsou odvětví IT (4 respondenti) a zdravotnictví (3 respondenti).

Celkově graf poskytuje zajímavý vhled do rozložení pracovních sil v České republice. Je ale důležité si uvědomit, že se jedná pouze o jeden průzkum složený z odpovědí pouze 70 respondentů a výsledky nemusí být zcela reprezentativní.

- Druhá otázka se zaměřila na jednotlivé přístupy:



Obrázek 4. Graf přístupů Zdroj: autor

Druhý graf navazuje na ten první a ukazuje, jaký přístup k bezpečnosti práce používají respondenti ve svých organizacích. Z grafu je zřejmé, že nejčastěji používaným přístupem je proaktivní přístup (61,4 %), následovaný reaktivním přístupem (48,6 %). Méně časté jsou pak systémový přístup (42,9 %), procesní přístup (14,3 %), Behavior based safety přístup (14,3 %) a rizikový přístup (18,6 %).

Z grafu je také zřejmé, že mnoho organizací používá kombinaci různých přístupů k bezpečnosti práce. Například 48,6 % respondentů uvedlo, že používají reaktivní přístup, ale zároveň 61,4 % respondentů uvedlo, že používají proaktivní přístup. To naznačuje, že mnoho podniků používá kombinaci obou přístupů, aby zajistily bezpečnost svých zaměstnanců.

6.3 Komparace přístupů

Na základě výše uvedených informací nelze jednoduše konstatovat, jaký je nejlepší přístup k danému podniku. Pokud se podíváme na dotazníkový průzkum je patrné, že většina podniků používá kombinaci různých přístupů k řízení bezpečnosti.

Pokud bychom je tedy chtěli komparovat, museli bychom si položit několik zásadních otázek. Především bychom museli jasně definovat cíle, kterých bychom chtěli dosáhnout – porovnat například proaktivní a reaktivní přístup v oblasti BOZP z hlediska jejich vlivu na míru nehodovosti v podniku. Zde bychom museli najít podniky, které používají výlučně jeden z těchto dvou přístupů, což na základě dotazníkového šetření bude obtížné a pravděpodobně to nebude mít vypovídající hodnotu.

Dále bychom museli shromáždit z těchto podniků dostatek dat, jako například míra nehodovosti, náklady na bezpečnost či zpětnou vazbu zaměstnanců. Na základě těchto dat vybrat vhodnou metodu buď kvalitativní nebo kvantitativní a výsledky zpracovat a interpretovat.

Kromě toho všeho je nutné komparovat podniky o stejné velikosti, typu a organizaci. Nelze porovnávat malou textilní firmu s velkým automobilovým průmyslem, nebo malého živnostníka s velkou firmou. Ideální by bylo porovnat středně velké podniky o zhruba 100 – 150 zaměstnancích a stejném zaměření,

například textilní výroba. Pouze pak by se dala komparace jednotlivých přístupů označit jako věrohodná a platná.

Mezi další otázky, které by bylo vhodné si položit při porovnání může být:

- Jaký přístup je efektivnější pro prevenci?
- Jaký přístup vede k vyšší spokojenosti zaměstnanců?
- Jaký přístup je ekonomicky výhodnější?

Na závěr autor vkládá tabulku, která, podle jeho subjektivního názoru, shrnuje jednotlivé přístupy z dotazníkového šetření:

Přístup	Cíle	Metody a nástroje	Výhody	Nevýhody
Proaktivní	Prevence vzniku rizik a nehod	Identifikace a hodnocení rizik, implementace preventivních opatření (školení, používání pomůcek, údržba), plánování a příprava na mimořádné události	Snižuje míru nehodovosti a náklady na bezpečnost	Vyžaduje čas, investice a zapojení všech
Reaktivní	Řešení rizik a nehod po jejich vzniku	Vyšetřování incidentů, poskytování první pomoci, nápravná opatření, sankce	Rychlá reakce na incidenty, učení se z chyb	Není preventivní, může vést k opakování incidentů
Systémový	Integrace prevence rizik do celkového systému řízení firmy	Zapojení všech zaměstnanců do bezpečnosti, monitorování a vyhodnocování efektivity bezpečnosti, průběžné zlepšování	Trvalá a efektivní prevence rizik, vysoká bezpečnostní kultura	Náročná na implementaci a udržení
Procesní	Zaměření na dodržování definovaných procesů a postupů	Standardizace pracovních postupů, dokumentace, audity	Zvyšuje kontrolu a snižuje variabilitu, usnadňuje dodržování předpisů	Může být rigidní a neflexibilní, omezuje autonomii
Behavior based safety	Zaměření na ovlivňování chování zaměstnanců	Pozorování a hodnocení chování, zpětná vazba, motivace, odměny	Změna chování a postojů k bezpečnosti, zvyšuje zodpovědnost	Vyžaduje trvalou podporu a motivaci
Rizikový	Akceptování rizik a jejich financování	Analýza rizik, analýza nákladů a benefitů	Minimalizace nákladů na bezpečnost	Není preventivní, může vést k závažným incidentům

Tabulka 1. Tabulka přístupů Zdroj: autor

7 Ověření hypotéz

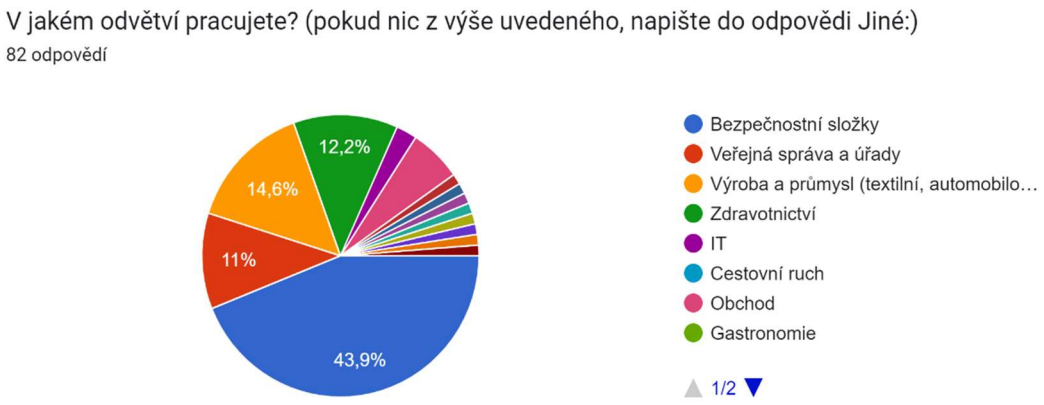
V poslední kapitole si na základě výsledků z dotazníkového šetření autor práce ověří, zda jsou výroky hypotéz stanovených na začátku této práce pravdivé, či nikoli, což bylo cílem této praktické části. Pro tento účel byl vytvořen dotazník a rozeslán napříč všemi okruhy zaměstnanců, přes různá diskusní fóra, různé Facebookové stránky a skupinové chaty, aby byli respondenti z rozličných zaměstnání.

7.1 Dotazník

Na dotazník odpovědělo celkem 84 respondentů, což není mnoho, vzhledem k tomu, kolikrát byl dotazník sdílen. Samotný dotazník je pak strukturovaný do tří základních bloků. První je demografický, kde jsou otázky zaměřené na věk, délku

pracovního poměru, pohlaví, rozhodovací pravomoci a v neposlední řadě odvětví, ve kterém respondent pracuje.

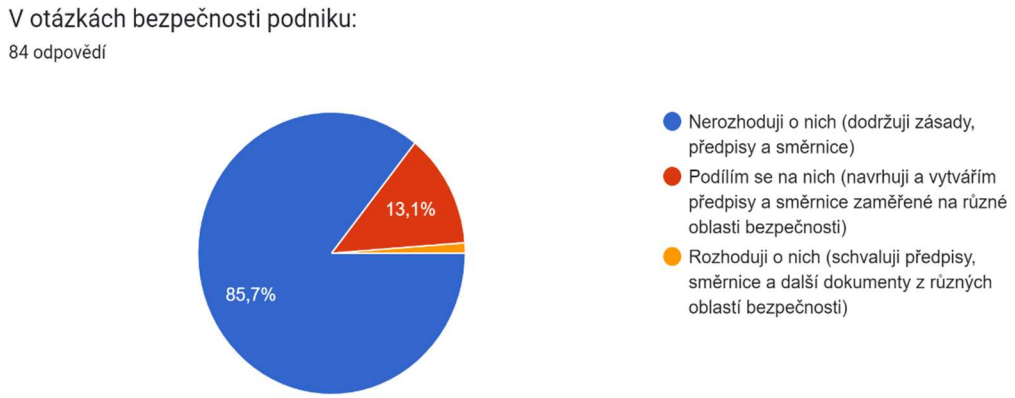
Z prvního celku lze zmínit složení respondentů, podle oblasti, ve které pracují.



Obrázek 5. Graf odvětví Zdroj: autor

Z grafu je patrné, že nejvíce respondentů je z bezpečnostních složek 43,9 % (36 dotázaných). Druhou, výrazně menší skupinou oproti první je skupina z oblasti průmyslu a výroby. Z té odpovědělo pouhých 14,6 % (12 respondentů). Z oblastí veřejné správy (9 respondentů) a zdravotnictví (10 respondentů) odpovídal zhruba stejný počet respondentů. Kromě odvětví, která jsou vidět v grafu odpovídali další respondenti například z oblasti stavebnictví, logistiky, školství, ministerstva obrany a další.

Druhou zajímavou otázkou z prvního bloku byla rozhodovací pravomoc v otázkách bezpečnosti podniku. Plnou rozhodovací pravomoc měl pouze jeden respondent. Dalších 11 respondentů se spolupodílí a zbytek respondentů jsou řadoví zaměstnanci, kteří budou mít nezaujatý pohled na zbylé otázky v dotazníku.



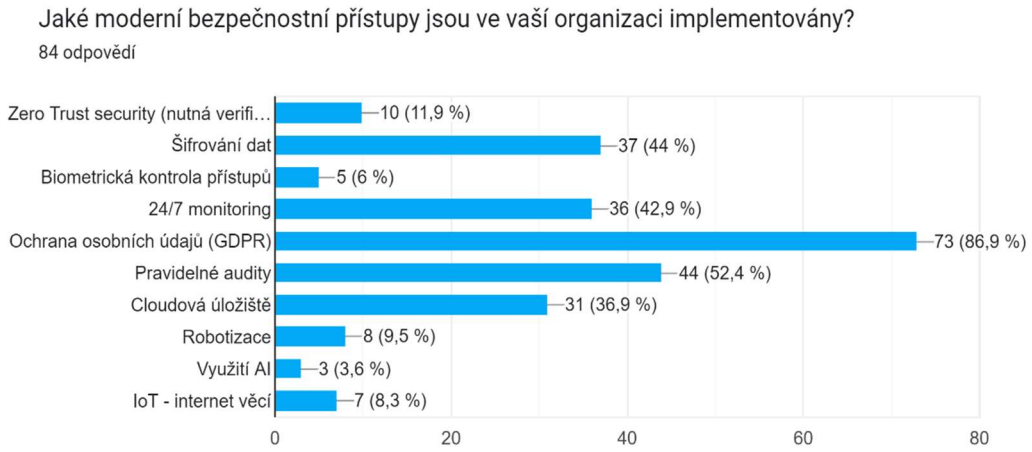
Obrázek 6. Graf rozhodovací pravomoc Zdroj: autor

7.2 Hypotéza č. 1

První hypotéza byla zaměřena na to, zda implementace nových bezpečnostních přístupů založených na nejnovějších trendech a inovacích v oblasti bezpečnosti podniku povede ke snížení počtu bezpečnostních událostí v organizaci.

V dotazníkovém šetření byl na ověření této hypotézy zaměřen druhý blok osmi otázek a respondenti mohli odpovídat z předem pečlivě vybraných možností sestavených na základě znalostí autora této práce v oblasti bezpečnosti.

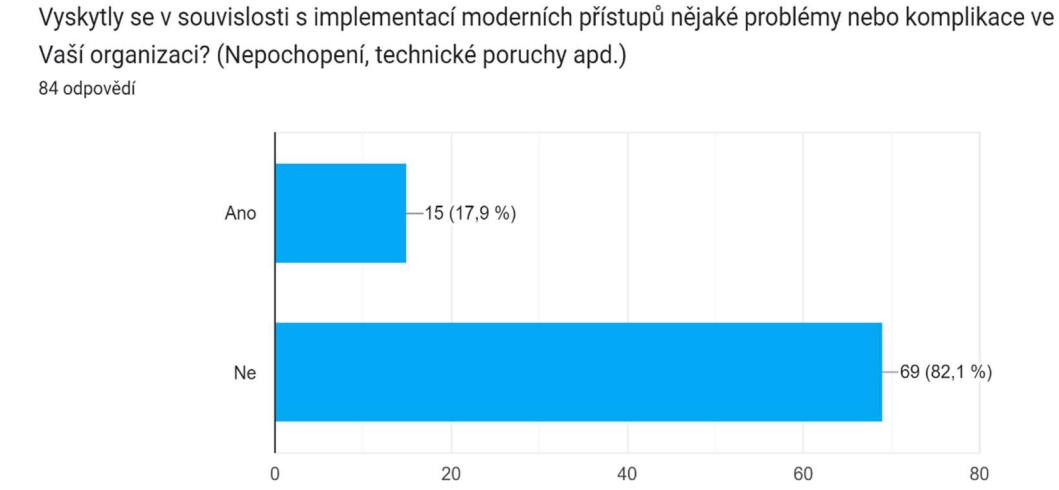
První otázka tohoto bloku byla zaměřená na to, jaké moderní bezpečnostní přístupy se v podnicích vůbec implementují. Z grafu níže je patrné, že nejvíce se organizace spoléhají na osvědčené bezpečnostní přístupy, jako je šifrování dat, monitoring a ochrana osobních údajů a pravidelné audity. Implementace novějších přístupů, jako je Zero Trust security, biometrie, AI nebo IoT je zatím méně rozšířená.



Obrázek 7. Graf moderních přístupů Zdroj: autor

Druhá otázka směřovala na to, jak sami respondenti hodnotí a znají tyto výše uvedené moderní přístupy a uplatňují je v praxi. Zde nejvíce respondentů hodnotilo tuto implementaci jako spíše pozitivně (37 respondentů) a 8 respondentů rozhodně pozitivně. Z toho lze vyvodit, že nadpoloviční většina respondentů má kladný vztah k moderním bezpečnostním přístupům, nebojí se inovací a využívají tyto metody v praxi.

Jako další se autor dotazoval na to, zda docházelo k nějakým problémům souvisejícím s implementací moderních přístupů.



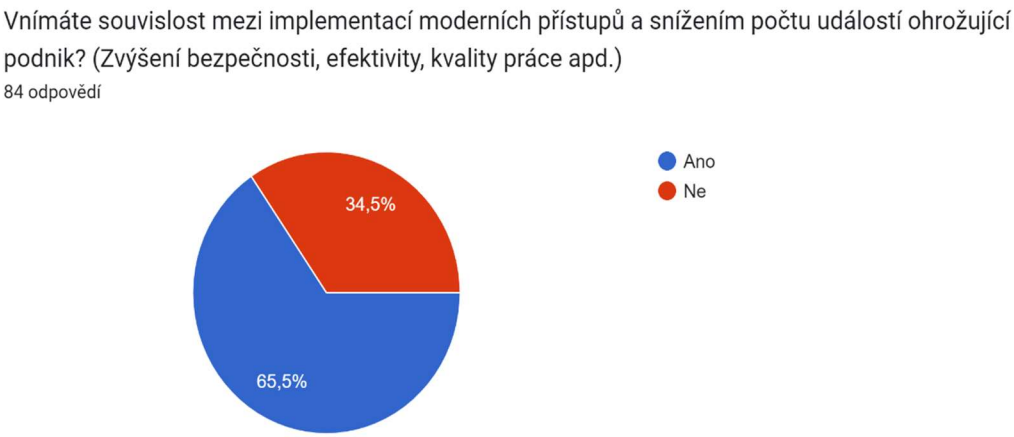
Obrázek 8. Graf implementace Zdroj: autor

Většina dotázaných odpověděla, že nenastaly žádné problémy. 15 respondentů ale uvedlo, že ano. Jako důvod, proč tomu tak bylo většina napsala technické potíže, jako nevyladěný systém, problémy s počítačem. Druhou velkou překážkou byl pak odmítavý postoj starších kolegů k moderním přístupům – odpověděli 4 respondenti.

Po těchto otázkách se autor již zaměřil na přímé potvrzení či vyvrácení hypotézy vyřčené na začátku. Směřovali na to tyto otázky:

- Jak vnímáte vliv moderních bezpečnostních přístupů na celkovou úroveň bezpečnosti ve Vaší organizaci?
- Myslíte si, že se díky implementaci moderních bezpečnostních přístupů zlepšila celková úroveň bezpečnosti Vaší organizace?
- Vnímáte souvislost mezi implementací moderních přístupů a snížením počtu událostí ohrožující podnik? (Zvýšení bezpečnosti, efektivity, kvality práce apd.)

Shrneme-li odpovědi z těchto otázek podle dotazníku, dojdeme k závěru, že většina respondentů vnímá vliv moderních bezpečnostních přístupů pozitivně, nebo velmi pozitivně (50 respondentů). Zhruba 57 % dotázaných si myslí, se zlepšila celková úroveň bezpečnosti organizace po implementaci moderních přístupů, pouze 2 respondenti si to nemyslí.



Obrázek 9. Souvislost implementace a počet incidentů Zdroj: autor

Na poslední otázku, zda vnímají respondenti souvislost mezi implementací moderních přístupů a snížením počtu incidentů uvedlo většina že ano – 65,5 %.

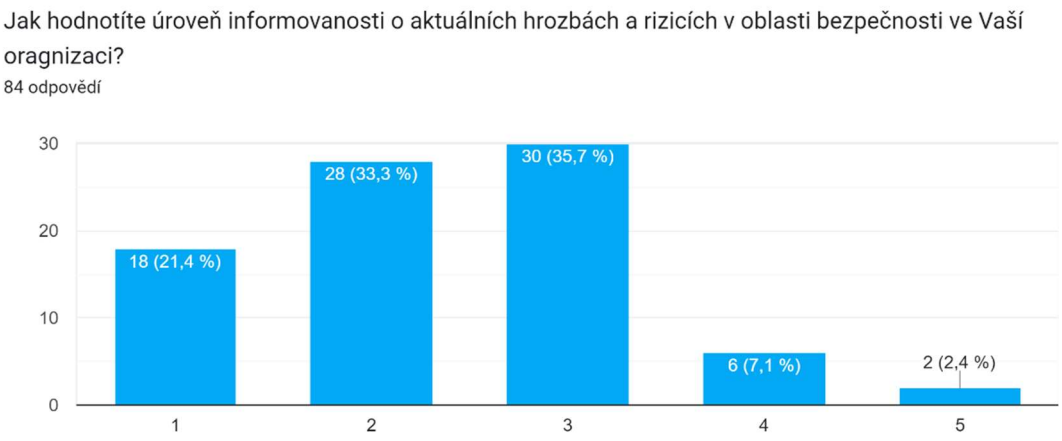
Dotazník se všemi otázkami je v příloze této práce. Tabulky s výsledky jsou na přiloženém CD této práce.

Pokud se tedy vrátíme k hypotéze č. 1, tak na základě analýzy dat a informací lze konstatovat, že existuje silná souvislost mezi implementací moderních bezpečnostních přístupů a snížením počtu bezpečnostních událostí v organizaci a lze tedy s jistou mírou jistoty **potvrdit hypotézu**, že implementace moderních bezpečnostních přístupů povede ke snížení počtu bezpečnostních událostí v organizaci. I když existují určité výzvy spojené s implementací moderních přístupů, jejich přínosy v podobě snížení rizika a včasné detekce hrozeb jsou značné.

7.3 Hypotéza 2

Druhá hypotéza byla zaměřena na to, zda je vztah mezi efektivitou stávajících bezpečnostních přístupů v organizaci přímo úměrný s úrovní vědomí a školení zaměstnanců v oblasti bezpečnosti.

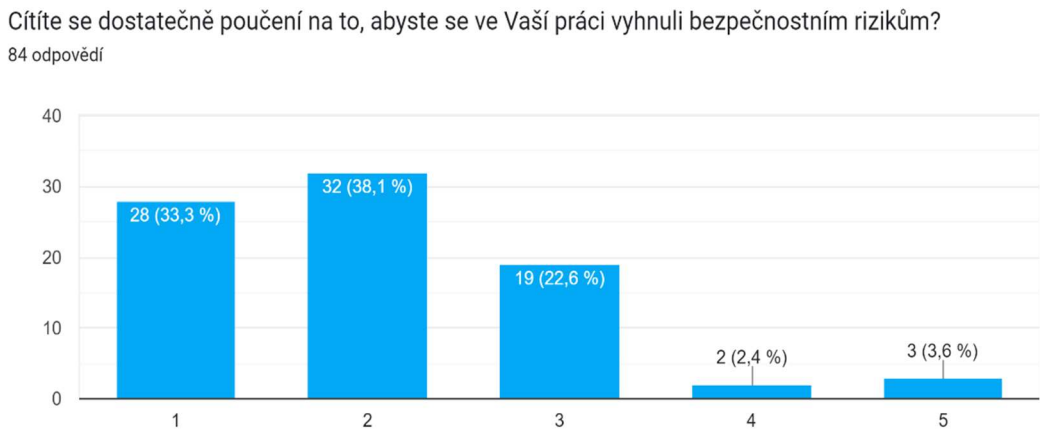
Této problematice se věnoval třetí blok deseti otázek v dotazníkovém šetření a respondenti opět volili z předem připravených odpovědí. Kromě otázek primárně zaměřených na potvrzení či vyvrácení hypotézy se autor zajímal také o to, jak jsou zaměstnanci podniků informování o hrozbách a rizicích.



Obrázek 10. Graf informovanosti Zdroj: autor

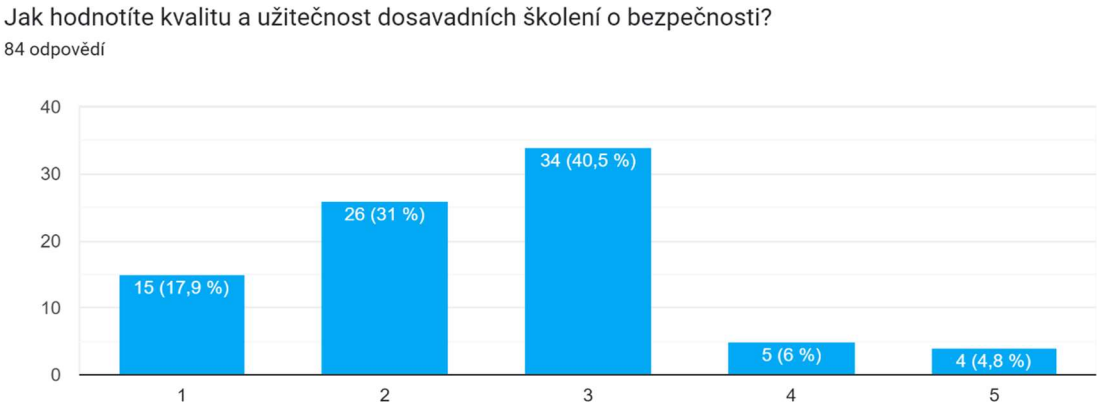
Nadpoloviční většina uvedla spíše pozitivní či neutrální vztah v této otázce, což může znamenat, že by se podniky měly více zabývat informováním svých zaměstnanců na možných hrozbách a rizicích.

I přes to však většina respondentů uvedla, že se cítí být dostatečně poučena na to, aby se vyhnula rizikům a hrozbám, které ohrožují jejich organizaci.



Obrázek 11. Graf vyhnutí se rizikům Zdroj: autor

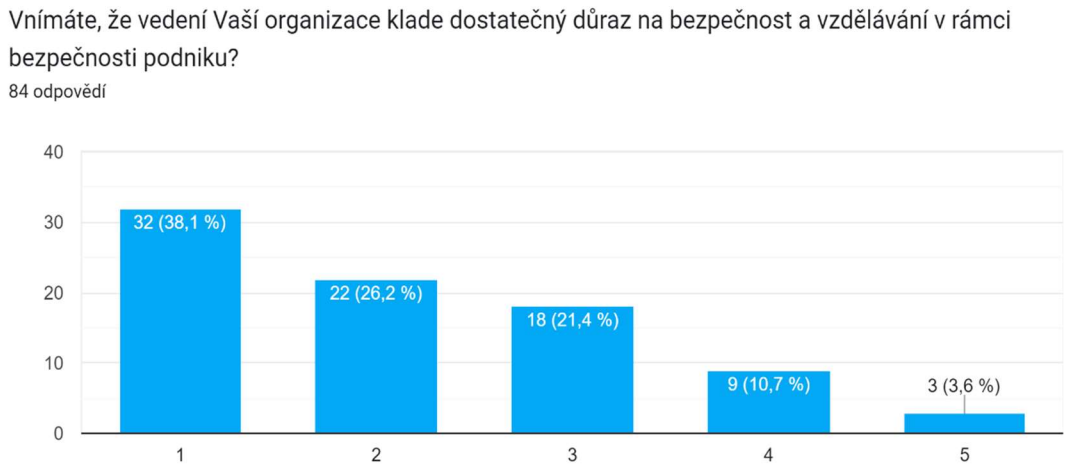
Dále se autor zaměřil na míru četnost a užitečnost školení. Téměř polovina respondentů uvedla, že absolvuje pouze jedno školení ročně (43 respondentů), dalších 29 respondentů uvedlo, že má několik školení ročně. Zbytek respondentů, celkem 1, nemá školení žádná. Ti mohou být pravděpodobně ze skupiny studentů škol.



Obrázek 12. Kvalita a užitečnost školení Zdroj: autor

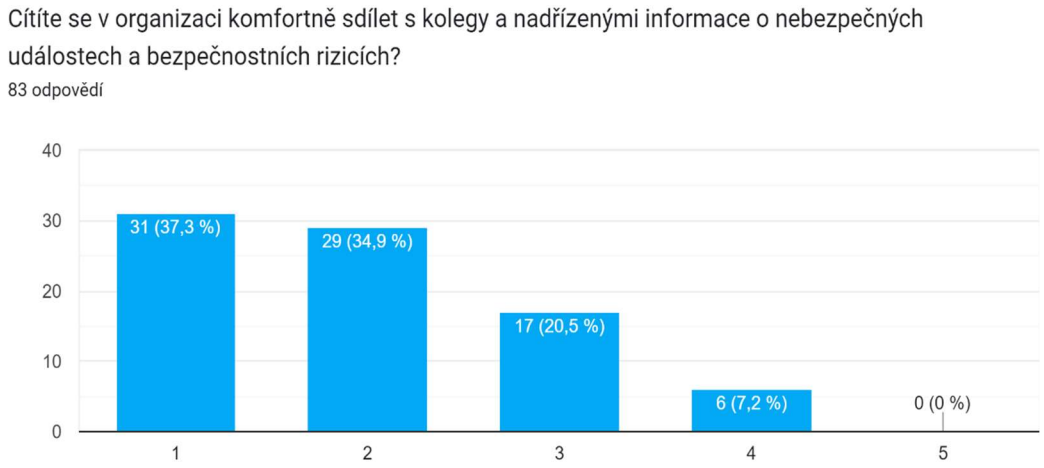
Co se týče kvality a užitečnosti školení, tak velká většina respondentů (43,9 %) hodnotí kvalitu a užitečnost školení o bezpečnosti alespoň jako velmi nebo spíše pozitivní. To naznačuje, že školení je efektivní při zvyšování povědomí o bezpečnosti u zaměstnanců. Dalších 40,5 % respondentů není zcela přesvědčena o kvalitě a užitečnosti, ale nevnímají tato školení negativně. Zbylí respondenti vnímají školení a jeho užitečnost negativně.

Další z důležitých otázek k ověření této hypotézy byla ta, zda samotná organizace klade důraz na bezpečnost a školení v rámci bezpečnosti podniku. Většina respondentů (64,3 %) vnímá, že vedení klade dostatečný nebo spíše dostatečný důraz na bezpečnost a vzdělávání v rámci podniku. Z toho lze odvodit, že organizace investuje do zvyšování povědomí o bezpečnosti u zaměstnanců.



Obrázek 13. Důraz na vzdělávání Zdroj: autor

Poslední otázka, k ověření hypotézy, byla zaměřena na sdílení bezpečnostních informací s kolegy a nadřízenými. Většina respondentů (72,2 %) se cítí komfortně nebo spíše komfortně při sdílení informací o nebezpečných událostech a bezpečnostních rizicích s kolegy a nadřízenými. To naznačuje, že v organizacích existuje jakási kultura sdílení informací a zodpovědnosti za bezpečnost, která je podpořena školeními a povědomím o možných rizicích a hrozbách.



Obrázek 14. Sdílení informací Zdroj: autor

Na základě dostupných informací z dotazníkového šetření můžeme s jistotou říct, že existuje přímá úměrnost mezi efektivitou stávajících bezpečnostních přístupů v organizaci a úrovní vědomí a školení zaměstnanců v oblasti bezpečnosti a lze tedy tuto **hypotézu potvrdit**. To znamená, že čím vyšší je úroveň vědomí zaměstnanců a školení, tím efektivnější jsou bezpečnostní přístupy v organizaci.

Závěr

V průběhu této diplomové práce jsem se věnoval důkladnému zkoumání a analýze řízení bezpečnosti podniku, což je, podle mého názoru, téma stále získávající na významu v rámci moderního podnikání. Řízení bezpečnosti podniku se ukázalo jako nezbytné pro ochranu nejen zaměstnanců a zákazníků, ale i samotného majetku podniku v různých oblastech bezpečnosti.

Práce byla strukturována do několika kapitol, které pokrývaly širokou škálu témat od teorie bezpečnostního managementu, přes popis jednotlivých přístupů, až po ověření hypotéz pomocí dotazníkového šetření.

Cílem této práce bylo vytvořit komplexní příručku na téma řízení bezpečnosti podniku, která by sloužila jako ucelený průvodce pro začínající managery, nebo pro podniky, které by se chtěli více zaměřit na svou bezpečnost. Myslím si, že tento cíl byl naplněn. Příručka, kterou práce představuje, obsahuje nejen

teoretické koncepty, ale také současné přístupy, které jsou nezbytné pro efektivní řízení bezpečnosti podniku.

V průběhu práce také byly ověřeny dvě hypotézy. První hypotéza, která předpokládala, že implementace moderních bezpečnostních přístupů povede ke snížení počtu bezpečnostních událostí, byla potvrzena. Analýza dotazníkového šetření ukázala, že existuje silná souvislost mezi implementací moderních bezpečnostních přístupů a snížením počtu bezpečnostních událostí v organizaci.

Druhá hypotéza, která tvrdila, že existuje přímá úměrnost mezi efektivitou stávajících bezpečnostních přístupů a úrovní vědomí a školení zaměstnanců, byla také potvrzena. To znamená, že čím vyšší je úroveň vědomí zaměstnanců a školení, tím efektivnější jsou bezpečnostní přístupy v organizaci.

Nicméně, práce také odhalila určitá omezení. Přestože se podařilo částečně určit, jaké přístupy se v praxi využívají nejčastěji, nepodařilo se komparovat tyto přístupy mezi sebou. Na základě dostupných dat nelze jednoduše konstatovat, jaký je nejlepší přístup k danému podniku. Výsledky dotazníkového průzkumu naznačují, že většina podniků používá kombinaci různých přístupů, což komplikuje možnost jednoznačné komparace.

Dalším omezením byl počet respondentů. S pouhými 84 respondenty je obtížné považovat výsledky za reprezentativní. Přesto se podařilo potvrdit obě hypotézy, což je pozitivním výsledkem. V budoucích výzkumech by bylo vhodné zvýšit počet respondentů a zaměřit se na specifičtější segmenty podniků, aby bylo možné provést důkladnější komparaci přístupů.

Dovoluji si tvrdit, že práce přináší cenný přehled o řízení bezpečnosti podniku a jeho významu v dnešním podnikatelském prostředí. Představuje užitečný zdroj informací pro podniky, které by se mohly snažit zlepšit svou bezpečnost, a poskytuje pevný základ pro další výzkum v této oblasti. Práce také poukazuje na potřebu dalšího výzkumu, zejména v oblasti komparace bezpečnostních přístupů a jejich efektivity v různých typech podniků.

Je zřejmé, že bezpečnostní management je dynamický a vyvíjející se obor, který vyžaduje neustálé sledování trendů a inovací, aby bylo možné efektivně reagovat na nové výzvy a hrozby. V této práci jsem také ověřil, že oblast

bezpečnostního managementu není jen statický proces, ale neustálý cyklus hodnocení, plánování, implementace a revizí.

Efektivní bezpečnost podniku vyžaduje nejen znalost teorie, ale také schopnost adaptace a aplikování těchto konceptů v praxi. Význam školení a vzdělávání zaměstnanců v oblasti bezpečnosti je nezpochybnitelný, stejně jako potřeba integrace bezpečnostních opatření do každodenního provozu podniku. Vzhledem k potvrzení obou hypotéz je zřejmé, že moderní přístupy k bezpečnosti a vzdělávání zaměstnanců jsou klíčové pro snížení počtu bezpečnostních událostí a zvýšení efektivity bezpečnostních opatření.

Myslím si, že tato zjištění poskytují solidní základ pro další výzkum a rozvoj v oblasti řízení bezpečnosti podniku a mohou sloužit jako vodítko pro podniky, které se snaží zlepšit svou bezpečnost. Výsledky této práce jsou relevantní nejen pro akademickou komunitu, ale také pro praktiky v oblasti řízení bezpečnosti podniku – odborně způsobilé osoby nebo vedoucí pracovníky, kteří mají zodpovědnost za bezpečnost.

Zjištění také poskytují užitečný přehled o stávajících přístupech a metodách a zdůrazňují důležitost pokračujícího vzdělávání a adaptace na nové bezpečnostní výzvy. Práce také poukazuje na potřebu dalšího výzkumu, který by se zaměřil na specifičtější aspekty řízení bezpečnosti a na vývoj nových nástrojů a strategií, které by pomohly podnikům lépe chránit své zaměstnance, zákazníky a majetek.

Použitá literatura a zdroje

Monografie

NEUGEBAUER, Tomáš. *Bezpečnost a ochrana zdraví při práci v kostce, neboli, O čem je současná BOZP*. 2., aktualizované a rozšířené vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-106-1.

NEUGEBAUER, Tomáš. *Školení bezpečnosti práce, požární ochrany a motivační školení k prevenci rizik. 2. vydání*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-957-2.

LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. Zlín: Radim Bačuvčík - VeRBuM, 2015, ISBN 978-808-7500-057.

LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-808-7500-194.

LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-35-4.

LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-808-7500-576.

LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík - VeRBuM, 2015, ISBN 978-808-7500-675.

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

TILHON, Jiří; SKŘEHOT, Petr a VALA, Jiří. *Komentované vydání ČSN ISO 45001: systémy managementu bezpečnosti a ochrany zdraví při práci: požadavky s návodem k použití*. Praha: Česká společnost pro jakost. ISBN 978-80-02-02840-6.

IVANKA, Ján. *Mechanické zábranné systémy*. Online. Druhé. Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-427-9.

HARTL, Jan. *Poplachové zabezpečovací a tísňové systémy*. Online. Česká zemědělská univerzita v Praze - Technická fakulta. ISBN 978-80-213-2962-1.

UHLÁŘ, Jan. *Technická ochrana objektů I. Díl: Mechanické zábranné systémy II*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-807-2513-123.

UHLÁŘ, Jan. *Technická ochrana objektů II. Díl: Elektrické zabezpečovací systémy II*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 9788072513130.

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity. Online*. 1. CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8.

DAŇOVÁ, Monika a Jaroslav GONOS. *VYBRANÉ ASPEKTY KVANTIFIKÁCIE EKONOMICKEJ BEZPEČNOSTI*. Prešovská univerzita v Prešově: Prešovská univerzita v Prešově, 2016. ISBN 978-80-555-1619-6.

BRABEC, František, Ivo LÁTAL, Rudolf MUSIL, Ivan PILNÝ, Miloš URBAN a Tomáš VEJLUPEK. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-864-4504-6.

LÁTAL, Ivo. *Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací*. Praha: Prospektrum, 2001. ISBN 80-717-5091-3.

KOVAŘÍKOVÁ, M. 2015. *Prevence ozbrojených útoků na školách jako součást didaktiky mimořádných situací*. Lifelong Learning – celoživotní vzdělávání, roč. 5, č. 3, s. 95-112. ISSN 1804-526X.

DVOŘÁKOVÁ, Zuzana; IĽKO, Michael Dezider. *Nové technologie v BOZP. Časopis výzkumu a aplikací v profesionální bezpečnosti* [online]. 2019, roč. 12, speciální č. Nové trendy v BOZP 2019. ISSN 1803-3687.

VALA, Jiří. 100 let BOZP 1918 - 2018. 1. vyd. Výzkumný ústav bezpečnosti práce, 2018. 31s.

JANÁKOVÁ, Anna. Abeceda bezpečnosti a ochrany zdraví při práci. Práce, mzdy, pojištění. [1999]-. Olomouc: ANAG, [1999].

KUČÁKOVÁ, Adriana. Systémová bezpečnost organizace. Bakalářská práce. Praha: Policejní akademie České Republiky v Praze, 2023.

HUNZIKER, Stefan. Enterprise *Risk Management. Online*. Wiesbaden: Springer Fachmedien Wiesbaden, 2021. ISBN 978-3-658-33522-9.

SNYDER, Paul a ULLRICH, Gary. *Practical Safety Management Systems*. Online. 2. Newcastle, Wahsington: Aviation Supplies & Academics, 2019. ISBN 978-1-61954-887-9.

OLSON, David L. a WU, Desheng Dash. *Enterprise Risk Management Models*. Online. Springer Texts in Business and Economics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017. ISBN 978-3-662-53784-8.

SHUMILO, Olha; BABENKO, Vitalina; LIUBOKHYNETS, Larysa; VOLOVELSKA, Iryna a AREFIEVA, Olena. *Method of Enterprise Economic Security Evaluation*. Online. Studies of Applied Economics. 2021, roč. 39, č. 7. ISSN 1697-5731.

ABANINA, E N, Yu S SERGEENKO, O V DEVYATOV, O YU GANYUKHINA a Yu M NIKITENKO. *The Structure of Training Program and Advanced Training of Enterprise Managers in Order to Ensure Environmental Safety*. IOP Conference Series: Materials Science and Engineering [online]. 2019, 2019-09-01, 582(1). ISSN 1757-8981.

GELLER, E. Scott. *Behavior-Based Safety and Occupational Risk Management*. Online. Behavior Modification. 2005, roč. 29, č. 3, s. 539-561. ISSN 0145-4455.

Veazie S, Peterson K, Bourne D. *Evidence Brief: Implementation of High Reliability Organization Principles*. Department of Veterans Affairs (US), Washington (DC); 2019. PMID: 31233295.

Hillnhagen, Simon & Mütze, Alexander & Nyhuis, Peter & Schmidt, Matthias. (2024). *Influence of ISO 9001 on the configuration of production planning and control*. Procedia CIRP. 120. 10.1016/j.procir.2023.09.165.

Hidayati, Ruti & SODIKIN, SODIKIN. (2023). *Benefit analysis of the implementation of Environmental Management System (EMS) ISO 14001:2015 in a tyres industry*. Indonesian Journal of Applied Environmental Studies. 4. 77-84. 10.33751/injast.v4i2.8897.

Bochkovskyi, A.. (2020). *Improvement of risk management principles in occupational health and safety*. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 94-104. 10.33271/nvngu/2020-4/094.

Rasmussen, L. B. (2010). From reactive to proactive approach of interactive leadership. In The Ambivalent Character of Participation: New Tendencies in Worker Participation in Europe (1. ed., Vol. 20, pp. 585-612). Peter Lang.

Zákonná úprava a interní akty řízení

Zákon č. 250/2021 Sb. Zákon o bezpečnosti práce v souvislosti s provozem vyhrazených technických zařízení

Zákon č. 262/2006 Sb. Zákon zákoník práce

Zákon č. 309/2006 Sb. Zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci

Zákon č. 133/1985 Sb. Zákon České národní rady o požární ochraně

Zákon č. 17/1992 Sb. Zákon o životním prostředí

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v posledním znění

Nařízení vlády č. 194/2022 Sb. Nařízení vlády o požadavcích na odbornou způsobilost k výkonu činnosti na elektrických zařízeních a na odbornou způsobilost v elektrotechnice

Nařízení vlády č. 190/2022 Sb. Nařízení vlády o vyhrazených technických elektrických zařízeních a požadavcích na zajištění jejich bezpečnosti

ČSN EN ISO 9001 Systémy managementu kvality

ČSN EN ISO 14001 Systémy environmentálního managementu

ČSN EN ISO 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí

ČSN EN ISO 45001 Systémy managementu bezpečnosti a ochrany zdraví při práci

ČSN ISO 31000 Management rizik

Webové stránky a elektronické zdroje

Přispěvatelé Encyklopedie BOZP, *Bezpečnostní management* [online], c2019, Datum poslední revize 11. 06. 2019, 08:50 UTC, [citováno 23. 10. 2023] https://ebozp.vubp.cz/wiki/index.php?title=Bezpe%C4%8Dnostn%C3%AD_management&oldid=23175

10 THINGS YOU SHOULD KNOW ABOUT SAFETY MANAGEMENT SYSTEMS (SMS). Online. In: The International Civil Aviation Organization. Dostupné z: https://www4.icao.int/demo/SMI/10_things.pdf

WIKIPEDIE, Přispěvatelé. Informační bezpečnost. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: Informační bezpečnost

Přispěvatelé Encyklopedie BOZP, Psychická bezpečnost práce [online], , c2021, Datum poslední revize 5. 03. 2021, 08:28 UTC, [citováno 4. 03. 2024] Psychická bezpečnost

AITOM. Elektronické zabezpečovací systémy. Online. Dodáváme zabezpečovací systémy! Dostupné z: https://www.elkov.cz/sluzby-poradenstvi-a-navrhy-elektronicke-zabezpecovaci-systemy-ezs/

ŠTĚPÁNOVÁ, Martina. Ekonomická bezpečnost vybraného podniku. Vedoucí Hoke, Eva. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení, 2018. Dostupné také z: http://hdl.handle.net/10563/43062.

KUDLOVÁ, Dagmar. Prostředí v managementu. Online, Učební materiál. Informační systém Masarykovy univerzity: Masarykova univerzita, 2005. Dostupné z: https://is.muni.cz/el/1451/jaro2005/t192/um/Prostredi_managementu.pdf

IDNES. Za požár liberecké Severochemy obvinili dělníka, stáčel načerno chemikálii. MAFRA A. S. IDnes [online]. 2017 [cit. 2024-02-07]. Dostupné z: https://www.idnes.cz/liberec/zpravy/severochema-liberec-pozar-obvineni-policie-cr-hasici.A190321_202010_liberec-zpravy_rko

Pre-employment background screening | Práce a mzda. Hlavní strana | Práce a mzda [online]. Copyright © 2023 Wolters [cit. 07.02.2024]. Dostupné z: https://www.praceamzda.cz/clanky/pre-employment-background-screening#footnote1

Inspektoři Čižp uložili masokombinátu pokutu přes milion korun za spáchání několika správních deliktů." Čižp, online, https://www.cizp.cz/aktuality/inspektori-cizp-ulozili-masokombinatu-pokutu-pres-milion-korun-za-spachani-nekolika

TA-SEEN, Junaid. ISO 27001: Information Security Management Systems. Online. In: . Dostupné z: https://doi.org/10.13140/RG.2.2.36267.52005

NOVÁK, Luděk a POŽÁR, Josef. Systém řízení informační bezpečnosti. Online. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

CONSTANTINE, Alister. ISO 45001:2018 OCCUPATIONAL HEALTH & SAFETY IMPLEMENTATION GUIDE [online]. In: . 1. NQA, 2018, s. 35. Dostupné z: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-45001-Implementation-Guide.pdf

Metody a způsoby hodnocení rizik na pracovišti. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

Analýza a řízení rizik BOZP. Identifikace, hodnocení a management ve firmách a jiných organizacích. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/analyza-rizik-bozp-rizeni-hodnoceni-identifikace-management/

WIKIPEDIE, Přispěvatelé. Brainstorming. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: https://cs.wikipedia.org/wiki/Brainstorming

WIKIPEDIE, Přispěvatelé. Dotazníkové šetření. Online. In: Wikipedie: Otevřená encyklopedie. Dostupné z: Dotazníkové šetření

HÁJKOVÁ, Martina. Identifikace nebezpečí a hodnocení rizik - metody. Online. BOZPinfo.cz. Dostupné z: https://www.bozpinfo.cz/identifikace-nebezpeci-hodnoceni-rizik-metody

Polokvantitativní metoda – parametr "pravděpodobnost ohrožení". Online. Parametr "pravděpodobnost ohrožení" | BOZPinfo.cz. Dostupné z:

https://www.bozpinfo.cz/polokvantitativni-metoda-parametr-pravdepodobnost-ohrozeni

JIŘINKA. Současný charakter vykonávané. Online. Znalostní systém prevence rizik v BOZP. Dostupné z: https://zsbozp.vubp.cz/metody-hodnoceni-rizik

Jaké jsou povinnosti na úseku zajištění požární ochrany? Zde je základní přehled. Online. BOZP.cz. Dostupné z: https://www.dokumentacebozp.cz/aktuality/jake-jsou-povinnosti-na-useku-zajisteni-pozarni-ochrany/

Audit bezpečnosti práce (BOZP). Příprava, postupy a tipy pro realizaci. Online. Dostupné z: https://www.bozp.cz/aktuality/audit-bezpecnosti-prace

Amanipour, Soheil & Klaus, Hubert. (2024). (PDF) Security Auditing and Monitoring: Incident response and management. Online. ResearchGate. Dostupné z: https://www.researchgate.net/publication/377358100_Security_Auditing_and_Monitoring_Incident_response_and_management

DASHÖFER, Verlag. Význam procesu vyšetřování incidentů. Online. Články na témata bezpečnost práce, Legislativa a komentáře, Poradna BOZP, Ochrana zdraví při práci, Prevence rizik, Technicko-bezpečnostní rozbory činností, Školení a vzdělávání BOZP, Vzorová dokumentace BOZP. Dostupné z: https://www.bozpprofi.cz/33/vyznam-procesu-vysetrovani-incidentu-uniqueidgOkE4NvrWuOKaQDKuox_Z6AjhnlZCh84IJR9Hs5aM2Y/

The Difference Between Reactive and Proactive Health. Online. Dostupné z: https://www.evotix.com/resources/blog/the-difference-between-reactive-and-proactive-health-safety-management

Proactive Vs Reactive Health And Safety Management. Online. HASpod. Dostupné z: https://www.haspod.com/blog/management/proactive-reactive-health-safety-management

What Is Proactive Risk Management? Online. RiskOptics. Dostupné z: https://reciprocity.com/resources/what-is-proactive-risk-management/

DUDEK, Martin. Procesní přístup. Online. Kvalita jednoduše - Zaměřeno na management kvality. Dostupné z: https://kvalita-jednoduse.cz/procesni-pristup/

Procesní přístup v ISO 9001:2015. Online. Česká společnost pro jakost. Dostupné z: https://www.csq.cz/fileadmin/user_upload/ISO9001_2015_Guidance_on_the_Process_Approach_CZ.pdf

Behavior Based Safety. Online. SafetyCulture. Dostupné z: https://safetyculture.com/topics/behavior-based-safety/

INHERENTLY SAFER DESIGN: THE FUNDAMENTALS. Online.Dostupné z: https://www.aiche.org/sites/default/files/cep/20120140-1.pdf

IChemE Safety Centre Guidance. Online. The Institution of Chemical Engineers. Dostupné z: https://www.icheme.org/media/14917/mb-0024_20-applying-process-safety-during-concept-select-phase-of-a-project-guidance.pdf

Human Factors Engineering. Online. Human Factors 101. Dostupné z: https://humanfactors101.com/topics/human-factors-engineering/

Www.systemonline.cz. Online. Dostupné z: https://www.systemonline.cz/it-security/preventivni-vs.-reaktivni-pristup-k-bezpecnostnim-hrozbam.htm

Politika a certifikace společnosti. Online. Škoda Auto a.s. Dostupné z: https://www.skoda-auto.cz/o-spolecnosti/politika-certifikace

FG FORREST, a.s. Certifikace. Online. ČEZ Energetické služby. Dostupné z: http://www.cez.cz/cs/o-spolecnosti/certifikace

Certifikáty. Online. Agrofert. Dostupné z: https://www.agrofert.cz/

Seznam obrázků

Seznam tabulek

Seznam zkratek

BOZP	Bezpečnost a ochrana zdraví při práce
BM	Bezpečnostní management
ISO	Mezinárodní organizace pro normalizaci
OHSAS	Série hodnocení bezpečnosti a ochrany zdraví při práci
IoT	internet věcí
MZS	Mechanické zábranné systémy
PZTS	Poplachové zabezpečovací a tísňové systémy
EZS	Elektronické zabezpečovací systémy
GSM	Globální standard pro digitální mobilní sítě
PIR	Pasivní infračervený senzor
VTZ	Vyhrazená technická zařízení
PO	Požární ochrana
OZO	Odborně způsobilá osoba
ČOV	Čistička odpadních vod
ISMS	Informační bezpečnostní management systém
QMS	Systém managementu kvality
EMS	Systém enviromentálního managementu
CLP	Klasifikace, označování a balení látek a směsí
ČSN	České technické normy
FTA	Strom poruch
ETA	Strom událostí
SWOT	Metoda silné, slabé stránky, příležitosti a hrozby
QRA	Kvantitativní analýza rizik
OOPP	Osobní ochranné pracovní pomůcky

SMS	Systém řízení bezpečnosti
BBS	Přístup založený na chování zaměstnanců
DO IT	Definuj, pozoruj, zasáhni, testuj
HRO	Přístup vysoce spolehlivé organizace
ISD	Přístup vlastního bezpečnostního plánování
HFE	Přístup pracující s ergonomií člověka

Přílohy

Příloha A – dotazník Vnímání bezpečnosti

Vaše pohlaví? *

- ○ Žena
- ○ Muž

Váš věk? *

- ○ Pod 18 let
- ○ 18 - 25
- ○ 25 - 45
- ○ 45 a více

Délka působení v podniku? *

- ○ Méně než 1 rok
- ○ 1 - 5 let
- ○ 5 - 15 let
- ○ 15 let a více

V otázkách bezpečnosti podniku: *

- ○ Nerozhoduji o nich (dodržuji zásady, předpisy a směrnice)
- ○ Podílím se na nich (navrhuji a vytvářím předpisy a směrnice zaměřené na různé oblasti bezpečnosti)
- ○ Rozhoduji o nich (schvaluji předpisy, směrnice a další dokumenty z různých oblastí bezpečnosti)

V jakém odvětví pracujete? (pokud nic z výše uvedeného, napište do odpovědi Jiné:) *

- ○ Bezpečnostní složky
- ○ Veřejná správa a úřady
- ○ Výroba a průmysl (textilní, automobilový aj.)
- ○ Zdravotnictví
- ○ IT
- ○ Cestovní ruch
- ○ Obchod
- ○ Gastronomie
- ○ Jiná...

Jaké moderní bezpečnostní přístupy jsou ve vaší organizaci implementovány? *

- ☐ Zero Trust security (nutná verifikace každého kroku)
- ☐ Šifrování dat
- ☐ Biometrická kontrola přístupů
- ☐ 24/7 monitoring
- ☐ Ochrana osobních údajů (GDPR)
- ☐ Pravidelné audity
- ☐ Cloudová úložiště
- ☐ Robotizace
- ☐ Využití AI
- ☐ IoT - internet věcí
- ☐ Jiná...

Jak hodnotíte úroveň znalostí a pochopení těchto moderních přístupů jako zaměstnanec? (například Vaše uplatnění nových přístupů v praxi) *

	1	2	3	4	5	
Velmi pozitivně	○	○	○	○	○	Velmi negativně

Probíhají ve Vaší organizaci pravidelná školení o používání moderních bezpečnostních nástrojů a technologií? (Využití AI, ovládání robotů apd.) *

- ○ Ano
- ○ Ne

Vyskytly se v souvislosti s implementací moderních přístupů nějaké problémy nebo komplikace ve Vaší organizaci? (Nepochopení, technické poruchy apd.) *

- ☐ Ano
- ☐ Ne

Pokud jste v předchozí odpovědi uvedli ANO, popiště stručně jaké komplikace, jinak přeskočte.

Text stručné odpovědi

Jak vnímáte vliv moderních bezpečnostních přístupů na celkovou úroveň bezpečnosti ve Vaší organizaci? *

	1	2	3	4	5	
Velmi pozitivně	○	○	○	○	○	Velmi negativně

Myslíte si, že se díky implementaci moderních bezpečnostních přístupů zlepšila celková úroveň bezpečnosti Vaší organizace? *

	1	2	3	4	5	
Rozhodně ano	○	○	○	○	○	Rozhodně ne

Vnímáte souvislost mezi implementací moderních přístupů a snížením počtu událostí ohrožující podnik? (Zvýšení bezpečnosti, efektivity, kvality práce apd.) *

- ◯ Ano
- ◯ Ne

Jak hodnotíte úroveň informovanosti o aktuálních hrozbách a rizicích v oblasti bezpečnosti ve Vaší oragnizaci? *

	1	2	3	4	5	
Velmi pozitivně	◯	◯	◯	◯	◯	Velmi negativně

Cítíte se dostatečně poučení na to, abyste se ve Vaší práci vyhnuli bezpečnostním rizikům? *

	1	2	3	4	5	
Rozhodně ano	◯	◯	◯	◯	◯	Rozhodně ne

Jak často se účastníte školení a kurzů zaměřených na bezpečnost ve Vaší organizaci? *

- ◯ Jedno školení ročně
- ◯ Několik školení ročně
- ◯ Žádné školení

Jak hodnotíte kvalitu a užitečnost dosavadních školení o bezpečnosti? *

	1	2	3	4	5	
Velmi pozitivně	◯	◯	◯	◯	◯	Velmi negativně

Jaké typy školení a vzdělání v oblasti bezpečnosti ve Vaší organizaci by Vám pomohly zlepšit vaše znalosti a dovednosti? (nepovinná odpověď)

Text dlouhé odpovědi

Vyhnuli jste se díky školení a znalostem z oblasti bezpečnosti nebezpečným situacím na pracovišti, ať už v souvislosti s kybernetickou bezpečností, nebo v souvislosti s BOZP či jinou z oblastí bezpečnosti ? *

- ◯ Ano
- ◯ Ne
- ◯ Jiná...

Vnímáte, že se Vaše chování v práci díky školení a vzdělávání v oblasti bezpečnosti stává zodpovědnějším z hlediska bezpečnosti? *

	1	2	3	4	5	
Rozhodně ano	◯	◯	◯	◯	◯	Rozhodně ne

Jak vnímáte důležitost dodržování bezpečnostních pravidel a postupů ve vaší práci? *

	1	2	3	4	5	
Velmi důležitá	◯	◯	◯	◯	◯	Velmi nedůležitá

Vnímáte, že vedení Vaší organizace klade dostatečný důraz na bezpečnost a vzdělávání v rámci bezpečnosti podniku?

	1	2	3	4	5	
Rozhodně ano	◯	◯	◯	◯	◯	Rozhodně ne

Cítíte se v organizaci komfortně sdílet s kolegy a nadřízenými informace o nebezpečných událostech a bezpečnostních rizicích?

	1	2	3	4	5	
Rozhodně ano	◯	◯	◯	◯	◯	Rozhodně ne

Příloha B – dotazník Přístupy podniků

V jakém odvětví pracujete? (pokud nic z výše uvedeného, napište do odpovědi Jiné:) *

- ○ Bezpečnostní složky
- ○ Veřejná správa a úřady
- ○ Výrobní průmysl (textilní, automobilový)
- ○ Zdravotnictví
- ○ IT
- ○ Cestovní ruch
- ○ Obchod
- ○ Gastronomie
- ○ Jiná...

Jaký přístup u Vás v organizaci využíváte? (Lze i kombinovat.) *

- ☐ Reaktivní přístup
- ☐ Proaktivní přístup
- ☐ Rizikový přístup
- ☐ Systémový přístup
- ☐ Procesní přístup
- ☐ Behavior based safety přístup
- ☐ Jiná...