

Prvky digitalizace a jejich vliv na zajištění bezpečnosti a ochrany zdraví při práci zaměstnanců

Bc. Martina Hanušová



Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Martina Hanušová
Osobní číslo:	L24853
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Prvky digitalizace a jejich vliv na zajištění bezpečnosti a ochrany zdraví při práci zaměstnanců

Zásady pro vypracování

- Zpracujte teoretická východiska zadaného tématu diplomové práce.
- Popište možnosti využití prvků digitalizace v oblasti zajištění bezpečnosti a ochrany zdraví při práci.
- Provedte kvantitativní výzkum využití prvků digitalizace ve vybraných organizacích v ČR.
- Na základě zjištění zpracujte návod pro efektivní implementaci a využívání prvků digitalizace v podnicích podobného zaměření.

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

Seznam doporučené literatury:

1. CHAKRAVORTI, Nirjhar. *Digital Transformation*. I. Produktivity Press, 2022. ISBN 9781032220192.
 2. MAŘÍK, Vladimír. *Průmysl 4.0: výzva pro Českou republiku*. Praha: Management Press, 2016. ISBN 9788072614400.
 3. NEUGEBAUER, Tomáš. *Bezpečnost a ochrana zdraví při práci v kostce*. 2. Česká republika: Wolters Kluwer, 2016. ISBN 9788075521071.
 4. STANĚK, Peter; MAŘÍK Vladimír; DOLIAK Dušan a ONDROVIČ Adrián. *Fakta a mýty o společnosti 5.0: zamyslenie se nad budúcnosťou*. Bratislava: Wolters Kluwer. 2019. ISBN 9788057100577.
 5. WINTER, Johannes. *Industry 4.0 – The Global Industrial Revolution*. CC BY-NC-ND license, 2023. ISBN 9783036596631.
- Další odborná literatura dle doporučení vedoucí diplomové práce.

Vedoucí diplomové práce: **Ing. Slavomíra Vargová, PhD.**
Ústav krizového řízení

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne25.4.2025.....

.....
podpis autora

ABSTRAKT

Diplomová práce se zabývá vlivem aspektů digitalizace na zajištění bezpečnosti a ochrany zdraví při práci zaměstnanců. Zaměřuje se na klíčové digitální technologie, mezi které patří blockchain, digitální dvojčata, kybernetická bezpečnost, elektronická veřejná správa, cloud computing, velká data, umělá inteligence a internet věcí. Tyto technologie jsou posuzovány z hlediska jejich přínosu pro efektivnější řízení rizik a prevenci pracovních úrazů.

Práce rovněž propojuje koncept Průmyslu 4.0 s cíli udržitelného rozvoje a zkoumá potenciál využití digitálních nástrojů v civilním i vojenském sektoru. Za účelem zjištění aktuálního stavu a vnímání digitalizace v praxi byla provedena kombinace dotazníkového šetření mezi organizacemi a řízených rozhovorů s odborníky z firem, které se zabývají vývojem a implementací prvků digitalizace.

Významným výstupem práce je návrh Roadmapy – vizuálního návodu, který poskytuje firmám postupný a praktický rámec pro implementaci digitalizačních prvků v oblasti BOZP. Roadmapa má za cíl usnadnit plánování, identifikaci prioritních oblastí a vyvarování se častých chyb v přechodu na digitální řešení. Zjištěné poznatky potvrzují pozitivní dopad digitalizace na bezpečnost práce, zároveň však upozorňují na nutnost důsledného řešení souvisejících rizik, zejména v oblasti ochrany osobních údajů a kybernetické bezpečnosti.

Klíčová slova: Digitalizace, bezpečnost práce, ochrana zdraví při práci, udržitelný rozvoj, Průmysl 4.0, ozbrojené síly, monitorovací technologie, analýza dat, Road Map.

ABSTRACT

The diploma thesis deals with the impact of the aspects of digitalization on the health and safety at work of employees. It focuses on key digital technologies including blockchain, digital twins, cyber security, e-government, cloud computing, big data, artificial intelligence and the Internet of Things. These technologies are assessed for their contribution to more effective risk management and prevention of workplace accidents.

The thesis also links the concept of Industry 4.0 to the Sustainable Development Goals and explores the potential for the use of digital tools in the civilian and military sectors. A combination of a questionnaire survey of organisations and guided interviews with experts

from companies involved in the development and implementation of digitalisation elements was conducted to determine the current status and perceptions of digitalisation in practice.

A significant output of the work is the design of a roadmap - a visual guide that provides companies with a step-by-step and practical framework for implementing digitalisation elements in the OSH sector. The roadmap aims to facilitate planning, identify priority areas and avoid common mistakes in the transition to digital solutions. The findings confirm the positive impact of digitalisation on occupational safety, but also highlight the need to address the associated risks consistently, particularly in the areas of data protection and cyber security.

Keywords: Digitalization, occupational safety, occupational health, sustainable development, Industry 4.0, armed forces, monitoring technologies, data analysis, Road Map.

Ráda bych poděkovala vedoucímu mé diplomové práce Ing. Slavomíře Vargové, PhD.

za odborné vedení, cenné rady, podnětné připomínky a trpělivost během celého zpracování této práce.

Dále děkuji všem respondentům, kteří se zúčastnili dotazníkového šetření a řízených rozhovorů, za ochotu sdílet své zkušenosti a názory, které významně přispěly k praktické části této části.

Velké poděkování patří také mé rodině a blízkým za podporu, pochopení a motivaci v průběhu celého studia.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 METODIKA PRÁCE.....	15
2 BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI	17
3 PRŮMYSL 4.0	19
4 DIGITALIZACE A JEJÍ PRVKY.....	24
4.1 KLÍČOVÉ TECHNOLOGIE DIGITALIZACE	24
4.2 PROPOJENÍ KONCEPTU PRŮMYSLU 4.0, DIGITALIZACE A UDRŽITELNÉHO ROZVOJE.....	47
5 DIGITALIZACE V OZBROJENÝCH SILÁCH.....	49
5.1 DIGITALIZACE SYSTÉMU VELENÍ A ŘÍZENÍ.....	49
5.2 KYBERNETICKÁ BEZPEČNOST A ELEKTRONICKÝ BOJ V ARMÁDĚ ČR.....	52
6 DOPAD DIGITALIZACE NA BOZP (AUTOMATIZACE A JEJÍ VLIV NA PRACOVNÍ RIZIKA).....	65
7 VÝZVY A RIZIKA DIGITALIZACE BOZP	69
8 TRENDY A BUDOUCNOST DIGITALIZACE V OBLASTI BOZP	73
8.1 TRENDY V DIGITALIZACI BOZP	73
8.2 BUDOUCNOST DIGITALIZACE BOZP	74
9 DÍLČÍ ZÁVĚR	77
II PRAKTICKÁ ČÁST.....	78
10 ŘÍZENÝ ROZHOVOR.....	79
11 DOTAZNIKOVÉ ŠETŘENÍ	86
11.1 VÝSLEDKY DOTAZNIKOVÉHO ŠETŘENÍ	87
11.2 VÝZKUMNÉ OTÁZKY	94
12 NÁVRH PODROBNÉHO ROADMAP K DIGITALIZACI BOZP.....	97
13 DISKUZE	102
ZÁVĚR	103
SEZNAM POUŽITÉ LITERATURY.....	105
SEZNAM OBRÁZKŮ	113
SEZNAM TABULEK.....	115
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	116
SEZNAM PŘÍLOH.....	118

ÚVOD

Jedním z hlavních trendů moderní společnosti je digitalizace, která radikálně mění fungování veřejného i komerčního sektoru. Moderní digitální technologie a aspekty Průmyslu 4.0 poskytují nové možnosti, jak zvýšit efektivitu výrobních, logistických, administrativních a bezpečnostních operací a zároveň lépe chránit majetek, životy a zdraví obyvatel a pracovníků. S postupující digitalizací se stále více prosazují velká data a datová analytika, umělá inteligence a strojové učení, internet věcí, cloud computing, blockchain, digitální dvojčata, systémy elektronické identifikace a nově vznikající myšlenka eGovernmentu.

Díky těmto technologiím lze shromažďovat, zpracovávat a vyhodnocovat velké objemy dat v reálném čase, což může zlepšit kybernetickou bezpečnost a zároveň zefektivnit výrobní a logistické postupy a předvídat potenciálně nebezpečné okolnosti. S tím, jak se fyzický a digitální svět v rámci Průmyslu 4.0 stále více propojuje, vyvstávají nové otázky týkající se zdraví zaměstnanců a bezpečnosti práce.

Druhá kapitola pojednává o využití současných technologií a aspektech digitalizace v kontextu ozbrojených sil. Nositelné technologie, jako jsou chytré náramky a biosenzory, které mohou identifikovat pád vojáka, sledovat jeho životní funkce nebo zdravotní stav v reálném čase a předávat informace velitelskému stanovišti nebo zdravotnickému personálu, jsou postupně zaváděny do ozbrojených sil po celém světě. Kromě tohoto vybavení využívá americká armáda, britská armáda nebo Armáda České republiky také inteligentní komunikační systémy, ochranu sluchu s aktivním potlačením hluku a pokročilé přístroje pro noční vidění. To je jen několik příkladů z reálného světa.

Dalším významným rysem nedávného pokroku je spojení digitalizace s myšlenkou udržitelného rozvoje. Kromě zachování vyšších bezpečnostních standardů při výrobních, průmyslových a vojenských činnostech pomáhají moderní digitální technologie minimalizovat důsledky pro životní prostředí, optimalizovat spotřebu energie a efektivněji využívat zdroje. Digitální transformace se tak stává prioritou společnosti i technologií.

I. TEORETICKÁ ČÁST

1 METODIKA PRÁCE

Cíl práce

Cílem této diplomové práce je analyzovat a zhodnotit vybrané prvky digitalizace a jejich vliv na zajištění bezpečnosti a ochrany zdraví při práci zaměstnanců, a to s důrazem na uplatnění v civilním i vojenském sektoru. Práce se zaměří na zmapování aktuálních možností a trendů v oblasti digitálních technologií, především Internetu věcí, cloud computingu, Big Data a analýzy dat, umělé inteligence a strojového učení, blockchainu, digitálních dvojčat, kybernetické bezpečnosti a elektronické identifikace a eGovernmentu. Dalším cílem je posoudit, jakým způsobem tyto technologie přispívají k zajištění bezpečnosti práce a ochraně zdraví zaměstnanců, případně osob v rizikovém prostředí, a navrhnout vhodná opatření pro jejich efektivní využití v souladu s principy udržitelného rozvoje.

Součástí cíle je rovněž vytvoření přehledného návrhu doporučení pro efektivní implementaci těchto digitálních prvků ve vybraných typech organizací, a identifikace jejich přínosů a možných rizik z pohledu bezpečnosti práce, ochrany zdraví a řízení rizik.

Metody zpracování

V rámci zpracování diplomové práce budou využity následující metody:

Dotazníkové šetření

Pro získání praktických poznatků a názorů zaměstnanců, pracovníků bezpečnosti práce bude realizováno dotazníkové šetření. Cílem bude zjistit povědomí o využívání digitálních technologií na pracovištích, jejich přínosy a případná rizika spojená s jejich implementací, a také vnímání digitální transformace z pohledu bezpečnosti a ochrany zdraví při práci.

Řízené rozhovory

S cílem doplnit výsledky dotazníkového šetření budou provedeny řízené rozhovory s vybranými odborníky z oblasti bezpečnosti práce. Tyto rozhovory umožní získat hlubší informace o praktických zkušenostech s využíváním digitálních nástrojů v oblasti ochrany zdraví, predikce rizik, řízení mimořádných událostí.

Roadmap

V rámci práce bude vytvořena přehledná „Road Map“ navrhuující postupný proces implementace vybraných prvků digitalizace do systému zajišťování bezpečnosti a ochrany zdraví při práci, a to v civilním sektoru. Mapa bude obsahovat jednotlivé kroky

implementace, předpokládané přínosy a rizika, a doporučení pro efektivní začlenění technologií do stávajících procesů organizací.

Analýza odborné literatury a výzkumných studií

Základní metodou bude analýza dostupné odborné literatury, legislativních dokumentů, standardů a aktuálních vědeckých studií zabývajících se digitalizací, Průmyslem 4.0, bezpečností práce a ochranou zdraví při práci. Cílem je zmapovat současný stav, trendy a přístupy k této problematice na národní i mezinárodní úrovni.

Kvantitativní a kvalitativní vyhodnocení dat

Získaná data z dotazníkového šetření a řízených rozhovorů budou vyhodnocena pomocí kvantitativních a kvalitativních metod. Kvantitativní data budou analyzována prostřednictvím statistických metod a grafického zpracování, kvalitativní data budou zpracována pomocí kategorizace a obsahové analýzy.

2 BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI

Cílem bezpečnosti a ochrany zdraví při práci (BOZP) je zabránit pracovním úrazům, nemocem z povolání a dalším škodlivým účinkům na zdraví zaměstnanců prostřednictvím souboru zásad, předpisů a zákonů. Zákony České republiky, které vymezují povinnosti zaměstnavatelů i zaměstnanců v oblasti bezpečnosti a ochrany zdraví při práci, činí z bezpečnosti a ochrany zdraví při práci základní součást pracovního práva.

Právní rámec BOZP v České republice

Mezinárodní směrnice a vnitrostátní právní předpisy slouží jako primární základ pro právní předpisy v oblasti BOZP. Základním právním předpisem upravujícím tuto oblast je zákon č. 262/2006 Sb., zákoník práce, v platném znění. Důležité jsou také následující právní normy:

- **Zákon č. 258/2000 Sb.**, o ochraně veřejného zdraví – obsahuje ustanovení o prevenci nemocí z povolání a hygienických požadavcích na pracoviště.
- **Zákon č. 281/2023 Sb.**, Zákon, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a některé další zákony.
- **Zákon č. 309/2006 Sb.**, o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci – doplňuje zákoník práce a stanovuje specifické požadavky na BOZP v různých pracovních prostředích.
- **Nařízení vlády č. 361/2007 Sb.**, kterým se stanoví podmínky ochrany zdraví při práci – definuje hygienické limity a podmínky práce v rizikovém prostředí.

Kromě národních předpisů se Česká republika řídí také normami Evropské unie, především **směrnicí Rady 89/391/EHS o zavedení opatření ke zlepšení bezpečnosti a ochrany zdraví pracovníků při práci.**

Povinnosti zaměstnavatelů a zaměstnanců

a) Povinnosti zaměstnavatelů

Podle zákoníku práce jsou zaměstnavatelé povinni zajistit bezpečné a zdraví neohrožující pracovní podmínky. Mezi hlavní povinnosti patří:

- Identifikace a hodnocení rizik na pracovišti.
- Přijetí opatření k eliminaci nebo minimalizaci rizik.

- Poskytování osobních ochranných pracovních prostředků (OOPP).
- Zajištění školení BOZP pro zaměstnance.
- Zajištění pravidelných lékařských prohlídek zaměstnanců.
- Vyšetřování pracovních úrazů a jejich evidence.

b) Povinnosti zaměstnanců

Zaměstnanci mají také povinnosti v oblasti BOZP, mezi které patří:

- Dodržování bezpečnostních předpisů a pokynů zaměstnavatele.
- Používání přidělených osobních ochranných prostředků.
- Oznamování nebezpečných situací a pracovních úrazů.
- Spolupráce se zaměstnavatelem při zajišťování bezpečnosti práce.

Rizika a prevence v oblasti BOZP

Každé pracoviště může obsahovat různá rizika, která se dělí na:

- **Fyzikální rizika** – hluk, vibrace, extrémní teploty, radiace.
- **Chemická rizika** – expozice nebezpečným látkám.
- **Biologická rizika** – kontakt s mikroorganismy, viry či plísněmi.
- **Ergonomická rizika** – nevhodná pracovní poloha, dlouhodobé statické zatížení.
- **Psychosociální rizika** – stres, šikana na pracovišti.

Pro snížení těchto rizik je nezbytné zavedení vhodných organizačních a technických bezpečnostních opatření, časté školení zaměstnanců a dodržování stanovených bezpečnostních předpisů.

Dodržování BOZP v České republice mají na starosti Státní úřad inspekce práce (SÚIP) a oblastní inspektoráty práce (OIP). Tyto organizace kontrolují pracoviště, řeší problémy, které se na nich vyskytnou, a mají pravomoc postihovat porušení bezpečnostních předpisů. Pokuty za nedodržování BOZP mohou v závislosti na závažnosti přestupku dosahovat až milion korun. Krajská hygienická stanice (KHS) určuje klasifikaci prací na základě stupně nebezpečnosti a jejich vliv na zdraví pracovníků. Dohlíží také na dodržování hygienických norem na pracovišti. (Neugebauer, 2016)

3 PRŮMYSL 4.0

Průmysl 4.0 představuje novou éru inovací a transformací ve výrobních procesech, kde digitalizace a internet umožňují jejich plnou automatizaci a vzájemné propojení, včetně souvisejících služeb.

Klíčovým prvkem tohoto konceptu jsou tzv. „chytré továrny“, které dokážou efektivně fungovat pouze díky precizně digitalizovaným a optimalizovaným předvýrobním procesům. Právě tyto digitalizované systémy umožňují firmám provoz dokonale automatizovaných továren, schopných zpracovávat různé digitální vstupy.

Jedním z těchto vstupů je již samotná zákaznická poptávka po konkrétním výrobku. Požadavky zákazníků je nutné systematicky řídit v průběhu celého vývojového i výrobního procesu. Správné řízení a implementace změn zajišťují vysokou kvalitu výrobků a jejich schopnost uspokojit potřeby zákazníků. Pouze spokojený zákazník ocení a zaplatí za přidanou hodnotu, která firmě pomáhá udržet si konkurenceschopnost na trhu.

Firmy, které dokážou efektivně pracovat s různorodými digitálními vstupy a adaptovat se na rostoucí trend sériové customizace, mají největší šanci stát se lídry v oblasti Průmyslu 4.0. (Masařík, 2016)

Globální trendy a mezinárodní kontext zavádění Průmyslu 4.0

Myšlenka Průmyslu 4.0 je nyní považována za hlavní faktor, který bude v budoucnu určovat vývoj logistiky, řízení datových toků a průmyslové výroby. I když ji různé státy zavádějí různými způsoby, jednotícím faktorem zůstává snaha o integraci automatizace, digitalizace a nových technologií s cílem zvýšit efektivitu výroby a posílit konkurenceschopnost na globálním trhu.

Celosvětová průmyslová revoluce známá jako „průmysl 4.0“ mění způsob organizace a struktury výrobních procesů napříč kontinenty. V tomto ohledu mají zásadní význam technologie jako big data, cloud computing, internet věcí, kyberneticko-fyzikální systémy a sofistikovaní roboti. Vzhledem k faktorům, mezi něž patří ekonomické zázemí, technická vyspělost a úroveň podpory inovací, však různé státy a ekonomiky přistupují k zavádění těchto aspektů odlišně na národní úrovni.

Kromě technologické připravenosti je pro úspěšné přijetí konceptu Průmyslu 4.0 nezbytná změna organizační kultury, přístupu k řízení a rozvoj digitálních kompetencí zaměstnanců. Tyto prvky jsou nezbytné pro úspěšné a dlouhodobé začlenění digitalizace do

výrobních procesů v souladu s požadavky moderního trhu a mezinárodní konkurenceschopnosti. (Winter, 2023)

Koncept Průmyslu 4.0 a digitalizace pracovního prostředí

Průmysl 4.0 přináší revoluci v organizaci výroby a pracovních procesů. Zefektivňuje výrobu, snižuje náklady a zvyšuje produktivitu využitím digitálních technologií, včetně robotiky, umělé inteligence (AI), velkých dat a internetu věcí (IoT). Klíčovou součástí tohoto procesu je digitalizace, která mění nejen technologické prostředí podniků, ale také pracovní podmínky jejich zaměstnanců.

Poskytování bezpečnosti a ochrany zdraví při práci se vyvíjí v důsledku rostoucí integrace těchto složek. Mění se jak nová, tak tradiční nebezpečí, což vyžaduje kreativní způsoby prevence. Digitalizace však s sebou přináší i možnosti, které umožňují zlepšit pracovní podmínky, předvídat rizika a účinněji monitorovat pracoviště. (Průmysl 4.0, Copyright © 2016 - 2025)

Automatizace a robotizace jako nástroj pro zvýšení bezpečnosti

Automatizace nebezpečných pracovních míst a nástup kolaborativních robotů (cobotů), kteří pomáhají pracovníkům s fyzicky náročnými nebo nebezpečnými úkoly, jsou dvě hlavní výhody Průmyslu 4.0 pro BOZP. Roboti mohou nahradit požadavek na lidský zásah v nebezpečných oblastech v odvětvích, jako je stavebnictví, těžký průmysl a chemická zařízení, kde existuje vysoké riziko poškození.

Na moderních výrobních linkách jsou často instalovány senzory a kamerové systémy, které sledují pracovní prostředí a v případě nebezpečné situace automaticky zastaví provoz. To kromě snížení pravděpodobnosti pracovních úrazů zaručuje i zvýšení efektivity výroby. (Robotizace a automatizace: Klíč k budoucnosti, 2024)

Internet věcí a chytré senzory pro prevenci rizik

Další důležitou součástí Průmyslu 4.0, která má vliv na bezpečnost pracovníků, je internet věcí. Chytré senzory instalované po celém pracovišti mohou v reálném čase shromažďovat a analyzovat údaje o teplotě, vlhkosti, úrovni škodlivých plynů a mobilitě zaměstnanců. Zaměstnanci mohou pomocí těchto dat včas reagovat a předcházet možným rizikům.

Nositelná technologie, jako jsou chytré přilby, náramky nebo vesty, se v některých podnicích používá ke sledování zdravotního stavu zaměstnanců a upozorňování na nebezpečí, jako je přetížení, vyčerpání nebo vystavení nebezpečným materiálům. Tato

metoda kromě zvýšení bezpečnosti pomáhá dlouhodobě chránit zdraví zaměstnanců. (Bezpečnost v systémech Internetu věcí (IoT), 2020)

Prediktivní údržba a minimalizace havárií

Zařízení, stroje nebo systémy lze udržovat nebo obnovovat jejich funkčnost prostřednictvím řady úkonů známých jako údržba. Jejím cílem je prodloužit životnost technologických nástrojů, snížit pravděpodobnost poruch a zaručit bezpečné a efektivní fungování. Reaktivní, preventivní a prediktivní údržba jsou tři tradiční kategorie; každá z nich má jedinečné výhody a nevýhody.

Prediktivní údržba, která využívá analýzu dat k předvídání poruch a závad zařízení dříve, než k nim dojde, je jednou z hlavních bezpečnostních výhod digitalizace. Konvenční údržba se často prováděla reaktivně, tedy těsně po zjištění závady nebo poruchy, což mohlo vést k nepředvídatelným událostem a ohrožení pracovníků.

Systémy umělé inteligence a strojového učení jsou schopny rozpoznat vzorce opotřebení a upozornit uživatele na nutnost opravy s velkým předstihem. Tím se snižuje možnost vzniku nebezpečných okolností, které by mohly ohrozit zdraví zaměstnanců, a zároveň se minimalizují neplánované prostoje. (Prediktivní údržba: definice, výhody, příklady ... to vše jedním kliknutím!, © igus, 2025)

Digitální simulace a školení zaměstnanců

Průmysl 4.0 navíc otevírá nové možnosti pro školení v krizových situacích a připravenost zaměstnanců. Díky simulaci nebezpečných scénářů v bezpečném prostředí může virtuální a rozšířená realita pomoci zaměstnancům lépe pochopit rizika a naučit se správné protokoly

pro případ nouze. Tato metoda se využívá například v jaderných elektrárnách, chemickém průmyslu a zdravotnictví, kde si pracovníci mohou nacvičit reakce na neštěstí, aniž by jim hrozilo skutečné nebezpečí. Kromě toho lze před zavedením bezpečnostních opatření do praxe v reálném prostředí tato opatření prověřit a vylepšit pomocí digitálních dvojčat, což jsou virtuální reprezentace pracovišť. (Moderní a efektivní přístup ke školení BOZP prostřednictvím virtuální reality, 2021)



Obrázek 1 – Školení zaměstnanců pomocí VR (How to Prepare and Guide Employees for VR Training?, © 2025 Visartech)

Výzvy a rizika Průmyslu 4.0 pro bezpečnost práce

Digitalizace má mnoho pozitivních dopadů na bezpečnost práce, ale přináší také nové problémy. Protože systémy Průmyslu 4.0 jsou závislé na síťové infrastruktuře a připojených zařízeních, je jedním z hlavních problémů kybernetická bezpečnost. Jakákoli technická porucha nebo kybernetický útok má potenciál způsobit narušení provozu, nepředvídatelné okolnosti a v nejhorších situacích ohrozit pracovníky.

Požadavek, aby se zaměstnanci přizpůsobili novým technologiím, představuje další obtíž. Zavádění automatizace a digitálních nástrojů vyžaduje změnu pracovních návyků a schopností. Paradoxně nesprávné nebo neuvědomělé používání digitálních technologií může způsobit nové problémy. Proto je nezbytné, aby se zaměstnancům dostalo kvalitního školení a pomoci v souvislosti se zaváděním Průmyslu 4.0.

Průmysl 4.0 zásadně mění způsob, jakým je zajištěna bezpečnost a ochrana zdraví na pracovišti. Četné nástroje, které přináší digitalizace, umožňují úspěšněji předcházet pracovním úrazům, zlepšují monitorování pracovišť a usnadňují předvídání rizik. Přináší

však také nové problémy, které je třeba řešit, zejména v oblasti adaptability pracovní síly a kybernetické bezpečnosti.

Aby se minimalizovaly nepříznivé dopady a maximalizovaly výhody pro zaměstnavatele i zaměstnance, měla by integrace digitálních technologií na pracoviště vždy probíhat s důrazem na bezpečnostní aspekty. Správné začlenění prvků Průmyslu 4.0 tak může vedle zvýšení produktivity přinést i bezpečnější a zdravější pracovní prostředí. (Staněk et al., 2019)

4 DIGITALIZACE A JEJÍ PRVKY

Na moderním pracovišti se digitalizace stala klíčovou součástí, která významně ovlivňuje produktivitu zaměstnanců, bezpečnost na pracovišti a způsob organizace práce. Digitalizace představuje metodickou přeměnu tradičních pracovních postupů pomocí digitálních technologií, automatizace a umělé inteligence.

Efektivnější řízení pracovních činností a optimalizaci výrobních procesů umožňuje rozvoj digitálních technologií včetně cloud computingu, internetu věcí, robotické automatizace procesů (RPA) a systémů pro správu dat. Digitalizace také usnadňuje spolupráci a komunikaci zaměstnanců, zejména díky využití nástrojů pro práci na dálku a digitálních platforem.

Digitalizace má zásadní význam pro odhalování a odstraňování pracovních rizik v souvislosti s BOZP. Současné systémy umožňují monitorovat pracoviště v reálném čase, automaticky vyhodnocovat bezpečnostní problémy a efektivněji školit zaměstnance.

Díky těmto faktorům je zásadní pochopit, jak digitalizace ovlivňuje pracoviště, a jak přispívá ke zdraví a bezpečnosti pracovníků. (Dopady digitalizace na trh práce v ČR a EU, 2015), (Chakravorti, 2022)

4.1 Klíčové technologie digitalizace

Díky těmto faktorům je zásadní pochopit, jak digitalizace ovlivňuje pracoviště a jak přispívá ke zdraví a bezpečnosti pracovníků. Aby bylo možné určit rozhodující prvky ovlivňující bezpečnostní opatření a jejich účinnost na digitálním pracovišti, zaměřuje se tato práce na analýzu těchto prvků.

Internet věcí (IoT – Internet of Things)

IoT je technologický koncept, který spočívá v propojení fyzických objektů prostřednictvím internetové sítě tak, aby mohly sdílet data a komunikovat mezi sebou bez lidské pomoci. Aplikace internetu věcí lze nalézt v mnoha různých oblastech, včetně dopravy, inteligentního řízení měst, zdravotnictví a průmyslu. Vedle efektivnějšího řízení a optimalizace procesů přináší využívání moderních technologií také nové problémy v oblasti kybernetické bezpečnosti a ochrany dat.

Základní komponenty Internetu věcí

Pro správné fungování systémů IoT je třeba propojit několik základních technologických komponent:

1. Systémy akčních členů a senzorů

Fyzikální faktory, jako je teplota, vlhkost, tlak a pohyb, lze shromažďovat díky senzorům. Poté jsou tato data odeslána k prozkoumání dalším systémovým komponentám. Aktory naopak umožňují přímou reakci na přijatá data, například spouštění automatických operací, změnu nastavení nebo ovládání strojů.

2. Komunikační technologie a síťová infrastruktura

Zařízení internetu věcí používají řadu komunikačních protokolů, které se liší přenosovou rychlostí, dosahem a potřebou energie. Mezi nejčastěji používané technologie patří:

- LoRaWAN a NB-IoT jsou technologie optimalizované pro zařízení s nízkou spotřebou energie a velkým dosahem;
- sítě 5G umožňují vysokorychlostní přenos dat a nízkou latenci, což vytváří nové možnosti pro autonomní systémy a chytrá města;
- Wi-Fi je vhodná pro domácí a průmyslové aplikace s vysokou spotřebou dat;
- Bluetooth a Zigbee jsou energeticky úsporná řešení pro krátké vzdálenosti.

3. Cloud computing a edge computing

Data generovaná zařízeními IoT lze zpracovávat v edge computingu nebo v cloudu. Zatímco edge computing analyzuje data přímo u zdroje, čímž snižuje latenci a šetří šířku pásma sítě, cloud computing nabízí téměř neomezené možnosti zpracování a usnadňuje centralizovanou analýzu dat.

4. Analytické nástroje a umělá inteligence

Zařízení internetu věcí generují velké množství dat a jejich efektivní využití vyžaduje sofistikovanou analýzu, často založenou na umělé inteligenci a strojovém učení. Tyto technologie umožňují automatizované rozhodování v reálném čase, rozpoznávání vzorů a prediktivní údržbu.

5. Kybernetická bezpečnost

Riziko kybernetických útoků roste s počtem připojených zařízení. Pro zajištění bezpečnosti systémů internetu věcí je nutné zavést šifrování dat, vícefaktorovou autentizaci, bezpečnostní protokoly a časté aktualizace firmwaru.

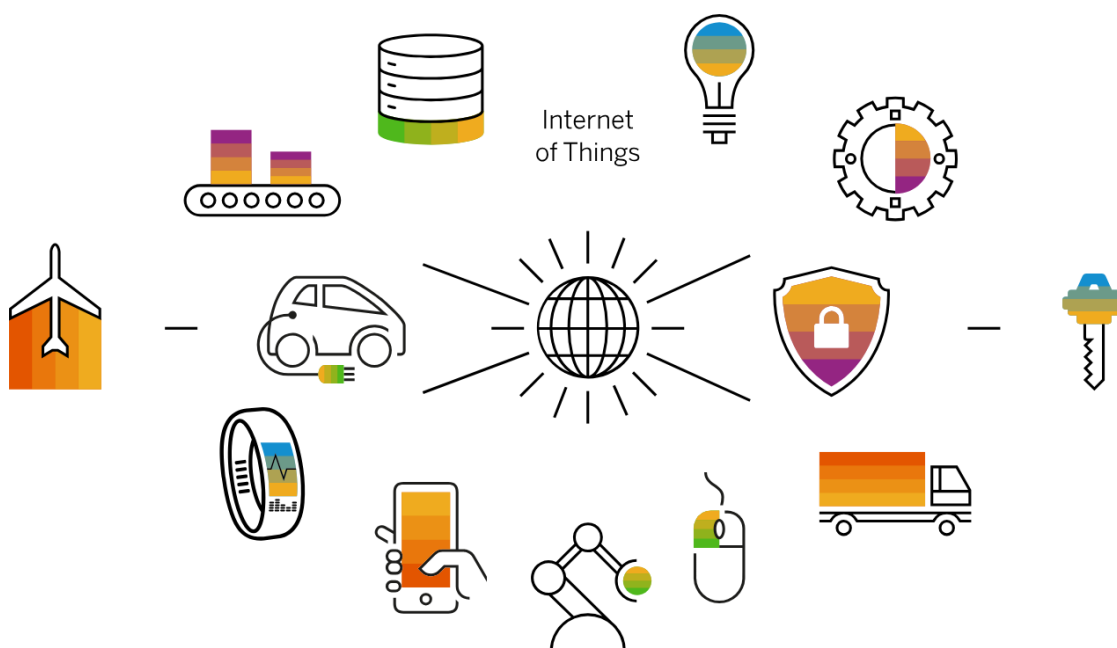
Výhody a úskalí používání internetu věcí

Mezi výhody patří:

- Zvýšení výroby a efektivity v celé řadě průmyslových odvětví;
- předvídatelná údržba a nižší provozní náklady;
- schopnost využívat data v reálném čase k automatizovanému rozhodování.

Jednou z výzev je:

- zajištění bezpečnosti připojených zařízení;
- interoperabilita a standardizace protokolů napříč různými platformami;
- zpracování a zabezpečení obrovského množství dat produkovaných systémy internetu věcí. (Internet věcí je budoucnost. V čem je jeho největší výhoda a nebezpečí, 2022)



Obrázek 2 – Internet věcí (What is the Internet of Things (IoT)?, 2022)

Cloud computing

Současná koncepce cloud computingu je založena na výpočetních službách, kdy jsou datová úložiště, výpočetní výkon a software distribuovány prostřednictvím internetu. Tento koncept umožňuje organizacím i jednotlivcům obejít se bez nutnosti vlastnit a spravovat fyzické servery nebo složité softwarové aplikace. Podstatou cloud computingu je jeho schopnost zajistit digitální transformaci, flexibilitu a efektivitu v oblasti IT.

Základní charakteristiky cloud computingu

Cloud computing charakterizuje několik základních rysů:

1. Samoobsluha na vyžádání: Zákazníci nemusí jednat přímo s dodavatelem, ale mohou přistupovat ke cloudovým službám podle potřeby.
2. Široká síťová dostupnost: Cloudové služby jsou přístupné přes internet z libovolného místa.
3. Sdílení zdrojů: Umožňuje efektivnější využití hardwarových zdrojů rozdělením výpočetního výkonu mezi více uživatelů (multi-tenancy).
4. Rychlá elasticita: Cloudové služby lze snadno rozšiřovat nebo snižovat podle měnících se potřeb.
5. Měřitelné služby: Ke sledování a účtování spotřeby cloudových zdrojů se používá skutečné využití.

Modely nasazení cloud computingu

Cloudové služby lze implementovat různými způsoby, aby vyhovovaly jedinečným požadavkům podniků:

1. Veřejný cloud (Public Cloud)

- Infrastrukturu vlastní a provozuje poskytovatel cloudu, například Amazon Web Services, Microsoft Azure nebo Google Cloud.
- Několik klientů dostává služby najednou.
- Mezi výhody patří vysoká dostupnost, nízké náklady a snadná správa.

2. Soukromý cloud (Private Cloud)

- Infrastruktura může být provozována interně nebo z externího zdroje a je určena pro jednu organizaci.

- Poskytuje větší kontrolu nad daty a zabezpečením.
- Mohou ji využívat podniky s přísnými požadavky na regulaci a ochranu dat.

3. Hybridní cloud (Hybrid Cloud)

- Můžete využít oba modely, protože integrují veřejné a soukromé cloudy.
- Umožňuje podnikům provádět méně důležité úkoly ve veřejném cloudu a citlivá data ukládat v soukromém cloudu.

4. Multi-cloud

- Společnost využívá hned několik poskytovatelů cloudových služeb, například Google Cloud a Amazon Web Services.
- Výhodou tohoto uspořádání je vyšší dostupnost, flexibilita a menší závislost na jediném zdroji. (Types of cloud computing, 2022)

Služby poskytované v rámci cloud computingu

V rámci cloud computingu jsou k dispozici tři základní typy služeb s různým stupněm správy a řízení infrastruktury:

1. **Infrastruktura jako služba** – Jedná se o službu, která nabízí mimo jiné úložiště a virtuální servery. Dvěma příklady těchto služeb jsou virtuální stroje Microsoft Azure a Amazon EC2.
2. **Platforma jako služba** – Tato služba umožňuje vytvářet a implementovat aplikace bez nutnosti správy infrastruktury. Běžnými příklady této kategorie jsou Microsoft Azure App Services a Google App Engine.
3. **Software jako služba** – Služba, která disponuje nabídkou předem připravených softwarových programů online, jako je Microsoft 365 nebo Google Workspace.

Výhody a výzvy cloud computingu

Výhody cloud computingu

- **Nižší náklady** – Organizace nemusí investovat do nákladné IT infrastruktury a platí pouze za skutečně využívané zdroje.
- **Škálovatelnost a flexibilita** – Schopnost IT systémů pružně se přizpůsobovat měnícím se potřebám.

- **Vysoká dostupnost a spolehlivost** – Velká míra redundance, kterou cloudové služby nabízejí, snižuje možnost výpadků.
- **Zabezpečení a zálohování** – Poskytovatelé cloudových služeb poskytují pokročilé bezpečnostní funkce, jako je šifrování dat a automatické zálohování.
- **Přístup odkudkoliv** – Uživatelé mohou pro přístup ke svým datům a aplikacím používat jakékoli zařízení s připojením k internetu.

Výzvy a omezení cloud computingu

Cloud computing přináší mnoho výhod, ale nese s sebou i nějaké nevýhody:

- **Závislost na poskytovateli** – Vzhledem k časté věrnosti dodavateli může být pro organizace obtížné přejít na jiný systém.
- **Bezpečnost a soukromí dat** – Při přenosu citlivých dat do cloudu jsou nezbytné přísné bezpečnostní postupy, zejména v regulovaných odvětvích, jako je zdravotnictví a bankovníctví.
- **Možné výpadky služeb** – I když mají velcí poskytovatelé cloudových služeb silnou infrastrukturu, přerušení služeb je stále možné.
- **Právní a regulační otázky** – Údaje mohou být uchovávány na serverech umístěných v mnoha jurisdikcích, což může ztěžovat dodržování zákonů (např. GDPR EU). (Vše, co potřebujete vědět o cloudu, Copyright © 2025 - Algotech a.s.)

Aplikace cloud computingu v praxi

Podniková sféra – Cloud computing využívají podniky ke zpracování dat, provádění obchodních aplikací a spolupráci zaměstnanců. Cloudové služby využívají například firmy jako Netflix, které poskytují milionům spotřebitelů streamovaná média.

Věda a výzkum – Výzkumné organizace analyzují velké soubory dat pomocí cloud computingu, například v klimatologii, umělé inteligenci nebo genomice.

Veřejná správa a zdravotnictví – Cloud computing využívají nemocnice a vládní agentury k bezpečnému ukládání dat a nabízení digitálních služeb pacientům nebo obyvatelům.

Vzdělávání – Vzdělávací instituce a školy využívají cloudové systémy pro správu online kurzů, sdílení výukových zdrojů a e-learning. (Co je cloud computing, jak funguje a proč ho zavést do firmy, 2024)



Obrázek 3 – Cloud computing (3 typy cloud computingu: SaaS, PaaS, IaaS, © 2025)

Big Data a analýza dat

Vzhledem k tomu, že množství digitálních dat v posledních desetiletích exponenciálně roste, začal se používat termín „Big Data“. Toto slovní spojení označuje neuvěřitelně rozsáhlé, dynamické a různorodé datové soubory, k jejichž dobré analýze je zapotřebí určitých technologií a analytických technik. Big Data se používají v celé řadě odvětví, včetně vládních agentur, zdravotnictví a finančnictví.

Charakteristika Big Data

- **Volume (Objem)** – Kapacita zpracování dat přesahuje kapacitu běžných databázových systémů, protože je obrovská.
- **Velocity (Rychlost)** – Standardem je generování a zpracování dat v reálném čase nebo s minimálním zpožděním.
- **Variety (Různorodost)** – Informace mají různorodou strukturu a pocházejí z mnoha zdrojů (text, fotografie, videa, senzory, sociální sítě atd.).
- **Veracity (Důvěryhodnost)** – Pro správnou interpretaci a rozhodování je zásadní kvalita a spolehlivost údajů.

- **Value (Hodnota)** – Dokud nejsou data řádně analyzována a využita k poskytnutí cenných informací, jsou bezcenná.

Využití Big Data v praxi

- Big Data se v současnosti uplatňují v mnoha odvětvích: Zdravotnictví – analýza genetických dat, předpovídání epidemií, personalizovaná medicína. Elektronické zdravotní záznamy umožňují lékařům efektivněji diagnostikovat a léčit.
- Finance – odhalování podvodů, algoritmické obchodování, vyhodnocování rizik. Banky a pojišťovny využívají Big Data ke zvýšení bezpečnosti a efektivity finančních operací.
- Marketing a obchod – Personalizovaná reklama, analýza spotřebitelských vzorců, doporučovací systémy. Společnosti využívají analýzu dat k cílení na zákazníky a zlepšování zákaznické zkušenosti. Průmysl 4.0 - Optimalizace výrobních procesů, prediktivní údržba strojů. Data ze senzorů umožňují efektivnější řízení výroby a snižování nákladů.
- Doprava a logistika – Optimalizace dopravních tras, předpovídání dopravy. Analýza dat z GPS a dopravních senzorů pomáhá snižovat dopravní zácpy a zlepšovat efektivitu dodávek. (What is Big Data?)

Výhody Big Data

Lepší rozhodování na základě dat

- Analýza velkých objemů dat pomáhá organizacím lépe se rozhodovat na základě faktických informací, nikoli na základě pocitů nebo předsudků.
- Přizpůsobení služeb a zkušeností klientů – Big Data dávají firmám důkladný přehled o chování uživatelů, což jim pomáhá poskytovat individualizovanější marketing, cílené produkty a efektivní služby zákazníkům.
- Předpovídání trendů a prediktivní analýza – v různých odvětvích (například ve zdravotnictví, bankovníctví a dopravě) umožňují pokročilá analytická řešení předpovídat chování klientů, budoucí poptávku, technické poruchy nebo výskyt rizik.

- Zvýšení produktivity a úspora nákladů – optimalizací provozu pomocí datové analytiky lze snížit náklady, zefektivnit řízení výroby nebo zásob a minimalizovat plýtvání.
- Vývoj nových služeb a inovací – analýzou požadavků, zvyků a zájmů uživatelů pomáhají velká data vytvářet nové zboží a služby.

Nevýhody Big Data

Nároky na technologickou infrastrukturu – pro zpracování a ukládání velkého množství dat je nutná silná hardwarová a softwarová infrastruktura, což může vyžadovat značné počáteční výdaje.

Nedostatek odborných znalostí a složitost – analýza velkých objemů dat vyžaduje specifické odborné znalosti v oblasti datové vědy, statistiky a IT a na trhu někdy nejsou k dispozici kompetentní odborníci.

Rizika pro ochranu soukromí – zpracování citlivých nebo osobních údajů ve velkém rozsahu může mít významné etické a právní důsledky, zejména v případě porušení zásad GDPR a dalších zákonů.

Možnost nesprávné interpretace údajů – nepřesná zjištění nebo špatně sestavená analýza mohou vést ke špatným rozhodnutím. Přestože velká data nabízejí množství informací, nejsou vždy přesná. (Velká data (big data): definice, výhody a výzvy (infografika), 2021)

Umělá inteligence a strojové učení

V současné digitální revoluci jsou umělá inteligence a její podmnožina, strojové učení (ML), zásadními technologiemi. Zatímco strojové učení se zaměřuje na metody, které umožňují počítačům učit se z dat bez explicitního programování, umělá inteligence označuje schopnost strojů napodobovat lidský intelekt, včetně myšlení, rozhodování a učení. Tyto technologie hojně využívá řada podniků, včetně zdravotnictví, bankovníctví a automobilového průmyslu. (Co je to strojové učení?, © 2025 SAP)

Umělá inteligence

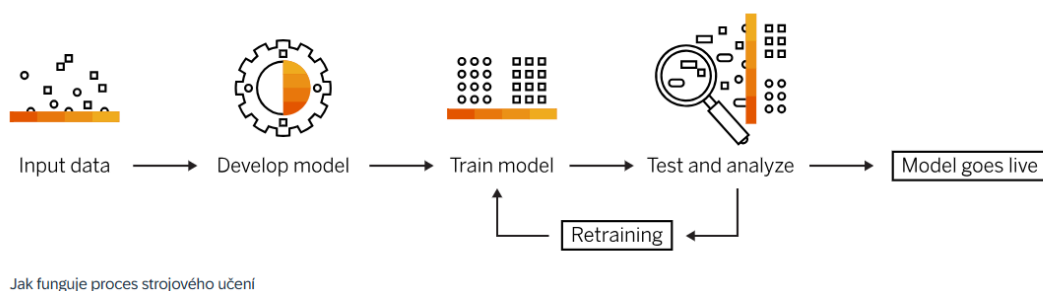
Cílem umělé inteligence je vyvinout systémy, které dokážou napodobit kognitivní procesy lidského mozku, včetně plánování, logického myšlení, rozpoznávání vzorů a přirozené komunikace. Existují dvě základní kategorie umělé inteligence:

- Slabá umělá inteligence (úzká umělá inteligence): Systémy určené k provádění určitých úkolů, včetně doporučovacích algoritmů (Netflix, YouTube) nebo hlasových asistentů (Alexa, Siri).
- Hypotetický typ umělé inteligence, která je stejně inteligentní jako člověk, schopná samostatného myšlení a adaptace na situaci, je známá jako „silná AI“ (známá také jako „obecná AI“). V současné době probíhá fáze studie. (Study on artificial intelligence: The state of the art and future prospects, 2021)

Strojové učení

Odvětví umělé inteligence zvané strojové učení umožňuje počítačům učit se a dosahovat lepších výsledků na základě analýzy velkého množství dat. Využívá řadu technik, které se dělí do tří základních skupin:

- Supervised Learning (učení pod dohledem): Naučit algoritmy, jak rozpoznávat objekty na obrázcích, lze například pomocí označených trénovacích dat.
- Když algoritmy analyzují neoznačená data, hledají vzory nebo shluky (např. segmentace zákazníků v marketingu). Tento postup se označuje jako učení bez dohledu.
- Učení s posilováním: Když algoritmus interaguje se svým okolím, dostává vstupy, které mu pomáhají učit se (např. systémy umělé inteligence hrající šachy nebo zlepšující pohyby robotů).



Obrázek 4 – Strojové učení (Co je to strojové učení?, © 2025 SAP)

Klíčové technologie a nástroje AI a ML

Moderní umělou inteligenci a ML umožňuje pokrok v řadě oblastí:

Hluboké učení (Deep Learning, DL) je sofistikovaný typ strojového učení, který identifikuje složité vzorce v datech pomocí hlubokých neuronových sítí (Deep Neural Networks, DNN).

Technologie, která umožňuje počítačům porozumět lidské řeči a vytvářet text (např. chatboti a překladače), je známá jako zpracování přirozeného jazyka neboli NLP.

Počítačové vidění: Techniky, které umělé inteligenci umožňují analyzovat vizuální data, jako je detekce objektů ve videích nebo rozpoznávání obličejů.

Edge AI je přímé využití AI v koncových bodech (jako jsou chytré telefony a senzory internetu věcí) bez nutnosti komunikace v cloudu.

Níže jsou uvedeny nejoblíbenější softwarové rámce pro vytváření modelů AI a ML:

- PyTorch (Facebook/Meta)
- TensorFlow (Google)
- Scikit-learn (Python knihovna pro ML) (Co je to strojové učení?, © 2025 SAP)

Aplikace AI a ML v různých odvětvích

Zdravotnictví

V současné zdravotní péči nabývá umělá inteligence stále většího významu. Jednou z hlavních výhod je schopnost diagnostikovat nemoci pomocí analýzy lékařských snímků, jako jsou snímky z CT a MRI, což umožňuje rychlejší a přesnější identifikaci zdravotních problémů. Předpovídání epidemií a vytváření individuálních léčebných programů, které zohledňují jedinečné požadavky každého pacienta, jsou další dvě oblasti použití. Kromě toho lékaři stále častěji využívají asistenty umělé inteligence, jako je IBM Watson, kteří pomáhají s diagnostikou, interpretací dat a plánováním terapie.

Finanční sektor

Umělá inteligence významně ovlivňuje bankovnínictví a finanční průmysl. Jednou z jejích hlavních aplikací je odhalování podvodů v reálném čase, které pomáhá chránit zákazníky a finanční instituce před podvody. Umělá inteligence se využívá také při algoritmickém obchodování a optimalizaci investičních strategií, kde vyhodnocuje obrovské objemy dat a rozhoduje se rychleji než člověk. Automatizovaní chatboti se také často používají v bankovních službách ke zlepšení zákaznické podpory, k zodpovídání dotazů spotřebitelů a ke zjednodušení správy finančních produktů.

Doprava a autonomní řízení

Umělá inteligence hraje klíčovou roli v moderní dopravě. Autonomní vozidla, jako například Tesla s funkcí Autopilot, využívají AI pro rozhodování v reálném provozu, čímž zvyšují

bezpečnost a efektivitu řízení. Kromě toho se AI uplatňuje i v optimalizaci dopravních toků pomocí prediktivní analýzy, která na základě aktuálních a historických dat pomáhá snižovat dopravní zácpy a zlepšovat plynulost dopravy ve městech.

Průmysl a výroba

AI přináší revoluci do průmyslové výroby a nové metody optimalizace procesů. Prediktivní údržba strojů zvyšuje produktivitu a snižuje náklady na opravy tím, že zkracuje prostoje výrobních linek a umožňuje včasnou identifikaci možných problémů. Automatizované robotické systémy se používají při kontrole kvality a montáži, aby se omezily chyby a zaručila vysoká přesnost výroby. Tyto technologie zvyšují rychlost, spolehlivost a efektivitu průmyslových operací.

Marketing a e-commerce

Současné digitální firmy stále častěji využívají umělou inteligenci k přizpůsobení zákaznické zkušenosti. Doporučovací systémy, které používají například společnosti Netflix a Amazon, zkoumají chování zákazníků a podle jejich vkusu jim předkládají vhodný materiál nebo zboží. Umělá inteligence se také používá ke generování reklam a předvídání chování spotřebitelů, což firmám pomáhá lépe zaměřit své marketingové iniciativy a zvýšit jejich úspěšnost. Podniky mohou s využitím těchto technologií poskytovat uživatelům personalizované informace a hlouběji porozumět jejich požadavkům. (Machine learning in manufacturing and industry 4.0 applications, 2021)

Výhody a výzvy ML

Výhody:

- Automatizace nudných a pravidelných prací – efektivní automatizace úkolů, které se dříve prováděly ručně, je možná díky AI a ML, což zvyšuje výkonnost, snižuje počet chyb a šetří peníze a čas.
- zpracování velkého množství dat – velké a komplikované soubory dat, které by člověk nedokázal zpracovat, lze analyzovat a zpracovat pomocí strojového učení, které v datech odhaluje i skryté vzorce a korelace.
- Zvyšování kvality úsudku – systémy umělé inteligence mohou pomocí prediktivních modelů a předchozích dat usnadnit rozhodování v reálném čase a zlepšit výsledky v oblastech, jako je řízení průmyslu, zdravotnictví a finance.

- Stálé fungování bez únavy – systémy AI mohou na rozdíl od lidí pracovat nepřetržitě a spolehlivě i při velkém stresu.

Nevýhody:

- Sociální a etické problémy – vývoj umělé inteligence vyvolává řadu etických otázek, včetně potřeby lidského dohledu nad rozhodováním, ztráty lidské interakce ve službách, algoritmických předsudků a otázek odpovědnosti.
- Ztráta pracovních míst – lidská práce může být nakonec v některých profesích a postupech nahrazena automatizací, zejména u manuálních nebo běžných úkonů, což může mít negativní společenské dopady.
- Závislost na datech – Kalibr vstupních dat má přímý dopad na kalibr výstupů AI a ML. V důsledku špatně kalibrovaných algoritmů nebo nerovnoměrných dat může dojít k neobjektivním rozhodnutím nebo nesprávným závěrům. (Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends, and Directions, 2020)

Blockchain

Technologie blockchain je distribuovaná databáze, která využívá kryptografické techniky k propojení digitálních dat v blocích v chronologickém pořadí. Ačkoli je nejčastěji spojována s kryptoměnami, zejména s Bitcoinem, její využití lze nalézt v celé řadě oblastí, včetně veřejné správy, zdravotnictví a logistiky.

Základem blockchainu je decentralizace; informace jsou rozptýleny v síti uzlů a nejsou uchovávány na jediném centrálním serveru. Každý člen sítě má přístup ke stejné verzi databáze a jakákoli změna záznamu – například převod kryptoměny – musí být schválena většinou členů prostřednictvím procesu konsensu.

Bloky tvoří tři základní komponenty: Jednotlivé otisky dat, které slouží jako digitální podpis, se nazývají hash bloku. Bloky jsou spojeny předchozím blokovým hashem, který také zaručuje integritu řetězce.

Dva nejoblíbenější konsensuální algoritmy Proof of Work (PoW) a Proof of Stake zaručují spolehlivost a neměnnost dat, aniž by vyžadovaly centrální autoritu. (What is blockchain?)

Výhody technologie blockchain

1. Otevřenost a odpovědnost

Protože je každý záznam neměnný a veřejný (v případě veřejných blockchainů), lze historii transakcí snadno ověřit.

2. Bezpečnost a odolnost proti neoprávněné manipulaci

Manipulace s daty je obtížná díky kryptografii a rozptýlené architektuře sítě.

3. Rozptýlenost snižuje možnost vzniku jediného bodu selhání a odstraňuje nutnost důvěry v centrální autoritu.

4. Automatizace chytrých smluv

Obchodní logika může být prováděna automaticky pomocí chytrých smluv, čímž odpadá potřeba prostředníka.

Nevýhody technologie blockchain:

1. Energetická náročnost (zejména u PoW)

Ekologickou stopu zvyšují konsensuální techniky, jako je Proof of Work, které vyžadují značné množství výpočetního výkonu.

2. Nízká rychlost zpracování a škálovatelnost

Propustnost blockchainových sítí je často omezená; například Bitcoin dokáže zpracovat pouze asi sedm transakcí za sekundu.

4. Nevratnost záznamů

Transakci nelze z blockchainu vymazat, jakmile byla ověřena. Tento prvek může být problematický v případě podvodu nebo chyby.

5. Nejistota v zákonech a předpisech

Zákony týkající se blockchainu a kryptoměn se stále vyvíjejí a v jednotlivých zemích se značně liší.

6. Složitost a vysoké nároky na implementaci

K integraci technologie blockchain do běžných systémů je zapotřebí jak finančních prostředků, tak technologického know-how. (Blockchain Faks: What Is, How It works, and How It Can Be Used)

Průmysl 4.0

Problematika související s konceptem Průmyslu 4.0 je detailně rozpracována v kapitole 3.

Digitální dvojčata (Digital Twins)

Digitální dvojče je virtuální reprezentace reálného systému, procesu nebo předmětu, která se používá pro monitorování, simulaci a optimalizaci v reálném čase. Tato myšlenka, jejímž cílem je zefektivnit řízení konkrétního zařízení nebo procesu od návrhu přes výrobu až po provoz a údržbu, je silně spojena s rozvojem průmyslu 4.0 a digitalizací.

K vytvoření digitálního dvojčete se propojuje několik důležitých technologií:

Internet věcí shromažďuje informace z fyzického světa prostřednictvím senzorů a chytrých zařízení. Výměnu a ukládání dat v reálném čase umožňuje cloud computing. Strojové učení a umělá inteligence zpracovávají a analyzují data za účelem vytváření předpovědí a optimalizace výsledků. Pokročilé analytické a simulační nástroje umožňují testování mnoha scénářů bez nutnosti fyzického zásahu do systému.

Digitální dvojče je živý systém, který je průběžně aktualizován na základě vstupních dat ze senzorů, nikoli pouze statický 3D model. To umožňuje kromě zpětné vazby také prediktivní řízení, které je klíčové pro maximalizaci efektivity, zajištění bezpečnosti a snížení nákladů. (Industry 4.0 – Digitální dvojčata, 2022)

Hlavní oblasti využití digitálních dvojčat:

1. Výroba a průmyslová automatizace

Digitální dvojčata výrobních linek a strojů umožňují prediktivní plánování údržby, optimalizaci provozu a simulaci bezeztrátových změn.

2. Stavebnictví a správa budov BIM (Construction and Building Management).

Skutečný stav budovy včetně její infrastruktury se odráží v digitálním modelu.

3. Energetika

Energetický monitoring a řízení elektráren, turbín, transformátorů a sítí v reálném čase.

4. Zdravotnictví

Vyvíjejí se digitální dvojčata lidských orgánů nebo celých pacientů pro využití v medicíně na míru a simulaci zákroků.

5. Doprava a logistika

Předvídání poruch infrastruktury a optimalizace tras a toků zboží.

Výhody digitálních dvojčat:

- **Prediktivní údržba** – Včasné odhalení možných nedostatků dříve, než se projeví.
- **Optimalizace výkonu** – Efektivnější řízení je výsledkem simulace různých provozních scénářů.
- **Snížení nákladů a rizik** – Při použití simulací není nutné ověřovat změny na skutečném systému.
- **Zrychlení vývoje produktů** – Inovace mohou probíhat rychleji díky digitálnímu prototypování.
- **Zvýšení bezpečnosti** – Bezpečnost provozu se zvyšuje díky monitorování v reálném čase.

Nevýhody a výzvy digitálních dvojčat:

- **Vysoká komplexita implementace** – Vyžaduje integraci několika technologií a systémů.
- **Nároky na kvalitu a objem dat** – Model nelze realizovat bez kvalitních a přesných údajů.
- **Bezpečnost a ochrana dat** – Silné zabezpečení je nezbytné pro ukládání i přenos dat.
- **Počáteční investiční náklady** – zejména v běžných průmyslových podnicích.
(Digital Twins in Industry 5.0, 2023)

Kybernetická bezpečnost

Kybernetická bezpečnost je soubor taktik, nástrojů, postupů a zásad, jejichž cílem je zabránit neoprávněnému přístupu, poškození, zneužití nebo narušení systémů, sítí, zařízení a dat. Kybernetická bezpečnost se v souvislosti s digitalizací a rostoucí závislostí na

informačních technologiích stává nezbytnou součástí každé organizace a veřejné správy. Kromě ochrany citlivých údajů je zabezpečení digitální infrastruktury nezbytné pro zachování důvěry uživatelů, kontinuity podnikání a dodržování právních předpisů a nařízení.

Hlavní oblasti kybernetické bezpečnosti:

1. **Síťová bezpečnost** – chrání dostupnost a integritu dat přenášených v počítačových sítích. Skládá se ze systémů detekce a prevence (IDS/IPS), firewallů a šifrování komunikace.
2. **Aplikační bezpečnost** – se zaměřuje na ochranu softwarových aplikací před hrozbami, jako je SQL injection, cross-site scripting, malware atd.
3. **Bezpečnost dat** zahrnuje volby a opatření týkající se správy a ochrany dat a systémů IT.
4. **Identita a správa přístupu (IAM)** – bezpečné přihlašování a přístupová práva pro určité uživatele a miniaplikace.
5. **Bezpečnost koncových zařízení** – využívání antivirového softwaru, aktualizací a pravidel k ochraně osobních počítačů, mobilních zařízení a dalších koncových bodů.
6. **Operační bezpečnost** zahrnuje volby a postupy týkající se správy a ochrany dat a systémů IT.
7. **Školení a povědomí uživatelů** – Vzdělávání zaměstnanců v oblasti kybernetických nebezpečí je zásadní, protože lidé jsou často nejslabším článkem bezpečnostního řetězce. (Cybersecurity for Industry 4.0 in the current literature: A reference framework, Copyright © 2025 Elsevier B.V. All)

Nejčastější kybernetické hrozby:

- **Phishing** – e-maily nebo internetová komunikace, které jsou podvodné a jejichž cílem je získat soukromé informace.
- **Ransomware** – šifrovací škodlivý software, který za odemčení dat požaduje výkupné.
- **Malware** – souhrnné označení pro škodlivý software, jako jsou spyware, trojské koně a viry.
- **DDoS útoky** – odeslání takového množství dotazů, že dojde k pádu serveru nebo služby.

Insider threats – interní hrozby, například ze strany rozzuřených zaměstnanců. (Bezpečnostní politika, 2019)

Výzvy v oblasti kybernetické bezpečnosti:

- Rychlý vývoj technologií – nové platformy a zařízení často nejsou dostatečně zabezpečené.
 - Nedostatek odborníků – rostoucí poptávka po kvalifikovaných odbornících na kybernetickou bezpečnost.
 - Rostoucí počet a sofistikovanost útoků – útočníci používají stále pokročilejší metody.
8. Legislativní a regulační požadavky – organizace musí dodržovat právní rámec (např. GDPR, zákon o kybernetické bezpečnosti). (Cybersecurity for Industry 4.0 in the current literature: A reference framework, Copyright © 2025 Elsevier B.V. All)

Zásady účinné kybernetické bezpečnosti:

- Zásada „nejmenšího oprávnění“ říká, že každý uživatel má přístup jen k těm informacím a funkcím, které skutečně potřebuje.
- Pro odstranění známých zranitelností jsou zásadní časté opravy a aktualizace.
- Kombinace hesla s dalším prvkem (např. mobilní autentizace) je známá jako vícefaktorová autentizace neboli MFA.
- Plán reakce na incidenty je taktika, která se používá k reakci na kybernetické útoky a k rychlému obnovení běžného provozu.
- Časté zálohování dat je nezbytné pro jejich obnovu v případě ztráty nebo útoku.

Výhody a nevýhody kybernetické bezpečnosti

Výhody:

- Ochrana soukromých informací a dat – Kybernetická bezpečnost zaručuje, že obchodní tajemství, strategické informace a osobní údaje jsou chráněny před neoprávněným přístupem, únikem a zneužitím.
- Zachování kontinuity provozu – Výpadky systému a narušení IT infrastruktury jsou méně pravděpodobné díky účinným bezpečnostním opatřením, což snižuje riziko provozních ztrát nebo poškození dobrého jména organizace.

- Prevence a identifikace útoků – Včasnou identifikaci hrozeb a preventivní opatření, která eliminují nebo výrazně snižují škody způsobené kybernetickými útoky, umožňují moderní bezpečnostní systémy.
- Zvýšení důvěry veřejnosti a obchodních partnerů – Pověst organizace u zákazníků, partnerů a regulačních orgánů se zvýší, pokud zaujme jasný a praktický přístup ke kybernetické obraně.
- Dodržování zákonů a předpisů – Právní přehlednost a prevenci pokut zajišťuje dodržování zákona o kybernetické bezpečnosti, GDPR a dalších zákonů.

Nevýhody a výzvy:

- Nákladná implementace a údržba – Implementace sofistikovaných bezpečnostních opatření (jako jsou firewally, šifrování a školení zaměstnanců) může být nákladná a organizačně náročná, zejména pro malé a střední podniky.
- Jsou nutné neustálé aktualizace – Kybernetická bezpečnost není jednorázová záležitost; aby bylo možné držet krok s neustále se vyvíjejícími nebezpečími, je třeba pravidelně aktualizovat systémy a odborné znalosti.
- Riziko vnitřní hrozby – Lidé jsou i nadále nejslabším článkem bezpečnostního řetězce, a to i s rozvojem technologií. Existuje vážné riziko vyplývající z neúmyslných chyb zaměstnanců nebo z úmyslných interních útoků.
- Složitost prostředí – množství systémů, zařízení a dat, které vyžadují ochranu, se v důsledku rostoucí digitalizace rozšiřuje. To vytváří velký tlak na správu a koordinaci bezpečnostních opatření.
- Možné zdržení některých postupů – v některých situacích mohou bezpečnostní opatření (například šifrování a vícefaktorová autentizace) bránit přístupu k datům nebo narušovat uživatelský komfort. (Cybersecurity for Industry 4.0 in the current literature: A reference framework, Copyright © 2025 Elsevier B.V. All)

Elektronická identifikace a eGovernment

Dvěma základními východisky současné digitalizace veřejné správy jsou elektronická identifikace (eID) a elektronická veřejná správa (eGovernment). Ty si od digitálních technologií slibují zjednodušení, zefektivnění a zprůhlednění komunikace mezi veřejností, soukromým sektorem a státní správou.

Elektronická identifikace

Oproti běžným fyzickým technikám autentizace (např. předložení průkazu totožnosti v práci) se autentizace uživatele provádí v digitálním prostředí a nazývá se elektronická identifikace. Používá se k bezpečnému přístupu k internetovým službám poskytovaným bankami, vládou a dalšími organizacemi. Využívá technologie, jako jsou mobilní klíče, čipové karty, biometrické údaje a certifikáty.

Nejrozšířenějším prostředkem elektronické identifikace v České republice je eObčanka, což je občanský průkaz s čipem, který umožňuje bezpečný přístup do systémů veřejné správy. Mezi další možnosti patří bankovní identita (BankID), která byla představena jako kompletní autentizační řešení v roce 2021, identita občana a mobilní klíč eGovernmentu.

Význam eID

Díky ověřeným autentizačním technikám, které snižují možnost krádeže identity, elektronická identifikace výrazně zvyšuje bezpečnost přístupu ke službám. Jednou z jejích hlavních výhod je, že umožňuje ověření totožnosti bez nutnosti fyzické přítomnosti, což šetří čas a usnadňuje přístup k digitálním portálům pro veřejnou správu, bankovníctví, zdravotnictví a další oblasti. Kromě toho elektronická identita podporuje růst digitální společnosti a efektivnější fungování elektronické veřejné správy tím, že díky standardizovaným metodám zaručuje konzistentní a jednotný přístup k široké škále technologických služeb napříč různými platformami a institucemi. (Elektronická identifikace, 2024)

eGovernment – Elektronizace veřejné správy

Pojem „eGovernment“ popisuje způsob, jakým veřejná správa využívá informační a komunikační technologie ke zvýšení dostupnosti, efektivity a transparentnosti veřejných služeb. Cílem je snížení byrokracie, urychlení vyřizování agendy a podpora komunikace mezi veřejností, soukromým sektorem a státní správou.

Mezi hlavní nástroje eGovernmentu v České republice patří:

- **Portál občana** – Přístup ke službám veřejné správy usnadňuje centrální rozhraní.

- **Datové schránky** – elektronický přenos právně závazných dokumentů.
- **Základní registry (např. registr obyvatel, registr práv a povinností)** – jediný bod pravdy reprezentovaný centrální databází.
- **eRecept, eNeschopenka, eDoklady** – konkrétní případy digitalizace ve zdravotnictví a dalších oblastech.
- **Jednotný identitní prostor (JIP)** – mechanismus pro řízení přístupu k digitálním službám a elektronickým identitám.

Digitální zapojení, jako jsou konzultace online, elektronické hlasování a účast veřejnosti na rozhodovacích procesech, umožňuje také eGovernment.

Výhody elektronické identifikace a eGovernmentu:

- Úspora peněz a času díky tomu, že odpadá nutnost chodit osobně na úřady.
- Služby jsou dostupné kdykoli a odkudkoli.
- Zvyšuje se transparentnost, protože je možné jednoduše sledovat a kontrolovat elektronické operace.
- lepší ochrana osobních údajů díky použití vhodných bezpečnostních opatření.

Výzvy a rizika:

- Zvyšující se riziko útoků na systémy veřejné správy se nazývá kybernetická bezpečnost.
- Část populace má omezený přístup k digitálním technologiím, což je jev známý jako „digitální propast“
- V právním a organizačním rámci je nutná koordinace mezi institucemi a vládními úrovněmi.
- Uživatelská přívětivost: Je velmi důležité, aby všichni občané mohli systémy snadno pochopit a používat. (Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion, Copyright © 2025)

Komparativní tabulka vybraných prvků digitalizace

Tabulka 1 – Porovnání prvků digitalizace (vlastní)

Prvek digitalizace	Účel / Funkce	Výhody	Nevýhody / Rizika	Příklady využití
Internet věcí	Propojení fyzických zařízení do sítě pro sběr a sdílení dat	Automatizace, prediktivní údržba, sběr dat v reálném čase	Kybernetická zranitelnost, složité zabezpečení, interoperabilita	Chytré domácnosti, senzory ve výrobě, sledování spotřeby energie
Cloud computing	eGovernment a eID	Flexibilita, škálovatelnost, snížení nákladů na infrastrukturu	Závislost na poskytovateli, bezpečnost dat, výpadky služeb	Google Cloud, Microsoft Azure, Amazon AWS
Big Data a analýza dat	Google Cloud, Microsoft Azure, Amazon AWS	Lepší rozhodování, identifikace trendů, personalizace služeb	Nároky na infrastrukturu a kvalifikaci, ochrana osobních údajů	Marketing, zdravotnictví, finanční sektor, predikce chování zákazníků
Umělá inteligence a ML	Automatizace rozhodování a analýza dat pomocí algoritmů	Rychlost, přesnost, adaptivní učení, optimalizace procesů	Netransparentnost rozhodování, etické otázky, zkreslení modelu	Rozpoznávání obrazu, chatboty, prediktivní údržba, autonomní vozidla
Blockchain	Decentralizované, bezpečné uchovávání a sdílení informací	Transparentnost, neměnnost záznamů, důvěryhodnost	Energetická náročnost, nízká rychlost zpracování, legislativní nejistota	Kryptoměny, dodavatelské řetězce, ověřování pravosti dokumentů
Průmysl 4.0	Integrace digitálních technologií do výroby a řízení procesů	Flexibilita výroby, vyšší efektivita, menší chybovost	Potřeba investic, kybernetická bezpečnost, potřeba	Automatizované továrny, robotika, digitální řízení výroby

Prvek digitalizace	Účel / Funkce	Výhody	Nevýhody / Rizika	Příklady využití
			rekvalifikace pracovní síly	
Digitální dvojčata	Virtuální modely reálných objektů či procesů pro simulaci a optimalizaci	Prediktivní údržba, testování bez rizika, optimalizace výkonu	Složitost implementace, vysoké nároky na data a propojení	Letecký průmysl, výrobní linky, energetika
Kybernetická bezpečnost	Ochrana systémů, sítí a dat před kybernetickými hrozbami	Ochrana citlivých dat, prevence útoků, důvěryhodnost	Náklady na implementaci, závislost na lidském faktoru, neustálé hrozby	Firewall, antiviry, školení zaměstnanců, bezpečnostní audit
eGovernment a eID	Digitalizace veřejné správy a ověřování identity občanů	Rychlejší přístup ke službám, transparentnost, dostupnost na dálku	Digitální propast, závislost na infrastruktuře, ochrana osobních údajů	Datové schránky, eRecept, portály občanů, mobilní identita

Studie

Automatizace výkopových prací pomocí umělé inteligence v rypadlech:

Americký startup, který je středem zájmu této studie, vytváří technologie a software pro automatizaci stavebních strojů, zejména bagrů. Cílem je zatraktivnit stavebnictví pro mladé pracovníky tím, že nabídne robotická řešení pro jeho rozvíjející se potřeby. (ARTIFICIAL INTELLIGENCE - BASED VEHICULAR AUTOMATION FITTED TO EXCAVATORS TO AUTOMATE TRENCHING (ID6), 2023)

Robotický systém pro paletizaci a depaletizaci produktů:

Roboti nyní "vidí" díky vynalézavé technologii 3D senzorů dánské společnosti, uvádí studie. Tato technologie eliminuje potřebu nočních směn a zlepšuje zdraví pracovníků tím, že umožňuje paletizaci a depaletizaci zboží na vyžádání bez nutnosti skladování. (Robotic system for palletising and depalletising products, 2023)

Chytré kontrolní centrum pro bezpečnost a zdraví při práci:

V této studii je hodnoceno multifunkční komunikační a datové analytické centrum, které dokumentuje údaje týkající se bezpečnosti a ochrany zdraví při práci, včetně interních kontrol, auditů, incidentů a vnějších faktorů. Cílem je řídit bezpečnost a pohodu zaměstnanců proaktivně i reaktivně. (An OSH smart control centre: smart digital systems for improving workers' safety and health, 2024)

Chytrý náramek pro analýzu dat v reálném čase v oblasti zdraví a bezpečnosti:

Studie se zaměřuje na využití chytrých nositelných technologií, jako jsou náramky, ke sledování fyzického zdraví zaměstnanců a pracovního prostředí v reálném čase. Tato technologie umožňuje zlepšit ergonomii pracoviště a identifikovat pravděpodobná rizika. (SMART DIGITAL SYSTEMS FOR IMPROVING WORKERS' SAFETY AND HEALTH, 2024)

Chytrá čelenka pro monitorování rizika únavy:

V této studii je zkoumáno použití chytrých čelenek, které sledují míru únavy zaměstnanců. Tyto pomůcky mohou zvýšit celkovou bezpečnost na pracovišti a monitorováním fyziologických signálů pomoci předcházet nehodám způsobeným únavou. (SMART DIGITAL SYSTEMS FOR IMPROVING WORKERS' SAFETY AND HEALTH, 2023-2025)

Rozpoznávání událostí pro zlepšení řízení bezpečnosti:

Studie popisuje systém, který pomocí počítačového vidění a umělé inteligence odhaluje nebezpečné události a nehody na pracovišti. Tento přístup zlepšuje celkové řízení bezpečnosti a umožňuje rychleji reagovat na možná rizika. (Event recognition for improved safety management: smart digital systems for improving workers' safety and health, 2024)

4.2 Propojení konceptu Průmyslu 4.0, digitalizace a udržitelného rozvoje

Efektivita, konkurenceschopnost a sociální a environmentální odpovědnost jsou v dnešní ekonomice stále důležitější. Nové paradigma pro růst veřejných institucí a průmyslových podniků se v této souvislosti utváří díky konvergenci tří důležitých témat: digitalizace, Průmyslu 4.0 a udržitelného rozvoje.

Čtvrtá průmyslová revoluce, známá jako Průmysl 4.0, je definována úzkou integrací digitálního a fyzického světa prostřednictvím cloud computingu, umělé inteligence, strojového učení, kyberneticko-fyzických systémů a digitálních dvojčat. Sběr, přenos, analýzu a využití dat v reálném čase umožňují tyto technologie, které automatizují postupy, maximalizují výkon a zvyšují adaptabilitu průmyslových systémů.

V širším slova smyslu zahrnuje digitalizace nejen technologický pokrok, ale také přechod na elektronická řešení v oblasti obchodu, komunikace se zákazníky, logistiky a administrativy. Digitalizované prostředí podporuje inovace v celém hodnotovém řetězci a vytváří základ pro efektivní řízení podnikových procesů. Z hlediska řízení organizace umožňuje prediktivní plánování, rozhodování založené na datech a lepší sledování výkonnosti.

V současném ekonomickém a sociálním klimatu hraje významnou roli také udržitelný rozvoj, který zdůrazňuje rovnováhu mezi ekonomickými, sociálními a environmentálními složkami činnosti organizace. Cíle environmentální udržitelnosti lze naplnit například snížením spotřeby energie a materiálu, předvídáním oprav zařízení, minimalizací odpadů nebo sledováním emisí uhlíku, a to zejména díky technologiím Průmyslu 4.0 a digitalizaci. Přesné vyhodnocení vlivu provozu na životní prostředí a následné přijetí strategií zmírnění dopadů je možné díky využití velkých dat a analytických nástrojů.

Pozitivní sociální dopady lze spatřovat také v lepších pracovních podmínkách, menším množství rizik při práci, používání asistenčních technologií a větší odpovědnosti a transparentnosti vůči komunitám a zaměstnancům. Z ekonomické udržitelnosti vyplývá dlouhodobý rozvoj organizací, zvýšená konkurenceschopnost a efektivní řízení rizik.

Spojení mezi digitalizací, Průmyslem 4.0 a udržitelností tedy nezahrnuje pouze nové technologie, ale také změnu pohledu na to, jak dosáhnout rovnováhy mezi odpovědností a výkonností. Samotné organizace i celá společnost z této synergie hodně získají. (The future of work: How innovation and digitalization re-shape the workplace)

5 DIGITALIZACE V OZBROJENÝCH SILÁCH

Vojenské operace 21. století jsou stále více závislé na digitálních technologiích, které radikálně mění způsob velení, logistiky, výcviku a bojových operací. Proces integrace velkých dat, pokročilých senzorů, automatizovaných systémů, umělé inteligence a moderních informačních technologií do vojenského prostředí s cílem zvýšit efektivitu, bezpečnost a rychlost rozhodování v dynamických bojových situacích je znám jako „digitalizace ozbrojených sil“.

Moderní armády po celém světě zjišťují, že digitalizace není jen konkurenční výhodou, ale také nutností vzhledem ke složitosti bojů a rychlému vývoji technologií. Investice do oblastí, jako je kybernetická bezpečnost, bezpilotní systémy, bojovní roboti, satelitní komunikace a sofistikované analytické nástroje pro zpravodajství, odrážejí tento trend.

Hlavní cíle digitalizace v ozbrojených silách

- **Zvýšení operační efektivity** – Lepší koordinace a rychlejší reakce na hrozby jsou možné díky rychlejšímu toku informací mezi bojovými jednotkami, velením a spojenci.
- **Zlepšení situačního povědomí** – Díky integraci senzorů, satelitních systémů a umělé inteligence dokáže detekovat pohyb protivníka, analyzovat topografii a poskytovat předpovědi nebezpečí v reálném čase.
- **Optimalizace logistiky a údržby** – Metody prediktivní údržby, bezpilotní zásobovací letouny a automatizované systémy sledování zásob snižují možnost selhání kritického vybavení během konfliktu.
- **Zvýšení bezpečnosti a ochrany vojenského personálu** – Aby se snížila možnost zranění na bojišti, používají se moderní ochranná opatření, kybernetická bezpečnost a technologie.
- **Zlepšení výcviku a přípravy vojáků** – Umělá inteligence, rozšířená realita a virtuální simulace umožňují realistický výcvik bez nutnosti přítomnosti na místě.

5.1 Digitalizace systému velení a řízení

Digitalizace systému velení a řízení v AČR využívá nejmodernějších informačních a komunikačních technologií k urychlení a zlepšení rozhodování, interoperability a schopnosti velení v dynamickém bojovém prostředí, a to je klíčem k modernizaci a zvýšení efektivity Armády České republiky.

Hlavní cíle digitalizace systému velení a řízení:

1. **Zrychlení rozhodovacích procesů** – Rychlejší reakce na hrozby je možná díky automatizaci shromažďování, zpracování a sdílení informací.
2. **Interoperabilita s NATO a spojenci** – Efektivní spolupráci v zahraničních operacích umožňuje kompatibilita s aliančními systémy.
3. **Zvýšení bezpečnosti a ochrany dat** – Kybernetická bezpečnost má zásadní význam pro zabezpečení komunikačních a řídicích systémů.
4. **Využití umělé inteligence a strojového učení** – Automatizovaná analýza bojových scénářů a predikce vývoje situace.

Klíčové prvky digitalizace velení a řízení

Systém C4ISTAR

Špičkový vojenský systém velení, řízení a průzkumu C4ISTAR nabízí efektivní sběr, zpracování a šíření dat v reálném čase. Je nezbytný pro současné bojové operace a umožňuje velitelským strukturám rychle reagovat na měnící se okolnosti.

- **C4 – Command, Control, Communications, Computers** (Velení, Řízení, Komunikace, Počítače)
- **I – Intelligence** (Zpravodajství)
- **S – Surveillance** (Sledování)
- **TAR – Target Acquisition and Reconnaissance** (Zaměřování cílů a Průzkum)

Komponenty C4ISTAR

1. Velení a řízení (C4)

Patří sem počítačová velitelská centra, která usnadňují rychlé plánování a koordinaci vojenských akcí. Velitelské struktury mohou lépe analyzovat dostupná data a řídit síly na bojišti s využitím automatizovaných rozhodovacích technologií. Další důležitou složkou velení je MOKYS (mobilní komunikační a informační systém), který usnadňuje bezpečnou a šifrovanou komunikaci mezi polními jednotkami a veliteli.

2. Zpravodajství a průzkum (ISTAR)

Využívá špičkovou technologii, která dokáže sledovat pohyb nepřítele a analyzovat bojové podmínky v reálném čase. K nepřetržitému sledování situace v zájmové oblasti se využívají například satelity a bezpilotní letouny (drony). Zatímco signální a elektronické zpravodajství (SIGINT a ELINT) se soustředí na sběr a analýzu komunikace protivníka, pokročilé senzory a radary umožňují sledovat a identifikovat objekty i v obtížných situacích.

3. Komunikace a kybernetická bezpečnost

Pro zajištění bezpečné a spolehlivé komunikace mezi spojeneckými silami provozuje armáda vysoce šifrované sítě, jako je například Federated Mission Network (FMN) NATO. Vzhledem k rostoucí hrozbě kybernetických útoků je kladen důraz na ochranu informačních systémů, jejichž zabezpečení zajišťují specializované kybernetické jednotky. Kromě toho je díky rostoucímu využívání cloud computingu a umělé inteligence umožněna dokonalejší analýza dat a předvídání budoucího vývoje války.



Obrázek 5 – Systémy C4ISTAR pozemních sil (Systémy C4ISTAR pozemních sil)

Díky integraci těchto klíčových oblastí nabízí C4ISTAR Armádě ČR komplexní schopnosti pro efektivní řízení vojenských operací, rychlé zpracování informací a bezpečnou výměnu informací s aliančními partnery. V důsledku toho je tento systém nezbytný pro modernizaci armády a její obranyschopnost v digitální éře. (Koncepce výstavby Armády České republiky 2035, 2024)

5.2 Kybernetická bezpečnost a elektronický boj v Armádě ČR

V současném vojenském prostředí jsou elektronický boj (EW) a kybernetická bezpečnost zásadní pro ochranu informačních systémů a komunikací před nepřátelskými průniky a rušením. Armáda České republiky proto klade velký důraz na budování svých schopností v těchto oblastech, aby byla schopna provádět operace v případě, že dojde ke snahám o narušení nebo zneužití digitální infrastruktury.

Kybernetická bezpečnost v AČR

V armádě se kybernetická bezpečnost týká ochrany zpravodajských databází, velitelských a řídicích systémů, vojenských sítí a dalších online platforem před online útoky. V této oblasti se používají jak ofenzivní, tak defenzivní kybernetické operace.

Vojenské jednotky zaměřené na kybernetickou bezpečnost monitorují síťový provoz, odhalují a eliminují kybernetické hrozby a brání se proti malwaru a útokům hackerů. Klíčovou organizací v této oblasti je Národní centrum kybernetických operací (NCKO), divize Vojenské zpravodajské služby, která se specializuje na ofenzivní i defenzivní kybernetické operace.

Ochrana životně důležitých vojenských sítí, včetně autonomních zbraňových systémů, velitelských systémů C4ISTAR a šifrovaných komunikačních kanálů, je jedním z hlavních cílů kybernetické bezpečnosti. Současné vojenské sítě využívají umělou inteligenci a nejmodernější šifrovací technologie k identifikaci a zastavení pochybného chování dříve, než způsobí škodu.

Elektronický boj (Electronic Warfare)

Využití elektromagnetického spektra k rušení zbraňových a komunikačních systémů nepřítele a zároveň k ochraně vlastních systémů před rušením je hlavním cílem elektronického boje.

Existují tři hlavní kategorie elektronického boje:

1. Příkladem elektronického boje je aktivní rušení, podvržení signálu a rušení radarových a komunikačních zařízení protivníka. Například radarové systémy mohou být oslepeny silným elektromagnetickým impulzem nebo mohou být rušeny rádiové frekvence, aby se ztížila schopnost protivníka účinně komunikovat.
2. Termín „elektronická ochrana“ se vztahuje k ochranným opatřením proti kybernetickým útokům a rušení vašich vlastních elektronických systémů. Ta

obsahuje sofistikované filtry, které mohou blokovat nebezpečné signály, silné šifrování komunikace a technologii proti rušení.

3. Monitorování a analýza elektromagnetického spektra za účelem nalezení nepřátelských signálů, určení jejich původu a využití dat pro podporu vojenských operací se označuje jako elektronická podpora.

V elektronickém boji se používají specializované systémy umístěné na zemi, ve vzduchu a na moři. Pozemní síly mohou například využívat rušičky k ničení dálkově řízených výbušných zařízení, zatímco vojenské drony mohou vyhledávat a rušit nepřátelské vysílání. (Security and Military Relevancies of Digitisation, Globalisation and Cyberspace, 2021)

Bezpilotní prostředky (drony)

- Bojové i průzkumné činnosti jsou do značné míry závislé na systémech epilot:
- Drony používané k průzkumu, jako je RQ-11 Raven, malý ručně odpalovaný dron, který používá pěchota. Bojové drony, jako je MQ-9 Reaper, který může bombardovat a nést řízené střely. Drony používané v elektronickém boji, například ALTIUS-600M, které mohou rušit nepřátelské radary a komunikaci.



Obrázek 6 – RQ-11 Raven (RQ-11B Raven, © 2025 Military Advantage)



Obrázek 7 – MQ-9 Reaper (Reaper Drones: The new close Air Support Weapon, 2017)

Bojovní roboti

Robotické platformy a autonomní systémy se stále vyvíjejí a testují. Bezpilotní pozemní vozidla (UGV) jsou robotická bojová vozidla, jako je ruský Uran-9 nebo Ripsaw M5. Ačkoli nejsou speciálně konstruována pro boj, lze je využít pro přepravu vybavení nebo sledování. Boston Dynamics Spot. Autonomní zbraňové systémy, jako je izraelský dron Harpy, který dokáže sám vyhledávat a ničit cíle.



Obrázek 9 – Ripsaw M5 (Ripsaw M5: Robotická hvězda akčních filmů pro americkou armádu, 2019)



Obrázek 8 – Ruský Uran-9 (Ruská armáda zavedla do výzbroje bojové roboty Uran-9, © 2018 - 2025 Armadninoviny.cz)

Propojení kybernetické bezpečnosti a elektronického boje

Kromě skutečného bojiště probíhají vojenské aktivity také v kyberprostoru a elektromagnetickém spektru. Úzký vztah mezi kybernetickou bezpečností a elektronickým bojem je tedy klíčový.

Integrované systémy kybernetické a elektronické obrany, které se používají v moderních vojenských technologiích, jsou schopny automaticky identifikovat snahy o rušení signálu, infiltraci nebo narušení komunikace. Díky tomu jsou vojenské síly schopny udržet si informační převahu nad nepřítelem a rychle reagovat na hrozby.

Armáda České republiky může díky sofistikovaným kybernetickým a elektronickým nástrojům úspěšně bránit svou digitální infrastrukturu, provádět elektronické útoky na systémy protivníka a snižovat vlastní zranitelnost na současném digitálním bojišti. (Kybernetická bezpečnost počítačových systémů AČR, 2024)

Digitalizace logistiky a výcviku v Armádě ČR

Armáda modernizuje nejen své zbraňové a velitelské systémy, ale také logistické a výcvikové systémy, kde je digitalizace klíčová. Moderní technologie umožňují zrychlit, zjednodušit a automatizovat postupy, což zvyšuje operační schopnosti a připravenost vojenských sil.

Digitalizace logistiky

Řízení zásob, přeprava, údržba vybavení a zabezpečení operačních jednotek, to vše projde v důsledku digitalizace logistiky Armády České republiky významnými změnami. Munice, benzín, náhradní díly a zásoby potravin mohou být řízeny efektivněji díky automatizovaným skladovým systémům, jako jsou informační platformy typu SAP, které umožňují přesné sledování zboží v reálném čase. Stále častěji se využívají čipy RFID a senzory internetu věcí, které maximalizují přehled o zásobách a jejich řízení, umožňují automatizovanou identifikaci skladových položek a zefektivňují logistické postupy.

Významnou součástí digitalizace je modernizace řízení a plánování vojenské dopravy. Geolokační technologie a sofistikované plánovací algoritmy umožňují efektivně monitorovat operace vojenských konvojů, snižovat pravděpodobnost ztrát a zlepšovat trasy. Za účelem zvýšení flexibility a úspory provozních nákladů automatizují systémy řízení dopravy, jako je systém řízení dopravy (TMS), plánování přepravních operací pomocí sofistikovaných analytických metod.

Digitalizace se projevuje i v oblasti vojenské údržby, kde se používají techniky prediktivní diagnostiky. Senzorové technologie a analýza velkých dat umožňují efektivně sledovat technický stav zbraní a vozidel, odhalovat možné problémy a s předstihem plánovat potřebné opravy. Prediktivní údržba tak pomáhá zvyšovat provozuschopnost vojenské techniky a snižovat prostoje, což zlepšuje bojovou připravenost armády.

Technologie blockchain se v logistických operacích používá stále častěji, aby se zvýšila kybernetická bezpečnost a transparentnost. Decentralizované databáze snižují možnost manipulace se záznamy, umožňují bezpečné řízení logistických dodávek a nabízejí silnou obranu proti online útokům. Při využití těchto technologií ve vojenské logistice se zefektivňuje řízení dodavatelského řetězce, chrání se citlivé údaje a je zaručena vysoká míra spolehlivosti.

Při zvážení všech okolností se digitalizací vojenské logistiky výrazně zvyšuje efektivita, přesnost a bezpečnost dodavatelských postupů. Strategickou samostatnost a bojovou připravenost Armády ČR posilují moderní technologie, které umožňují optimalizovat skladové hospodářství, předvídat opravy techniky a efektivně organizovat přepravu vojenského materiálu. (Dlouhodobý výhled pro obranu 2035, 2019)

Digitalizace výcviku

Důležitou součástí modernizace ozbrojených sil je digitalizace výcviku Armády ČR, která umožňuje efektivnější, bezpečnější a realističtější přípravu vojáků na bojové operace. Využití virtuální a rozšířené reality (VR/AR) je klíčovou součástí digitalizace, protože umožňuje modelování skutečných bojových situací bez nutnosti fyzické přítomnosti na cvičišti. Tankové operace, letecké mise a boj pěchoty lze úspěšně vyučovat v urbanizovaném prostředí s využitím sofistikovaných simulací a vojáci mohou průběžně vyhodnocovat a zdokonalovat své rozhodovací techniky. Technologie rozšířené reality navíc umožňuje vizualizovat důležité informace v reálném prostředí, což má využití při výcviku taktických operací speciálních sil nebo zdravotnického personálu.

Digitalizaci výcviku výrazně napomáhá umělá inteligence, která umožňuje přizpůsobit výcvikové situace jedinečným schopnostem každého vojáka. Zařízení poháněná umělou inteligencí mohou v reálném čase vyhodnocovat výkony vojáků a dynamicky měnit náročnost výcviku, což urychluje proces učení a zrychluje získávání taktických schopností. Simulace s podporou umělé inteligence rovněž umožňují realistické chování protivníka, což výrazně zvyšuje věrnost výcviku.

Další oblastí digitalizace je využívání sofistikovaných válečných simulací, jako je například Virtual Battlespace System, který umožňuje napodobit složité vojenské operace s využitím skutečných geografických dat. Velitelé mohou s pomocí tohoto programu, který nabízí realistické scénáře v řadě bojových situací, posoudit přesnost taktických rozhodnutí. Simulace napojené na skutečná data jsou přínosné nejen při individuálním výcviku vojáků, ale také při výcviku koordinace mezi různými vojenskými jednotkami.



Obrázek 10 – Virtual Battlespace System (Virtual Battlespace 2 (VBS2),
Copyright © 2025)

Výcvik robotických systémů a bezpilotních letadel rovněž využívá současné technologie. Výcvikové programy zavádějí systémy pro ovládání a používání bezpilotních letounů a autonomních bojových platform v různých operačních podmínkách, protože tyto nástroje se stávají nezbytnou součástí současných ozbrojených sil. Kombinace rozšířené reality a pokročilých analytických nástrojů umožňuje vojákům absolvovat interaktivní výcvik, který simuluje skutečné bojové operace s využitím nejmodernějších technologií.

Dalším zásadním aspektem digitalizace výcviku je využití biometrických senzorů a analytických nástrojů k hodnocení psychické a fyzické připravenosti vojáků. Jednotliví vojáci i celé jednotky mohou být důkladně hodnoceni z hlediska výkonnosti pomocí systémů, které sledují srdeční tep, reakční časy nebo přesnost střelby. Tyto informace lze využít k úspěšné personalizaci výcviku a optimalizaci výcvikových programů tak, aby odpovídaly jedinečným požadavkům každého vojáka.

Po zvážení všech okolností lze říci, že digitalizace vojenského výcviku výrazně zvyšuje jeho efektivitu a realističnost. Výcvik v prostředí, které přesně napodobuje skutečné bojové podmínky, umožňují moderní technologie, které nabízejí i zpětnou vazbu založenou na sofistikované analýze dat. Výsledkem je vyšší úroveň připravenosti vojáků, lepší adaptabilita na neustále se měnící bojové situace a efektivnější řízení výcvikového procesu v Armádě ČR. (Umělá inteligence v bojových simulacích: Jak AI mění výcvik vojáků NATO a AČR)

V obtížných bojových situacích zlepšují pokročilé technologie efektivitu vojáků, jejich situační povědomí a ochranu. Bojovní roboti, noční vidění, bezpilotní letadla a inteligentní ochrana sluchu jsou některé z hlavních oblastí, kde má digitalizace velký dopad. Kromě toho, že inteligentní chrániče sluchu snižují pravděpodobnost poškození sluchu, usnadňují jasnou komunikaci v hlučném prostředí. Vojáci mají výhodu při bojových operacích za snížené viditelnosti díky technologiím nočního vidění a termovize. Drony pro přímé údery, elektronický boj a průzkum jsou příklady bezpilotních prostředků, které mají v dnešním konfliktu stále větší význam. A konečně vznikají autonomní systémy a bojovní roboti, kteří mají zlepšit efektivitu a bezpečnost vojenských operací.

Jednotlivým technologiím a konkrétním příkladům jejich použití v armádě se budeme podrobněji věnovat v následujících kapitolách. (The future of work: How innovation and digitalization re-shape the workplace)

Chrániče sluchu

Chytré elektronické chrániče sluchu se dnes používají v armádě, aby kromě blokování hlasitých zvuků, jako je střelba a výbuchy, zlepšily rádiovou komunikaci a šepot v okolí. Mezi příklady patří: Armády NATO používají 3M PELTOR ComTac, který funguje s rádiovou komunikací a přilbami. Taktický komunikační a ochranný systém (TCAPS) americké armády zlepšuje situační povědomí a zachovává sluch.



Obrázek 11 – 3M PELTOR (EEP-100 EU 3M PELTOR, Copyright 2025)



Obrázek 12 – Taktický komunikační a ochranný systém (TACTICAL COMMUNICATION AND PROTECTIVE SYSTEM, 2019)

Noční vidění

Digitální válka stále více zahrnuje noční vidění, které zahrnuje: Brýle pro noční vidění, jako je například AN/PVS-31 pro speciální síly. Termovizní zaměřovače, jako je FLIR Thermosight nebo Trijicon IR-HUNTER. Systémy digitální fúze, jako je například ENVG-B americké armády, které kombinují termovizi a noční vidění a poskytují optimální viditelnost ve tmě.

Nositelné technologie a digitální monitoring zdravotního stavu v ozbrojených silách

Využití nositelných technologií neboli wearables v armádě roste v důsledku digitalizace a současných technologií. Tato zařízení umožňují přímé sledování fyziologického a zdravotního stavu vojáků v terénu. Tyto technologie, které mají často podobu chytrých hodinek, opasek, náramků, senzorů zabudovaných do zařízení nebo chytrých tkanin, umožňují v reálném čase zaznamenávat a vyhodnocovat životní funkce, úroveň stresu, úroveň fyzické aktivity, hydrataci a další důležité ukazatele.

Jednou z klíčových rolí těchto zařízení je detekce neočekávaných událostí, jako je kolaps vojáka, jeho bezvědomí, rychlý pokles zdravotního stavu nebo pokles srdeční frekvence pod bezpečnou hranici. Pokud je takový scénář rozpoznán, je velitelskému stanovišti, lékařskému týmu nebo ostatním členům jednotky automaticky doručena poplašná zpráva. To umožňuje rychlou reakci a snižuje nebezpečí spojené se zpožděním pomoci.

Při vývoji nositelných technologií pro armádu se berou v úvahu náročné podmínky nasazení vojáků. Musí být schopny odolat nárazům, vodě, prachu a extrémně vysokým nebo nízkým teplotám. Tyto pomůcky se často zabudovávají přímo do vojenských uniforem jako chytré oblečení, které nejen sleduje základní operace, ale umožňuje také sledovat fyzickou únavu, míru úsilí a místo pobytu konkrétních členů jednotky.

Tyto technologie se ukázaly jako nezbytné nejen při skutečných bojových operacích, ale také při výcviku, cvičeních a lékařské péči o vojáky. Optimalizují lékařskou péči, zlepšují rozhodování na všech úrovních velení a zvyšují bezpečnost a efektivitu vojenských operací. (A Brief Overview of Digital Military Systems Used in the Armies of NATO Member Countries, 2021)

Armáda nyní testuje nebo používá řadu těchto technologií, včetně:

- Empatica E4 – nositelný náramek, který dokáže detekovat pády a sledovat elektrodermální aktivitu, teplotu kůže, úroveň stresu a srdeční tep. (Empatica, 2020)
- Hexoskin Smart Shirts – senzory na chytrých tričkách, které sledují polohu vojáka v prostoru, jeho fyzickou aktivitu, frekvenci dýchání a EKG. (Hexoskin Smart Shirts, Hexoskin © 2025)
- Garmin Tactix Delta Solar – robustní vojenské hodinky s funkcemi pro nouzová upozornění, GPS polohu, detekci nehod a sledování srdečního tepu. (Tactix® Delta - Solar Edition with Ballistics)

Tyto systémy jsou často napojeny na centrální velitelské a zdravotnické informační systémy, které zpracovávají, analyzují a vyhodnocují data pro potřeby velitelů a zdravotníků. Při použití těchto technologií se výrazně zvyšuje bezpečnost vojáků, zlepšuje se situační povědomí a umožňuje se řízení lidských zdrojů v nebezpečných a dynamických podmínkách.

Přínosy využívání těchto technologií v ozbrojených silách:

- zvýšení bezpečnosti armády díky včasné identifikaci krizových okolností.
- přímé sledování zdravotního stavu na velitelských stanovištích v reálném čase.
- lepší rozhodování na základě dat.
- prevence přetížení a vyčerpání vojáků během výcviku a operací.

- rychlejší zásah profesionálních lékařů v případě nouze. (A Brief Overview of Digital Military Systems Used in the Armies of NATO Member Countries, 2021)

Příklady využívání nositelných technologií v ozbrojených silách:

Americká armáda

Jednou z prvních organizací, která začala používat nositelné zdravotní senzory a biometrická zařízení, byla americká armáda. Např:

Projekt TALOS (Tactical Assault Light Operator Suit) (známý také jako „Iron Man suit“) integroval biometrické senzory pro sledování zdravotního stavu vojáků přímo do bojové vesty a přilby. Chytrá trička Hexoskin umožňují sledování EKG, dechové frekvence, úroveň aktivity a detekci pádů během výcviku a bojových simulací. Náramky Empatica E4 v jednotkách logistiky a zdravotnických služeb monitorují stres a zdravotní stav personálu ve stresových situacích.

Britská armáda (British Army)

Britská armáda experimentuje s několika chytrými náramky a tričky se senzory v rámci iniciativy Future Soldier, která umožňuje určit, zda voják upadl nebo ztratil vědomí. Automaticky informovat zdravotnický personál a velení. Během celých procedur sledovat teplotu, srdeční tep a úroveň stresu.

Kanadské ozbrojené síly

Aby se zabránilo přetížení armády během výcviku, používají pásy s biosenzory a chytré textilie, které kontrolují úroveň hydratace, dále sledují tepovou frekvenci a tělesnou teplotu a analyzují reakci těla na stres a cvičení.

Nizozemská armáda

V rámci iniciativy VOSS (Verbeterd Operationeel Soldaat System) hodnotí integrované nositelné systémy.

Mezi ně patří např:

- senzory pro detekci polohy a pádu
- komunikační zařízení, která přenášejí zdravotnické údaje do řídicího centra.

Digitální komunikační a ochranné systémy v osobní výstroji vojáků

Chytré a integrované osobní ochranné prostředky se používají stále častěji, protože obranný a bezpečnostní sektor je stále více digitálně propojen. Toto vybavení poskytuje nejen primární ochranu, ale také zvyšuje povědomí o situaci, usnadňuje datovou a hlasovou komunikaci a pomáhá přijímat lepší rozhodnutí v reálném čase. Příkladem takových zařízení jsou výrobky společnosti 3M, které integrují monitorování prostředí, komunikaci a ochranu sluchu.

Mezi nejvýznamnější technologie patří:

3M™ PELTOR™ Tactical Headsets a ComTac systémy – Ty nejen chrání uši vojáků před hlasitými zvuky, ale také jim umožňují poslouchat okolí tím, že bezpečně zesilují hluk na pozadí, což zlepšuje situační povědomí. Kromě toho tato zařízení usnadňují rádiovou komunikaci na bojišti a umožňují plynulé přepínání kanálů.

3M™ PELTOR™ Tactical Modular Audio System (TMAS) – Je vojenský modulární komunikační systém. Umožňuje integraci mnoha druhů komunikačních zařízení, náhlavních souprav a mikrofónů s možností digitálního přenosu řeči a dat. Modulární architektura systému umožňuje jeho přizpůsobení požadavkům mise a konkrétním okolnostem.

3M™ Scott™ CBRN Respiratory Protection – Je špičkový systém ochrany dýchacích cest, který lze použít v situacích zahrnujících chemické, biologické, radiologické a jaderné nebezpečí. Má digitálně řízené proudění vzduchu a filtrační funkce. Tato technologie výrazně zvyšuje bezpečnost jednotky v náročných podmínkách tím, že nabízí sledování účinnosti a stavu zařízení v reálném čase.

Tyto moderní technologie ukazují trend spojování datových a komunikačních schopností s osobními ochrannými prostředky, což nejen zvyšuje individuální bezpečnost, ale také umožňuje efektivnější velení a koordinaci jednotek v terénu. Digitalizace v armádě tedy neprobíhá pouze ve velitelských centrech a informačních systémech, ale pomalu se dostává i na úroveň jednotlivých vojáků, jejich výstroje a ochranných prostředků. (3M Worker Health and Safety, © 3M 2025)

6 DOPAD DIGITALIZACE NA BOZP (AUTOMATIZACE A JEJÍ Vliv NA PRACOVNÍ RIZIKA)

Jedním z hlavních prvků, které dnes mění trh práce, je digitalizace a automatizace. Digitální technologie a automatizované procesy rostou v průmyslových oblastech logistiky, administrativy a služeb. Pro bezpečnost a ochranu zdraví při práci to představuje nové obtíže i výhody. Tato kapitola se zaměřuje na to, jak automatizace ovlivňuje pracovní nebezpečí, jak je digitalizace změnila a jak je mohou současná technologická řešení odstranit.

Automatizace a změna pracovního prostředí

Povaha pracoviště a způsob provádění činností se v důsledku automatizace a digitalizace dramaticky mění. Zaměstnanci vynakládají méně fyzické námahy a vyhýbají se rizikům spojeným se zvedáním těžkých břemen a opakující se prací, protože lidskou práci nahrazují automatizované technologie. Tato tendence je patrná zejména v oblasti průmyslové výroby, logistiky a zdravotnictví, kde jsou rutinní nebo nebezpečné operace nahrazovány robotizací.

Kvůli změně na pracovišti se však objevují i nové potíže. Pracovníci mohou mít větší psychickou zátěž v důsledku toho, že musí upravit své schopnosti a naučit se používat nové technologie. Automatizace také mění charakter práce, některé profese možná zaniknou a jiné budou vyžadovat specializované znalosti. V důsledku tohoto vývoje se zvyšují nároky na školení a rekvalifikaci pracovníků. (Howard, 2019)

Nová rizika spojená s automatizací

Automatizace přispívá ke snížení běžných rizik na pracovišti, jako je fyzické poškození nebo vystavení nebezpečným materiálům, ale přináší také nová rizika. Mezi ně patří kybernetická bezpečnost, která se rychle stává klíčovou součástí bezpečnosti pracovníků. Pokud se automatizované systémy stanou terčem kybernetického útoku, který ohrozí provozní bezpečnost, mohou zaměstnanci a lidé v jejich blízkosti utrpět okamžité následky.

Dalším nebezpečím je porucha digitální technologie, která může vést k nepředvídatelným okolnostem ohrožujícím bezpečnost zaměstnanců. Robotické systémy, automobily bez řidiče a automatizované výrobní linky jsou závislé na přesném naprogramování a funkčním softwaru. Chyby mohou vést ke škodlivým situacím, které lze jen těžko předvídat nebo jim zabránit pomocí tradičních bezpečnostních opatření.

Psychosociální dopady digitalizace

Digitalizace má významný vliv na psychické zdraví zaměstnanců. Rychlé změny jsou něčím, čemu se mnoho pracovníků musí přizpůsobit, což může způsobovat stres a pocity nejistoty. Obavy ze ztráty zaměstnání v důsledku automatizace mohou mít nepříznivý vliv na motivaci a celkovou spokojenost v zaměstnání.

Větší závislost na digitálních technologiích má za následek také zvýšený tlak na výkon a průběžné sledování procesů. Protože musí udržovat vysokou úroveň výroby a přizpůsobovat se požadavkům automatizovaných systémů, mohou pracovníci na pracovištích řízených umělou inteligencí pociťovat větší psychickou zátěž.

Možnosti prevence a opatření

Má-li automatizace a digitalizace zlepšit bezpečnost práce, je třeba přijmout preventivní opatření. Zaměstnanci, kteří absolvují pravidelná školení, budou lépe vybaveni pro zacházení s novými technologiemi a pochopí jejich bezpečnostní prvky. Podniky by měly stanovit výslovné pokyny pro používání automatizovaných technologií a zajistit, aby zaměstnanci mohli v případě potřeby zasáhnout a změnit způsob jejich fungování.

Klíčová je také kontrola pracovních podmínek, která by měla zahrnovat přijetí opatření ke snížení psychického stresu. Ke zmírnění negativních důsledků digitalizace by mohla pomoci například nabídka psychologické podpory zaměstnancům nebo flexibilní pracovní doba. Aby se snížila rizika spojená s možnými kybernetickými útoky, měla by být kybernetická bezpečnost považována za prioritu.

Tendence automatizace pracovních procesů je nevyhnutelná a přináší výhody i obtíže. Vedle snižování fyzických rizik je velmi důležité mít na paměti potenciální nové hrozby, které digitalizace přináší. Úspěšná adaptace vyžaduje nalezení rovnováhy mezi dlouhodobou životaschopností pracovních podmínek, bezpečností zaměstnanců a duševním zdravím při zavádění nových technologií. (PNAS,2019)

Studie:

Dopady automatizace a digitalizace na bezpečnost a ochranu zdraví při práci jsou předmětem řady výzkumů. Tyto studie zkoumají dopady současných technologií, jako je umělá inteligence a sofistikovaní roboti, na zaměstnance, pracoviště a související rizika.

1. Kognitivní automatizace: dopad, rizika a příležitosti v oblasti BOZP

Tato studie zkoumá využití umělé inteligence při automatizaci kognitivních úkolů s důrazem na kognitivní automatizaci a její dopady na BOZP. Umělá inteligence snižuje chybovost, zvyšuje produktivitu a snižuje úzkost, která je spojena s rozhodováním. S jejím zaváděním jsou však spojeny i obavy, jako je možnost nejednoznačnosti nebo chybné interpretace výstupů těchto systémů a větší psychosociální zátěž osob, které dohlížejí na systémy UI. Zpráva navrhuje stanovit jednoznačná pravidla pro používání UI na pracovišti, poskytnout pracovníkům metodické školení a rutinně vyhodnocovat účinky na jejich zdraví a bezpečnost. (COGNITIVE AUTOMATION: IMPACT, RISKS AND OPPORTUNITIES FOR OCCUPATIONAL SAFETY AND HEALTH, 2022)

2. Studie REDECA o umělé inteligenci v BOZP

Studie klade důraz na využití umělé inteligence ke zvýšení bezpečnosti pracovníků a předcházení nehodám. Umělá inteligence je užitečným nástrojem pro monitorování pracoviště v reálném čase, identifikaci nebezpečí a předvídání škodlivých scénářů. S její implementací jsou však spojena určitá rizika, například požadavek na vysoký stupeň kybernetické bezpečnosti, protože jakékoli přerušení systému může mít za následek neštěstí nebo selhání bezpečnostních opatření. V důsledku toho studie navrhuje, aby nasazení umělé inteligence bylo podpořeno přísnou kontrolou kvality vstupních dat, otevřeností algoritmů a častými bezpečnostními audity. (AI ve službách BOZP. Co nám ukázala studie REDECA o umělé inteligenci?, 2023)

3. Pokročilá robotika a automatizace: důsledky pro BOZP

Článek zkoumá, jak rostoucí automatizace a robotizace ovlivňují BOZP, se zvláštním důrazem na bezpečnost pracovníků při práci s roboty. Robotizace přináší řadu výhod, včetně menší fyzické zátěže zaměstnanců, odstranění opakujících se činností a výrazného snížení počtu pracovních úrazů. Se spolupracující robotikou však vznikají i nová nebezpečí, kdy může dojít k nedorozumění mezi člověkem a strojem, které může vést k neštěstí. Podle zprávy by měli být zaměstnanci aktivně zapojeni do procesu zavádění nových technologií, měly by být zavedeny bezpečnostní postupy pro práci s kolaborativními roboty a bezpečnostní zařízení by měla být pravidelně testována. (Advanced robotics and automation: implications for occupational safety and health, © 2025 EU-OSHA)

4. Automatizace kognitivních úkolů: Důsledky pro BOZP

Studie se zaměřuje na to, jak automatizace kognitivních úkolů ovlivňuje psychické zdraví pracovníků a jejich schopnost rozhodovat se. Automatizace může pracovníkům pomoci soustředit se na složitější úkoly a snížit kognitivní přetížení, ale pokud nejsou systémy umělé inteligence dostatečně transparentní a zaměstnanci jim nerozumí, může to vést ke ztrátě kontroly nad rozhodovacími procesy. Z tohoto důvodu studie navrhuje zajistit, aby systémy AI byly srozumitelné a jasné a aby zaměstnanci byli dostatečně proškoleni k jejich efektivnímu používání. (Automation of cognitive and physical tasks in the health and social care sector: implications for safety and health, 2024)

7 VÝZVY A RIZIKA DIGITALIZACE BOZP

Digitalizace přináší kromě nových příležitostí také několik nebezpečí a problémů pro bezpečnost a ochranu zdraví při práci. Změny, které digitální pracoviště přináší, mají dopad nejen na technické prvky, ale také na pracovní návyky, flexibilitu a obecnou bezpečnost pracovníků. Mezi hlavní překážky patří obavy týkající se lidského faktoru, kybernetické bezpečnosti a ochrany dat.

Lidský faktor v digitálním pracovním prostředí

Způsob práce lidí se díky digitalizaci zásadně mění, což přináší i nové problémy v oblasti bezpečnosti a ochrany zdraví při práci. Vystavení zaměstnanců digitálním technologiím roste, což může mít dopad na jejich soustředění, fyzické a duševní zdraví. Digitální přetížení a kratší doba udržení pozornosti jsou dva hlavní problémy. Ztráta soustředění, nárůst počtu chyb a zvýšené riziko nehod mohou být důsledkem neustálého přecházení mezi jednotlivými činnostmi, používání mnoha programů najednou a nepřetržitého toku informací. Digitální únava je syndrom, který zhoršuje kognitivní schopnosti pracovníků a jejich schopnost adekvátně reagovat v rizikových scénářích.

Ergonomické podmínky, které se vyvíjejí s rozvojem digitálních technologií, představují další problém. Nevhodné pracovní prostředí může být důsledkem přechodu na práci s počítačem a rostoucí oblíbenosti práce na dálku, což zvyšuje riziko zdravotních problémů, jako je syndrom karpálního tunelu, nepohodlí zad a oční problémy. Pracovníci často pracují v prostředí, které nedodržuje ergonomické zásady, což má vliv na jejich výkonnost a dlouhodobé zdraví.

Ergonomické podmínky, které se vyvíjejí s rozvojem digitálních technologií, představují další problém. Nevhodné pracovní prostředí může být důsledkem přechodu na práci s počítačem a rostoucí oblíbenosti práce na dálku, což zvyšuje riziko zdravotních problémů, jako je syndrom karpálního tunelu, nepohodlí zad a oční problémy. Pracovníci často pracují v prostředí, které nedodržuje ergonomické zásady, což má vliv na jejich výkonnost a dlouhodobé zdraví.

Je třeba zavést opatření, která pomohou zaměstnancům přizpůsobit se digitálním technologiím, aby se tato nebezpečí snížila. Důležitými prvními opatřeními jsou pravidelná školení, ergonomické úpravy pracoviště a pomoc v oblasti duševního zdraví. Zaměstnavatelé by měli zaručit, aby zaměstnanci měli přístup ke školení digitálních dovedností a dostatečnou pomoc při přechodu na nové pracovní postupy. Škodlivé účinky digitalizace

na lidi na pracovišti lze zmírnit otevřenou komunikací, důrazem na spolupráci a realizací iniciativ v oblasti duševního zdraví. (Digitalizace a bezpečnost a ochrana zdraví při práci (BOZP), 2020)

Kybernetická bezpečnost jako součást BOZP

S rostoucím rozšířením digitálních technologií na pracovišti se kybernetická bezpečnost stává důležitou součástí bezpečnosti a ochrany zdraví při práci. Digitální řešení, jako jsou systémy řízení výroby, databáze uchovávající soukromé údaje zaměstnanců nebo chytré senzory dohlížející na bezpečnostní podmínky, se na moderních pracovištích stávají stále běžnějšími. To však s sebou přináší i zvýšené nebezpečí kybernetických útoků, které mohou ohrozit nejen provoz organizace, ale i osobní bezpečnost pracovníků.

Mezi největší nebezpečí patří cílené kybernetické útoky, jako je ransomware a phishing, jejichž cílem je kompromitovat organizaci nebo ukrást důvěrná data. Zaměstnanci mohou být přímo ohroženi, pokud dojde k narušení bezpečnostních systémů, například změnou údajů ze senzorů, které sledují nebezpečné prostředí. Útoky na digitální bezpečnostní prvky mohou vést k selhání ochranných opatření, nepřesnému vyhodnocení rizik nebo dokonce k nebezpečným okolnostem, které ohrožují životy a zdraví pracovníků.

Dalším problémem je neoprávněný přístup k citlivým údajům, jako jsou zprávy o nehodách, výsledky bezpečnostních auditů nebo osobní údaje zaměstnanců. Zaměstnavatelé a zaměstnanci mohou čelit právním a finančním důsledkům, pokud tato data nejsou dostatečně zabezpečena proti úniku. Organizace musí s ohledem na tyto obavy zavést důkladná bezpečnostní opatření.

Důležitými kroky jsou zavedení více faktorového ověřování, časté aktualizace bezpečnostních systémů a školení zaměstnanců v oblasti kybernetické bezpečnosti. Při práci s digitálními systémy by zaměstnanci měli být informováni o nebezpečí pokusů o phishing, o tom, jak zacházet s citlivými údaji, a o bezpečnostních protokolech. Klíčové je také šifrování dat a sledování jakékoli podivné aktivity v systému, která by mohla poukazovat na útok.

Vzhledem k tomu, že digitální rizika mohou přímo ovlivnit bezpečnost zaměstnanců, měla by být kybernetická bezpečnost považována za základní součást BOZP. Pouze kombinací technologických řešení, vhodného školení a proaktivního přístupu můžeme zaručit, že digitalizace pracoviště proběhne bezpečně a bez negativních dopadů na

zaměstnance. (Kybernetická bezpečnost ve firmách. Tři pilíře pro efektivní ochranu před kyberútoky, 2022)

Ochrana dat v digitálním pracovním prostředí

Množství citlivých údajů shromažďovaných a uchovávaných elektronicky na pracovišti v důsledku procesu digitalizace roste. Zabezpečení těchto dat je klíčové pro dodržení souladu s právními předpisy, ochranu soukromí zaměstnanců a zajištění kybernetické bezpečnosti. Podniky musí přijmout nezbytná opatření, aby snížily riziko zneužití informací, neoprávněného přístupu a úniku dat.

Důležitou součástí je dodržování zákonů, jako je obecné nařízení o ochraně osobních údajů, které stanoví přísná pravidla pro nakládání s osobními údaji zaměstnanců a jejich uchovávání. Nedodržení těchto požadavků může vést ke značným sankcím a právním důsledkům, proto je nezbytné, aby společnosti měly dobře zavedené zásady ochrany osobních údajů a s citlivými informacemi nakládaly zodpovědně.

Dalším problémem je zabezpečení dat v cloudových úložištích. Podniky široce využívají cloudové služby pro sdílení a ukládání dokumentů, což nabízí výhody z hlediska flexibility a dostupnosti. Kybernetické útoky, neoprávněný přístup a ztráta dat v důsledku technologických poruch jsou však stále možné. Proto je zásadní zavést sofistikovaná bezpečnostní opatření, jako je šifrování dat, více faktorová autentizace a časté zálohování.

S digitalizací pracoviště souvisí i využívání moderních technologií pro sledování zaměstnanců. Podniky často využívají monitorovací technologie ke sledování výkonnosti zaměstnanců, dokumentování jejich docházky do práce, a dokonce i ke sledování jejich polohy pomocí GPS. Tyto činnosti mohou narušovat soukromí zaměstnanců a představovat etická dilemata. Proto je zásadní stanovit výslovné pokyny pro používání monitorovacích systémů, aby byla zachována otevřenost a respektovány rozdíly mezi ochranou údajů a monitorováním výkonu.

Účinná ochrana dat na digitálním pracovišti vyžaduje kombinaci organizačních, právních a technických ochranných opatření. Aby bylo zaručeno bezpečné nakládání s citlivými údaji, měly by podniky investovat do moderních technologií, školit zaměstnance v oblasti ochrany údajů a pravidelně aktualizovat své bezpečnostní zásady. Pouze komplexní strategie pomůže organizacím snížit nebezpečí spojená s digitalizací a nabídnout svým zaměstnancům bezpečné pracovní prostředí. (Digitalizace a bezpečnost a ochrana zdraví při

práci (BOZP), 2020) (Smart digital systems: implications for occupational safety and health, 2025)

8 TRENDY A BUDOUCNOST DIGITALIZACE V OBLASTI BOZP

V oblasti bezpečnosti a ochrany zdraví při práci postupuje digitalizace, která s sebou přináší kreativní způsoby, jak snížit počet pracovních úrazů, lépe řídit rizika a zlepšit pracovní podmínky. V této kapitole bude představen současný vývoj v oblasti digitalizace BOZP a možné budoucí směry.

8.1 Trendy v digitalizaci BOZP

Internet věcí a chytré senzory

Chytré senzory a internet věcí umožňují průběžné sledování zdraví pracovníků a pracoviště. Polohu pracovníků a jejich fyziologické charakteristiky, jako je srdeční tep, sledují chytré přilby, vesty nebo náramky, které je také upozorňují na potenciálně nebezpečné stavy, jako je únava nebo přehřátí. Díky detekci nebezpečných materiálů, úniku plynu, vibrací nebo hluku mohou senzory na pracovišti pomoci snížit dlouhodobé vystavení rizikovým faktorům. Průmyslové provozy používají systémy prevence kolizí, které upozorňují zaměstnance a zařízení na potenciální nebezpečí.

Tyto technologie umožňují sledování a analýzu dat v reálném čase, což zvyšuje bezpečnost na pracovišti tím, že umožňuje rychleji reagovat na možné hrozby. (Bude v budoucnu BOZP řešit i naši duševní pohodu? Trendy bezpečnosti a ochrany zdraví při práci tomu nasvědčují, 2020)

Umělá inteligence a prediktivní analýza

Analýzou nebezpečí na základě minulých údajů a současných okolností pomáhají systémy umělé inteligence předcházet pracovním úrazům. Prediktivní údržba s využitím umělé inteligence umožňuje analyzovat data ze senzorů internetu věcí s cílem identifikovat problémy se stroji a zastavit nehody způsobené technologickými problémy. Kromě toho umělá inteligence umožňuje analyzovat videodata a identifikovat nebezpečné chování pracovníků, jako je nerespektování bezpečnostních pokynů, a indikovat potřebu rehabilitace. Kromě toho umělá inteligence automatizuje tvorbu bezpečnostních zpráv, které nabízejí shrnutí BOZP v podniku a doporučují opatření ke zvýšení bezpečnosti.

Využití AI v oblasti BOZP umožňuje efektivněji identifikovat a řídit rizika, což snižuje počet nemocí z povolání a úrazů. (Digitalizace a dynamické hodnocení rizik jako vize budoucnosti, 2022)

Rozšířená a virtuální realita (AR/VR) v BOZP školení

Školení pracovníků v oblasti BOZP je výrazně inovováno digitálními technologiemi. Školení zaměstnanců v bezpečném virtuálním prostředí a simulaci nebezpečných scénářů umožňuje virtuální realita. Pomocí rozšířené reality, například chytrých brýlí, mohou zaměstnanci získávat interaktivní bezpečnostní informace v reálném čase.

Tyto technologie zvyšují efektivitu školení a připravenost zaměstnanců na krizové situace. (Školení BOZP a PO ve virtuální realitě, © 2025 VR Education)

Digitální pracovní checklisty a mobilní aplikace

Digitální řešení, která usnadňují řízení rizik a bezpečnostní kontroly, postupně nahrazují papírové dokumenty. Zaměstnanci mohou pomocí mobilních aplikací ve svých chytrých telefonech přímo hlásit nebezpečné situace. Automatizované kontrolní seznamy odstraňují nutnost ručního vyplňování formulářů a zaručují rychlé a přesné kontroly BOZP. Digitální dokumentace navíc odstraňuje problémy se ztracenými nebo neaktuálními záznamy a usnadňuje přístup k bezpečnostním normám. Díky digitalizaci těchto postupů lze bezpečnostní normy plnit přesněji a efektivněji. (Elektronické nástroje v oblasti BOZP, © 2025 EU-OSHA)

8.2 Budoucnost digitalizace BOZP

Plná automatizace BOZP procesů

V budoucnu budou kontroly BOZP prováděny v reálném čase pomocí inteligentních kamer a senzorů ve zcela automatizovaných systémech. Umělá inteligence automaticky rozpozná, vyhodnotí a doporučí opatření ke zvýšení bezpečnosti. Robotická zařízení a drony budou dohlížet na nebezpečná místa, jako jsou chemická zařízení a staveniště.

Díky této automatizaci se zvýší účinnost bezpečnostních postupů a sníží se počet lidských chyb.

Pokročilá personalizace ochrany pracovníků

K přizpůsobení bezpečnostních opatření jedinečným požadavkům každého zaměstnance se bude používat umělá inteligence a analýza biometrických dat. Optimalizace pracovních podmínek a snížení nebezpečí přetížení bude umožněno dynamickým přizpůsobením pracovní doby na základě aktuálního zdravotního stavu zaměstnanců. Na základě toho, jak je člověk unavený, budou počítače schopny navrhnout přestávky nebo

změny pracovního tempa. Využití těchto řešení na míru pomůže zvýšit bezpečnost práce a snížit počet nemocí z povolání a pracovních úrazů. (Digitalizace a dynamické hodnocení rizik jako vize budoucnosti, 2022)

Trendy a budoucnost digitalizace BOZP: případ společnosti Virtubea

V této kapitole je užitečné uvést konkrétní příklad podniku, který se specializuje na digitalizaci BOZP a nabízí v této oblasti špičková řešení. Jedním z takových podniků je Virtubea, který se specializuje na vytváření digitálních nástrojů pro efektivní správu BOZP v podnicích všech velikostí a odvětví. Jejich strategie je v souladu se současnými trendy digitalizace, jako je využívání platform cloud computingu, mobilních aplikací nebo očekávané spojení rozšířené reality a umělé inteligence. Ve výsledku se jedná o podnik, který může ukázat, jak lze digitalizaci využít k efektivnímu řízení bezpečnosti práce a jaké perspektivy představuje pro budoucí ochranu zdraví zaměstnanců.

Vytváření digitálních řešení v oblasti bezpečnosti a ochrany zdraví při práci je oblastí, které se společnost Virtubea věnuje. Její zboží a služby jsou určeny ke zvýšení bezpečnosti pracovníků a urychlení postupů v oblasti BOZP.

Digitální řešení BOZP od společnosti Virtubea

- **Virtubea Safety Manager**

Tato platforma umožňuje komplexní správu dokumentace BOZP, školení a auditů. Zaměstnavatelé mohou lépe plnit interní normy a zákonné povinnosti díky centralizovanému systému, který jim poskytuje komplexní přehled o bezpečnosti práce.

- **Virtubea Training Platform**

Platformu pro online školení zaměstnanců v oblasti BOZP poskytuje společnost Virtubea. Interaktivní hodnocení a kurzy zaručují efektivní výuku a umožňují sledovat rozvoj každého pracovníka.

- **Virtubea Incident Reporting Tool**

Tato aplikace umožňuje rychle a efektivně hlásit problémy na pracovišti. Mobilní aplikace usnadňuje zaměstnancům hlášení problémů a zaručuje rychlou reakci a analýzu příčin.

- **Virtubea Risk Assessment Module**

Potenciální nebezpečí na pracovišti lze identifikovat a analyzovat díky modulu pro hodnocení rizik. To umožňuje přijmout opatření ke snížení nebezpečí a zajistit bezpečnost pracovníků.

Budoucnost digitalizace BOZP s Virtubea

Společnost Virtubea neustále inovuje své výrobky, aby zvýšila požadavky na bezpečnost práce. Hodlá využívat nejmodernější technologie, jako je rozšířená realita pro interaktivní školení a umělá inteligence pro prediktivní hodnocení rizik. Tento vývoj má sílu zlepšit ochranu pracovníků a způsobit revoluci v přístupu k BOZP.

9 DÍLČÍ ZÁVĚR

Digitální technologie zásadně mění podobu řízení bezpečnosti a ochrany zdraví při práci (BOZP). Vývoj v oblasti Průmyslu 4.0 a souvisejících nástrojů přináší nové možnosti, jak efektivněji předcházet rizikům, monitorovat pracovní prostředí a zajišťovat zdraví a bezpečí zaměstnanců v reálném čase. S tímto vývojem však přicházejí i nové výzvy, které vyžadují komplexní přístup, odborné zázemí a zohlednění legislativních a etických aspektů.

Významnými technologiemi jsou **internet věcí**, umožňující propojení senzorů a zařízení pro sběr dat přímo z pracovního prostředí, a **umělá inteligence**, která dokáže tato data analyzovat a předvídat vznik rizikových situací. **Big Data** se uplatňují při vyhodnocování trendů úrazovosti nebo odhalování opakujících se nebezpečných jevů. **Cloudová řešení** pak poskytují prostor pro bezpečné sdílení a zálohování důležitých informací, zatímco **digitální dvojčata** umožňují simulaci reálných provozních podmínek pro testování bezpečnostních opatření.

Zájem je věnován také **blockchainu**, který může přinést vyšší míru transparentnosti a důvěry při vedení auditních záznamů nebo zaznamenávání bezpečnostních školení. Důležitou roli hraje **kybernetická bezpečnost**, protože většina digitálních řešení pracuje s osobními údaji zaměstnanců a citlivými informacemi, jejichž únik může mít závažné následky nejen právní, ale i reputační.

Teoretický rámec zahrnoval rovněž příklady dobré praxe ze zahraničí, zejména z prostředí ozbrojených složek, které patří mezi lídry ve využívání digitálních technologií pro ochranu života a zdraví personálu. Nositelná elektronika, chytré senzory, AR/VR nástroje nebo systémy detekující stres a fyzickou zátěž v reálném čase se ukazují jako účinné prostředky pro zvýšení bezpečnosti, a to i ve vysoce rizikových podmínkách.

Na základě zkoumání dostupné odborné literatury, technologických trendů a mezinárodních přístupů bylo potvrzeno, že digitalizace představuje účinný nástroj ke zvyšování úrovně BOZP. Je však třeba ji vnímat jako komplexní proces, který zahrnuje nejen technologické, ale i organizační, legislativní a lidské faktory. Nezbytné je důsledné plánování, osvěta, vzdělávání pracovníků a zajištění souladu se zákonnými normami a standardy.

II. PRAKTICKÁ ČÁST

10 ŘÍZENÝ ROZHOVOR

V rámci výzkumné části práce byly realizovány řízené rozhovory se zástupci firem, které se aktivně zabývají implementací prvků digitalizace, a to zejména v oblasti bezpečnosti a ochrany zdraví při práci. Cílem těchto rozhovorů bylo získat praktický vhled do způsobů zavádění digitálních nástrojů, jejich přínosů i možných překážek v reálném firemním prostředí. Tato kvalitativní metoda byla zvolena jako doplněk k dotazníkovému šetření s cílem obohatit získané poznatky o konkrétní zkušenosti a názory odborníků z praxe.

Rozhovory probíhaly podle předem připravené osnovy, která však umožňovala volnější formu vedení diskuse tak, aby bylo možné zachytit individuální přístupy, firemní specifika a hodnotná doporučení pro další organizace. Respondenti zastupovali společnosti působící v oblastech průmyslu, technologií a BOZP, které již s digitalizací určité zkušenosti mají nebo ji aktuálně zavádějí.

Výstupy z těchto rozhovorů slouží jako důležité doplnění analytické části práce. Pomáhají lépe pochopit faktory úspěchu i bariéry digitalizačních projektů v oblasti BOZP a přispívají k formulaci návrhů a doporučení pro další firmy, které se chtějí touto cestou vydat.

Rozhovor s výrobcem chytrých OOPP (osobních ochranných pracovních prostředků)

Rozhovor byl veden s odborníkem ze společnosti specializující se na vývoj a výrobu inteligentních technologií pro zvyšování bezpečnosti a ochrany zdraví při práci. Cílem rozhovoru bylo získat přehled o aktuálních trendech, míře zájmu ze strany firem a identifikovat překážky při zavádění těchto produktů do praxe.

(Celý rozhovor je pro účely diplomové práce anonymizován.)

Autor DP: V posledních letech sledujeme rostoucí zájem o tzv. chytré osobní ochranné pracovní prostředky. Mohl byste nám přiblížit, jaké produkty aktuálně spadají do této kategorie a jaké jsou jejich hlavní přínosy pro oblast bezpečnosti práce?

Výrobce: Mezi nejčastěji používané chytré OOPP patří například chytré brýle s rozšířenou realitou, které zobrazují pracovníkům důležité informace přímo v zorném poli – například bezpečnostní pokyny nebo varování před riziky. Dále pak chytrá sluchátka umožňující obousměrnou komunikaci i v hlučném prostředí a zároveň sloužící k ochraně sluchu. Nabízíme také inteligentní rukavice se senzory detekujícími vibrace, teplotu či

nebezpečné látky, a ochranné vesty s biometrickými čidly, které monitorují fyziologické parametry pracovníků, jako je srdeční tep, tělesná teplota nebo míra únavy.

Autor DP: Jaký je podle Vaší zkušenosti aktuální zájem ze strany firem o zavádění těchto technologií do praxe?

Výrobce: Zájem postupně roste, zejména ve velkých společnostech působících v odvětvích, jako je energetika, chemický průmysl, stavebnictví či logistika. Firmy si uvědomují, že investice do chytrých OOPP mohou výrazně přispět ke snížení rizika pracovních úrazů, a tím i ke zvýšení produktivity a snížení nákladů na nemocnost a fluktuaci zaměstnanců. Zároveň se snaží být konkurenceschopné a využívat moderní přístupy v oblasti řízení BOZP.

Autor DP: Jaké překážky vnímáte při prosazování těchto inovativních řešení v praxi?

Výrobce: Mezi hlavní bariéry patří:

- Vysoké pořizovací náklady, které mohou být limitující zejména pro malé a střední podniky.
- Skepticismus nebo odpor ze strany zaměstnanců, kteří mají obavy ze ztráty soukromí či nekomfortního nošení technologií.
- Nedostatečná legislativní opora, kdy platné normy a předpisy v oblasti BOZP zatím nepočítají s využitím pokročilých technologií.
- Problémy s integrací do stávajících procesů a IT systémů firem.

Autor DP: Máte pro zaměstnavatele, kteří o implementaci chytrých OOPP uvažují, nějaká doporučení nebo osvědčené postupy?

Výrobce:

1. Zahájit pilotní projekt v konkrétní provozní jednotce – vyhodnotit funkčnost, komfort a přínosy.

2. Zapojit zaměstnance do výběru a testování – aby technologie přijali jako nástroj podpory, nikoliv kontroly.

3. Konzultovat implementaci s odborníky na BOZP a IT, případně využít služeb externích poradců.

4. Zaměřit se na dlouhodobou návratnost investice – i když jsou náklady vyšší, prevence vážného úrazu nebo nehody se ekonomicky i lidsky vyplatí.

Autor DP: Děkuji za podnětný rozhovor a věřím, že chytré OOPP najdou své pevné místo v moderním systému BOZP.

Výrobce: Děkuji i já. Věříme, že technologie mají pracovníky chránit, nikoli omezovat – a právě v tom vidíme jejich největší potenciál.

Závěr: Rozhovor poukázal na dynamicky se rozvíjející oblast chytrých OOPP, která má potenciál významně přispět ke zvyšování úrovně BOZP ve firmách. Navzdory technologickému pokroku však implementace těchto řešení naráží na řadu praktických bariér, zejména ekonomického a legislativního charakteru. Do budoucna bude klíčové propojit technologické inovace s reálnými potřebami zaměstnanců, zajistit aktivní účast managementu a systematicky vzdělávat v oblasti moderních nástrojů ochrany zdraví při práci.

Rozhovor s výrobcem VR/AR nástrojů pro bezpečnostní školení

Rozhovor byl veden s odborníkem ze společnosti vyvíjející výukové simulace na bázi virtuální a rozšířené reality, které slouží jako inovativní nástroj pro vzdělávání v oblasti bezpečnosti a ochrany zdraví při práci (BOZP), požární ochrany a poskytování první pomoci. Cílem rozhovoru bylo zjistit, jaké požadavky organizace na tato řešení mají, s jakými problémy se výrobci při vývoji potýkají a jaké postupy doporučují pro úspěšné zavedení těchto technologií do praxe.

(Rozhovor je pro účely diplomové práce anonymizován.)

Autor DP: Mohl byste na úvod přiblížit, s jakými požadavky se na vás organizace nejčastěji obracejí v souvislosti s vývojem VR a AR nástrojů pro oblast BOZP?

Výrobce: Firmy nás nejčastěji oslovují s cílem zefektivnit školení zaměstnanců, zvýšit jejich pozornost a zapojení během výuky a zároveň vytvořit bezpečné prostředí pro nácvik krizových situací. V rámci BOZP jde typicky o simulace pohybu na rizikových pracovištích, rozpoznávání nebezpečí nebo evakuace. V oblasti požární ochrany vytváříme interaktivní scénáře hašení požárů různých tříd – včetně správné volby hasicího přístroje. A pokud jde o první pomoc, klienti oceňují simulace, kde si mohou „nanečisto“ vyzkoušet například resuscitaci nebo ošetření masivního krvácení.

Autor DP: To zní jako velmi komplexní řešení. S jakými obtížemi se při vývoji těchto nástrojů pro firmy potýkáte?

Výrobce: Nejčastěji řešíme následující výzvy:

- Technologická infrastruktura – ne všechny firmy mají dostatečné vybavení (např. VR headsety, výkonné počítače) nebo s tímto typem technologií nemají zkušenosti.
- Přesné přizpůsobení obsahu konkrétním pracovním podmínkám – každé pracoviště má svá specifika, která je potřeba v simulaci zohlednit, což je časově i finančně náročné.
- Očekávání managementu vs. realita – některé firmy očekávají, že VR okamžitě nahradí klasické školení, ale jde spíš o doplňkový nástroj, který má své silné i slabé stránky.
- Uživatelská adaptace – ne všichni zaměstnanci se ve virtuálním prostředí cítí komfortně, a je třeba s tím počítat.

Autor DP: Setkáváte se u svých klientů i s určitými nerealistickými očekáváním ohledně toho, co může VR školení nabídnout?

Výrobce: Ano, poměrně často. Některé organizace přicházejí s představou, že virtuální realita kompletně nahradí veškeré tradiční formy školení v oblasti BOZP. Domnívají se, že implementací VR automaticky dojde ke zvýšení efektivity, zkrácení času školení a současně k výraznému snížení nákladů.

Ve skutečnosti však VR technologie představuje doplněk ke klasickým formám výuky, nikoli jejich plnohodnotnou náhradu. Virtuální školení je velmi efektivní v oblasti nácviku krizových situací, simulace nebezpečných prostředí a zvyšování schopnosti rychle a správně reagovat pod tlakem. Nicméně ne vždy je vhodné pro přenos teoretických znalostí, nebo administrativních informací, kde může být klasická výuka efektivnější.

Je tedy důležité, aby management měl reálná očekávání a pohlížel na VR jako na inovativní nástroj rozšiřující možnosti vzdělávání, nikoli jako na „všeřešící“ technologii.

Autor DP: Jaká doporučení byste tedy firmám dal, pokud zvažují implementaci VR/AR školení do svých procesů?

Výrobce:

1. Začněte pilotním projektem – testujte v malém měřítku, ideálně s motivovanou skupinou zaměstnanců.
2. Přizpůsobte obsah konkrétním rizikům a procesům vaší firmy, nevolte univerzální šablony.
3. Zapojte BOZP specialisty i běžné pracovníky už ve fázi návrhu – získáte cennou zpětnou vazbu.
4. Nepodceňte zaškolení personálu v práci s technikou – samotná technologie nestačí, důležitá je i její správná obsluha.
5. Sledujte efekt školení – ideálně porovnávejte výsledky tradičního a VR školení a vyhodnocujte přínosy.

Autor DP: Děkuji e za velmi inspirativní rozhovor. Věřím, že VR a AR školení se stanou v oblasti BOZP stále běžnějším standardem.

Výrobce: Děkuji i já. Naší ambicí je nabídnout nástroj, který zaměstnancům umožní zažít rizikové situace „nanečisto“ – bez ohrožení zdraví, ale se silným zapamatováním. To je skutečný přínos virtuální reality pro prevenci.

Závěr rozhovoru:

Rozhovor s výrobcem VR/AR nástrojů pro školení v oblasti BOZP, požární ochrany a první pomoci ukázal, že tyto technologie mají výrazný potenciál zefektivnit vzdělávání zaměstnanců, zejména díky možnosti simulovat rizikové situace v bezpečném prostředí. Firmy o tato řešení stále častěji projevují zájem, avšak implementace naráží na technologické, obsahové i personální výzvy. Úspěch zavádění VR školení do praxe závisí především na realistickém očekávání ze strany managementu, aktivním zapojení zaměstnanců a důkladné přípravě obsahu i technického zázemí. Virtuální realita tak představuje cenný doplněk tradičního školení, nikoli jeho úplnou náhradu.

Rozhovor s poskytovatelem digitálních řešení v oblasti BOZP

Rozhovor byl veden se zástupcem společnosti, která se specializuje na vývoj a implementaci digitálních nástrojů a softwarových řešení zaměřených na zajištění bezpečnosti práce, prevenci rizik a efektivní řízení procesů BOZP. Cílem rozhovoru bylo zjistit, jaké konkrétní produkty a technologie jsou v této oblasti nabízeny, jaká je poptávka

ze strany organizací usilujících o digitalizaci bezpečnostních procesů, a jaké přínosy či výzvy s sebou tato řešení v praxi nesou. Diskutovány byly také doporučené postupy pro úspěšnou implementaci do různých provozních prostředí a přístupy k uživatelské podpoře a vzdělávání.

(Rozhovor je pro účely diplomové práce anonymizován.)

Autor DP: Dobrý den, děkujeme, že jste si na nás udělal čas. Mohl byste nám představit, jaké produkty a řešení v oblasti Průmyslu 4.0 vaše firma nabízí?

Výrobce: Dobrý den, děkuji za pozvání. Naše firma se dlouhodobě specializuje na oblast bezpečnosti práce a technologických řešení pro průmysl. V rámci konceptu Průmysl 4.0 nabízíme především chytré bezpečnostní prvky, jako jsou bezdrátové senzory, systémy pro monitoring pracovního prostředí, prediktivní údržbu a datové platformy pro zpracování a vyhodnocení dat z výrobních provozů.

Autor DP: To zní velmi moderně. S jakými omezeními se setkáváte při implementaci těchto řešení do firemní praxe.

Výrobce: Nejčastější překážkou je kulturní i technologická připravenost firem. Mnoho podniků má ještě starší infrastrukturu, která není kompatibilní s novými technologiemi. Dále se setkáváme s omezeným rozpočtem nebo s nedůvěrou vůči novým technologiím – například obavy z narušení soukromí nebo příliš složité správy dat. Někdy bývá překážkou i nedostatek kvalifikovaného personálu, který by nové systémy efektivně obsluhoval a interpretoval jejich výstupy.

Autor DP: A jaký je aktuálně zájem o tyto produkty na českém trhu?

Výrobce: Zájem určitě roste, hlavně u středně velkých a větších podniků. Především výrobní a logistické firmy si uvědomují, že bez automatizace a chytrých systémů nebudou konkurenceschopné. Nejvíce se zajímají o systémy prediktivní údržby, sledování stavu zařízení a bezpečnostní systémy, které dokáží předcházet úrazům. V poslední době zaznamenáváme zvýšený zájem i ze strany firem, které chtějí zlepšit udržitelnost svých provozů a optimalizovat spotřebu energií.

Autor DP: Jaké příležitosti v oblasti Průmyslu 4.0 podle vás v České republice existují?

Výrobce: Velký potenciál vidíme v digitalizaci malých a středních podniků, které zatím technologie Průmyslu 4.0 příliš nevyužívají. Dále také v integraci datových platforem s bezpečnostními a environmentálními systémy – například sledování expozice pracovníků

chemikáliím nebo hluku. Obrovskou příležitostí je i zapojení do evropských dotačních programů, které firmám umožňují financovat zavádění těchto technologií.

Autor DP Máte nějaká doporučení pro firmy, které zvažují zavedení produktů Průmyslu 4.0?

Výrobce: Určitě doporučujeme začít analýzou současného stavu. Mnoho firem chce jít hned do komplexních řešení, ale často je lepší začít pilotním projektem – třeba sledováním jednoho zařízení nebo procesu. Je také důležité vybrat správného partnera, který pomůže s návrhem a implementací řešení šitého na míru. A hlavně – nezapomínat na školení zaměstnanců. Technologie jsou jen nástroj, skutečnou změnu dělají lidé, kteří je používají.

Autor DP: Děkuje za velmi přínosné informace. Přejeme vám mnoho úspěchů při dalším rozvoji technologií Průmyslu 4.0.

Výrobce: Děkuji, a pokud by některé firmy měly zájem o konzultaci nebo pilotní projekt, rádi pomůžeme.

Závěr:

Společnost nabízí v rámci Průmyslu 4.0 chytré bezpečnostní systémy, senzory, monitoring prostředí a prediktivní údržbu, které zvyšují efektivitu a bezpečnost provozů. Při zavádění těchto technologií firmy často čelí problémům se zastaralou infrastrukturou, omezenými rozpočty a nedostatkem kvalifikovaného personálu. Zájem na českém trhu však roste, zejména u větších firem, přičemž příležitosti vidí i u menších podniků a v možnostech evropského financování. Doporučuje začít pilotním projektem, volit spolehlivého partnera a důkladně školit zaměstnance.

11 DOTAZNIKOVÉ ŠETŘENÍ

Cílem dotazníkového šetření uvedeného v této části práce bylo zjistit současný stav využívání digitálních technologií v organizacích a vyhodnotit jejich vliv na bezpečnost a ochranu zdraví při práci. Hlavní cílovou skupinou dotazníku byli zaměstnanci odpovědní za BOZP, bezpečnostní technici a další odborníci v této oblasti.

Dotazníkové šetření bylo vytvořeno tak, aby poskytlo důkladný obraz o stupni digitalizace v jednotlivých společnostech, o používaných technologiích, vnímaných rizicích a výhodách a o problémech, které se při zavádění těchto technologií vyskytly. Studie se rovněž dotazovala na budoucí cíle a přání pokračovat v digitalizaci postupů v oblasti bezpečnosti a ochrany zdraví zaměstnanců.

Průzkum byl šířen dvěma způsoby: osobně prostřednictvím QR kódu na odborné konferenci zaměřené na problematiku BOZP a elektronicky prostřednictvím e-mailu. Tím byl zaručen různorodý vzorek respondentů z různých odvětví.

Zjištění průzkumu tvoří základ pro určení vzorců, problematických míst a šancí pro další digitalizační iniciativy v oblasti BOZP. Na základě těchto výsledků je pak navržena Road Map pro pokrok v digitalizaci v této oblasti.

Pro vizuální představu o podobě dotazníkového šetření je níže přiložen QR kód, který umožňuje nahlédnout na jeho strukturu a obsah a možného vyplnění nebo je přiložen v PŘÍLOZE P I.



Obrázek 13 – QR kód Dotazníkového šetření

11.1 Výsledky dotazníkového šetření

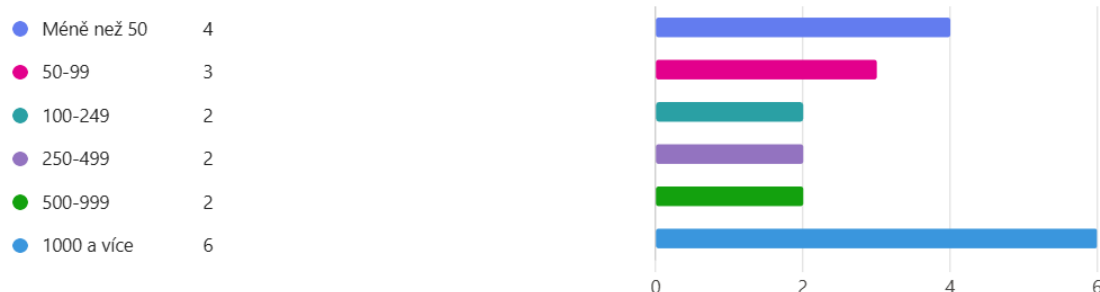
Otázka č. 1 – Působnost vaší firmy se nachází na území:



Obrázek 14 – Grafické znázornění otázky týkající se působnosti firmy (zdroj Microsoft Forms)

Graf znázorňuje působnost firem, které se zúčastnily dotazníkového šetření. Z výsledků vyplývá, že 95 % respondentů pochází z České republiky a zbývajících 5 % tvoří firmy ze Slovenska.

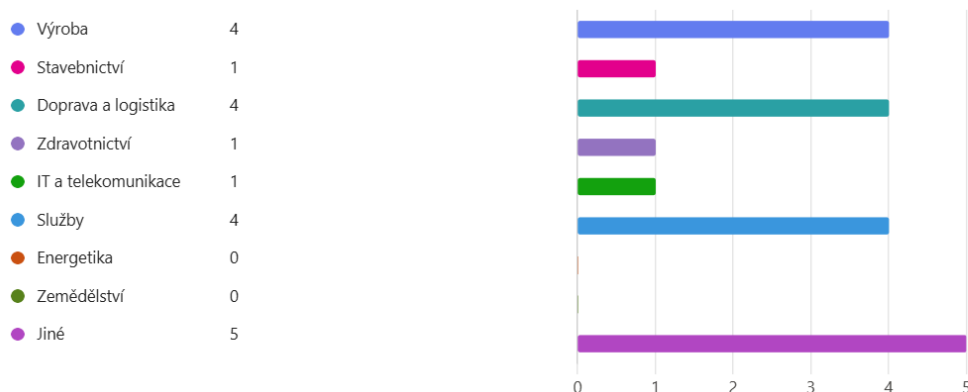
Otázka č. 2 – Kolik má vaše organizace zaměstnanců?



Obrázek 15 – Grafické znázornění týkající se počtu zaměstnanců ve firmě (zdroj Microsoft Forms)

Graf ukazuje rozdělení firem podle počtu zaměstnanců. Největší zastoupení mají firmy s více než 1000 zaměstnanci, které tvoří 32 %. Následují malé firmy s méně než 50 zaměstnanci, a to s podílem 21 %. Třetí nejčastější skupinou jsou firmy s 50 až 99 zaměstnanci, které představují 16 %. Zbývajících tři kategorie – firmy se 100–249, 250–499 a 500–999 zaměstnanci – jsou rovnoměrně zastoupeny, každá s podílem 11 %.

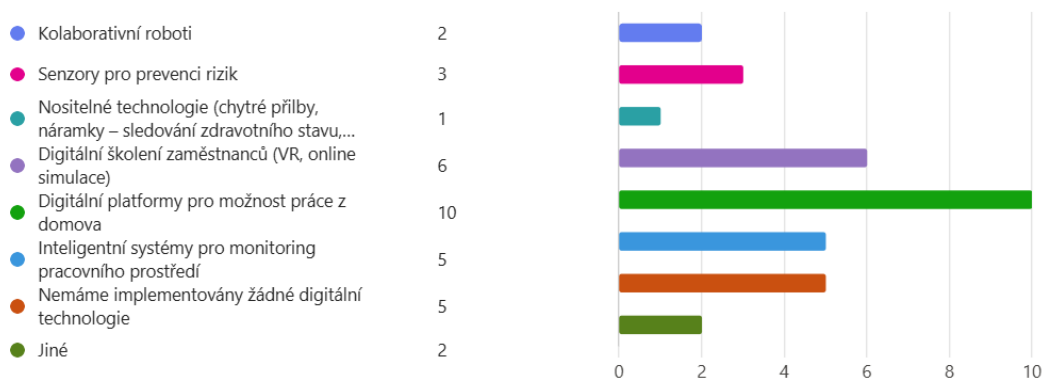
Otázka č. 3 – V jakém průmyslovém odvětví působí vaše organizace?



Obrázek 16 – Grafické znázornění otázky týkající se působnosti firmy (zdroj Microsoft Forms)

Z grafu vyplývá, že nejvíce respondentů zaškrtnulo možnost „jiné“. Podrobnější analýza těchto odpovědí ukázala, že se jedná například o Armádu ČR, Správní úřad (SÚJB) či subjekty veřejné správy. Mezi další výrazně zastoupené oblasti patří služby, doprava a logistika a výroba. Ostatní kategorie byly zastoupeny pouze jednotlivci.

*Otázka č. 4 – Jaké digitální technologie jsou ve vaší organizaci implementovány?
(Vyberte všechny relevantní možnosti.)*



Obrázek 17 – Grafické znázornění otázky týkající se digitálních technologií zavedené ve firmě (zdroj Microsoft Forms)

Graf ukazuje, které prvky digitalizace firmy nejčastěji využívají. Nejvýznamnější podíl zauímají digitální platformy umožňující práci z domova, které využívá 29 % respondentů. Na druhém místě jsou digitální školení zaměstnanců s podílem 18 %. Shodně po 15 % mají inteligentní systémy pro monitoring pracovního prostředí a firmy, které zatím žádné digitální prvky neimplementovaly. Další skupinu tvoří kolaborativní roboti a různé specifické

technologie, jako je vyhledávání informací, AI pro kamerové systémy či bezpečnostní prvky ve vozidlech, které celkem tvoří 6 %. Nejmenší zastoupení mají nositelné technologie, které využívá pouze 1 % respondentů.

Otázka č. 5 – Jak hodnotíte dopad těchto digitálních technologií na zajištění bezpečnosti a ochrany zdraví při práci (BOZP) ve vaší organizaci?



Obrázek 18 – Grafické znázornění otázky týkající se dopadu digitálních technologií na BOZP (zdroj Microsoft Forms)

Z grafu je patrné, že polovina respondentů hodnotí dopad digitálních technologií neutrálně (50 %). Přibližně pětina respondentů (20 %) vnímá jejich vliv pozitivně a zbývající třetina (30 %) jej hodnotí jako velmi pozitivní. Zároveň žádný z respondentů neuvedl, že by dopad digitalizace vnímal negativně nebo velmi negativně, což naznačuje celkově spíše příznivé vnímání těchto technologií.

Otázka č. 6 – Zaznamenali jste po zavedení digitálních technologií zlepšení v oblasti prevence rizik na pracovišti?



Obrázek 19 – Grafické znázornění otázky týkající se zlepšení prevence rizik (zdroj Microsoft Forms)

Z grafu vyplývá, že u 40 % respondentů nelze jednoznačně posoudit, zda implementace digitálních technologií vedla ke zlepšení v oblasti prevence rizik. Dalších 30 % uvedlo, že žádná změna nenastala. Mírné zlepšení zaznamenalo 25 % respondentů a výrazné zlepšení

uvedlo 5 %. Zároveň žádný z respondentů neuvedl, že by po zavedení digitálních technologií došlo ke zhoršení v oblasti prevence rizik, což naznačuje alespoň stabilní nebo mírně pozitivní vývoj.

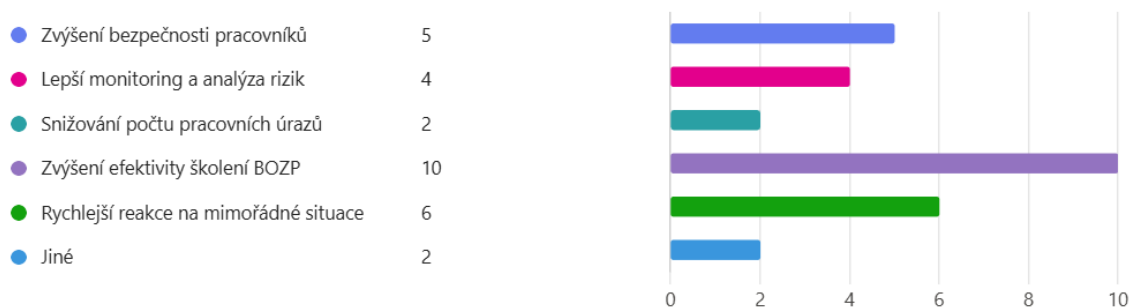
Otázka č. 7 – Evidujete ve vaší organizace počet pracovních úrazů před a po zavedení digitálních technologií?



Obrázek 20 – Grafické znázornění otázky týkající se evidování úrazů před a po zavedení digitálních technologií (zdroj Microsoft Forms)

Z grafu lze vyčíst, že 55 % respondentů neeviduje pracovní úrazy nebo nemá k dispozici potřebná data. Dalších 35 % uvedlo, že mají údaje o pracovních úrazech za obě sledovaná období – tedy před i po zavedení digitálních technologií. Pouze 5 % respondentů má údaje pouze za období před implementací digitálních technologií a zbývajících 5 % uvedlo, že zatím žádné digitální technologie nezavedli.

Otázka č. 8 – Jaké konkrétní přínosy v oblasti BOZP přinesla digitalizace ve vaší organizaci? (Vyberte všechny relevantní možnosti.)

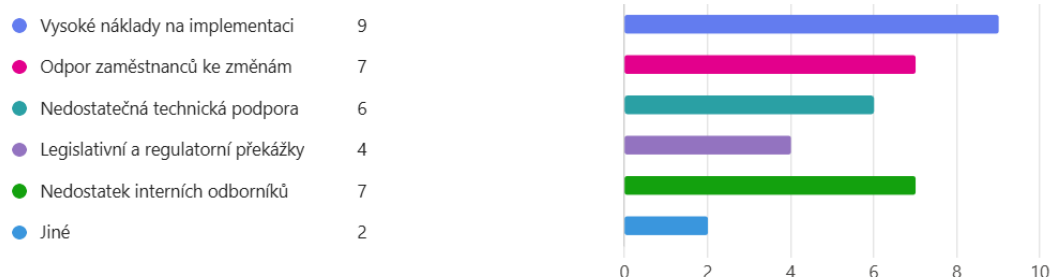


Obrázek 21 – Grafické znázornění otázky týkající se přínosů digitalizace BOZP (zdroj Microsoft Forms)

Tento graf ukazuje, jaké hlavní přínosy vnímají respondenti v souvislosti se zaváděním digitálních technologií. Nejčastěji zmiňovaným přínosem je zvýšení efektivity, které uvedlo 34 % respondentů. Dalších 21 % ocenilo rychlejší reakce na mimořádné události a 17 %

uvedlo zvýšení bezpečnosti pracovníků. Lepší monitoring a analýzu rizik zmínilo 14 % respondentů. Mezi méně často uváděné přínosy patří snižování počtu pracovních úrazů. Do kategorie „jiné“ respondenti nejčastěji uvedli, že zatím k žádné digitalizaci ve firmě nedošlo

Otázka č. 9 – Jaké hlavní výzvy nebo problémy jste při implementaci digitálních technologií v oblasti BOZP zaznamenali? (Vyberte všechny relevantní možnosti.)



Obrázek 22 – Grafické znázornění otázky týkající se hlavních problémů a výzev spojené se zavedením digitálních prvků (zdroj Microsoft Forms)

Graf ukazuje hlavní problémy, se kterými se organizace potýkají při implementaci digitálních technologií. Nejčastěji zmiňovanou překážkou jsou vysoké náklady, které uvedlo 26 % respondentů. Dále byl často zmiňován odpor zaměstnanců ke změnám a nedostatek interních odborníků, oba tyto faktory získaly shodně po 20 %. Nedostatečná technická podpora představuje problém pro 17 % respondentů a legislativní překážky pro 11 %. Do kategorie „jiné“ respondenti zahrnuli například nezáměr vedení o digitalizaci nebo skutečnost, že k jejímu zavedení dosud nedošlo.

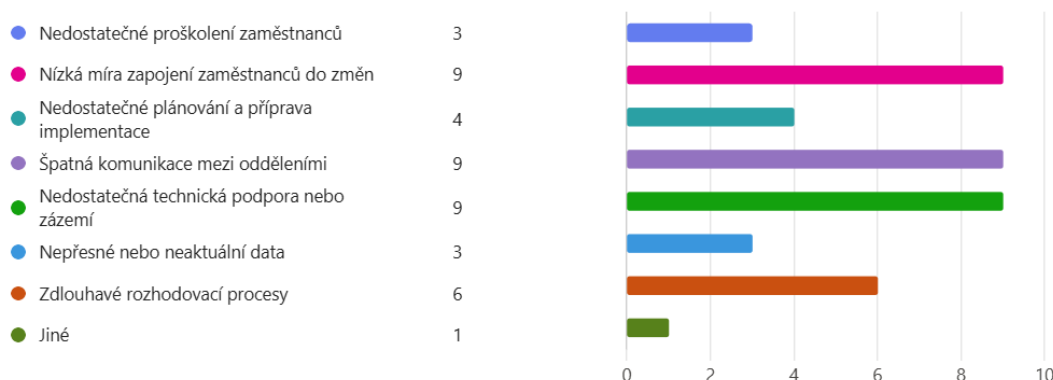
Otázka č. 10 – Setkali jste se při implementaci digitálních technologií s procesními nedostatky?



Obrázek 23 – Grafické znázornění otázky týkající se procesních nedostatků po implementaci (zdroj Microsoft Forms)

Z grafu vyplývá, že většina respondentů, konkrétně 56 %, se při implementaci digitálních technologií setkala s mírnými procesními nedostatky. Dalších 39 % uvedlo, že se s žádnými nedostatky nesetkalo, což naznačuje hladký průběh zavádění. Pouze 6 % respondentů zaznamenalo výrazné procesní nedostatky, což svědčí o tom, že vážnější problémy při implementaci byly spíše výjimečné.

Otázka č. 11 – Jaké konkrétní procesní nedostatky jste zaznamenali při implementaci digitálních technologií? (Vyberte všechny relevantní možnosti.)



Obrázek 24 – Grafické znázornění otázky týkající se konkrétních nedostatků (zdroj Microsoft Forms)

Graf ukazuje, jaké konkrétní procesní nedostatky firmy nejčastěji vnímají při implementaci digitálních technologií. Nejčastěji zmiňované problémy, každý s podílem 20 %, zahrnují nízkou míru zapojení zaměstnanců do změn, špatnou komunikaci mezi odděleními a nedostatečnou technickou podporu či zázemí. Další významnou překážkou jsou zdlouhavé rozhodovací procesy, které uvedlo 14 % respondentů. Nedostatečné plánování a příprava implementace tvoří 9 %, zatímco nepřesná nebo neaktuální data a nedostatečné proškolení zaměstnanců byly zmiňovány shodně po 7 %. Do kategorie „jiné“ spadá 2 % odpovědí, které uvádějí nulový počet zavedených digitálních technologií.

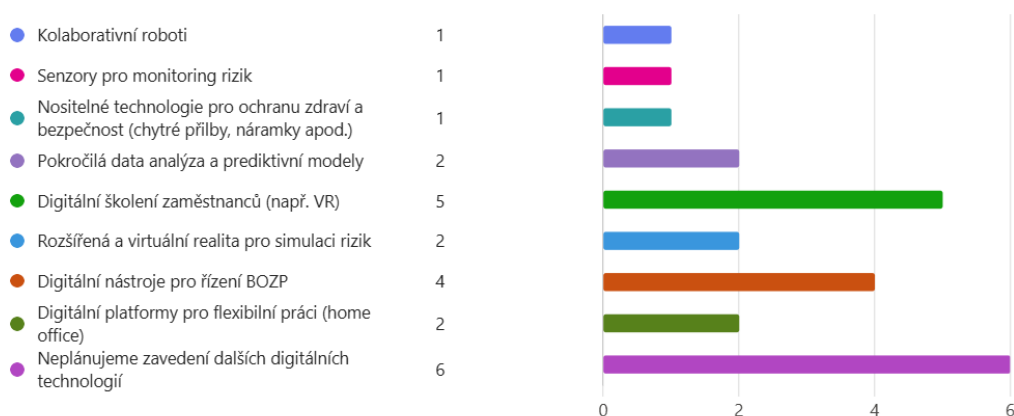
Otázka č. 12 – Plánujete implementovat další prvky digitalizace?



Obrázek 25 – Grafické znázornění otázky týkající se zavedení dalších prvků digitalizace (zdroj Microsoft Forms)

Z grafu vyplývá, že více než polovina respondentů (55 %) v současnosti neplánuje zavedení dalších digitálních technologií. Dalších 30 % sice zavedení plánuje, ale zatím bez stanoveného časového harmonogramu. Přibližně 10 % respondentů má v úmyslu implementaci realizovat v horizontu 1 až 3 let a zbývajících 5 % plánuje zavést nové digitální technologie do 12 měsíců.

Otázka č. 13 – Pokud plánujete zavedení dalších digitálních technologií, o jaké konkrétní prvky se jedná? (Vyberte všechny relevantní možnosti.)

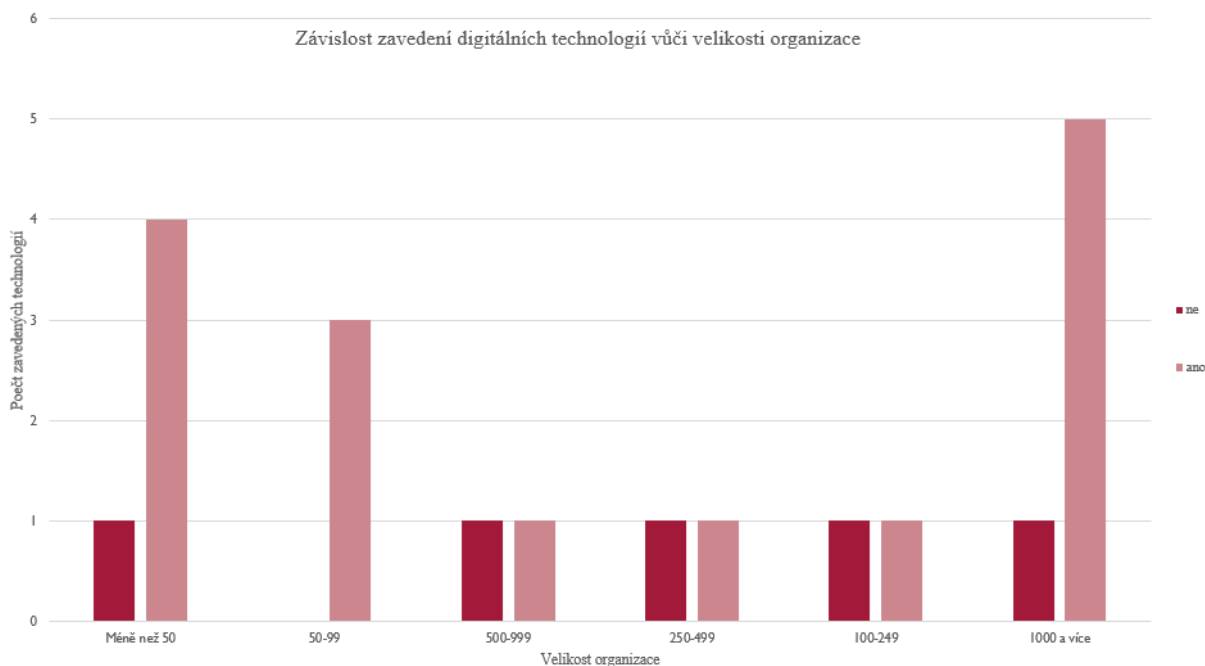


Obrázek 26 – Grafické znázornění otázky týkající se zavedení dalších konkrétních prvků digitalizace (zdroj Microsoft Forms)

Tento graf vypovídá o to, že 25 % neplánuje zavedení dalších technologií, dalších 21 % plánuje zavést digitální školení zaměstnanců, 17 % plánuje digitální nástroje pro řízení BOZP, 8 % respondentů má v plánu zavést pokročilá data analýzy a prediktivní modely, rozšířenou a virtuální realitu pro simulaci rizik a také digitální platformy pro flexibilní práci. Poslední kategorie po 4 % je zavedení kolaborativních robotů, senzorů pro monitoring rizik a nositelné technologie pro ochranu zdraví a bezpečnost.

11.2 Výzkumné otázky

Existuje souvislost mezi velikostí organizace a rozsahem zavedení digitalizačních prvků v oblasti BOZP?



Obrázek 27 – Graf závislosti digitálních technologií vůči velikosti organizace (vlastní)

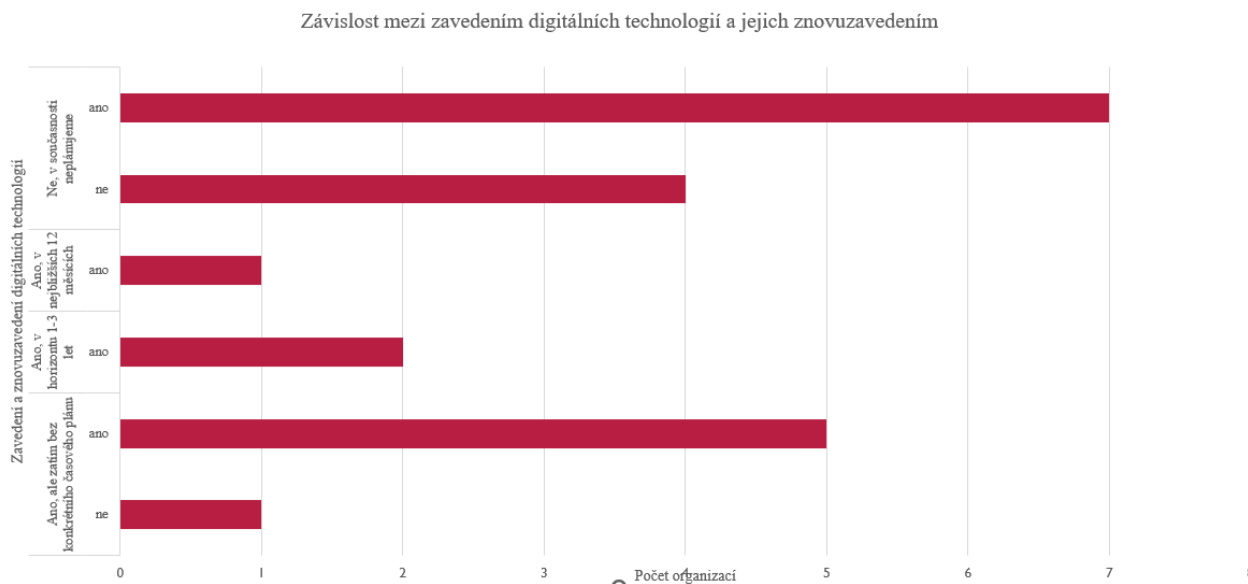
Graf zobrazuje závislost zavedení digitálních technologií v oblasti BOZP na velikosti organizace. Osa X uvádí velikost organizace podle počtu zaměstnanců, zatímco osa Y znázorňuje počet organizací, které daný počet prvků digitalizace zavedly. V legendě jsou uvedena dvě časová období nebo dvě skupiny dat – označeny jako „1 až 3“ (tmavě červená) a „3 a více“ (světle červená), což lze chápat jako rozsah zavedených prvků digitalizace.

Organizace s více než 1000 zaměstnanci mají nejvyšší zastoupení ve skupině, která zavedla více než tři prvky digitalizace, což odpovídá očekávání, protože větší firmy zpravidla mají více zdrojů pro implementaci těchto technologií.

Zajímavým zjištěním je, že i firmy s méně než 50 zaměstnanci mají poměrně vysoké zastoupení v obou kategoriích, tedy jak s menším, tak větším počtem digitalizačních prvků.

Středně velké organizace (50–999 zaměstnanců) mají vyrovnanější nebo nižší počet zavedených technologií a žádná velikostní skupina v tomto rozmezí výrazně nevyniká.

Má prvotní implementace digitalizačních technologií vliv na ochotu či připravenost organizace zavádět další prvky digitalizace?



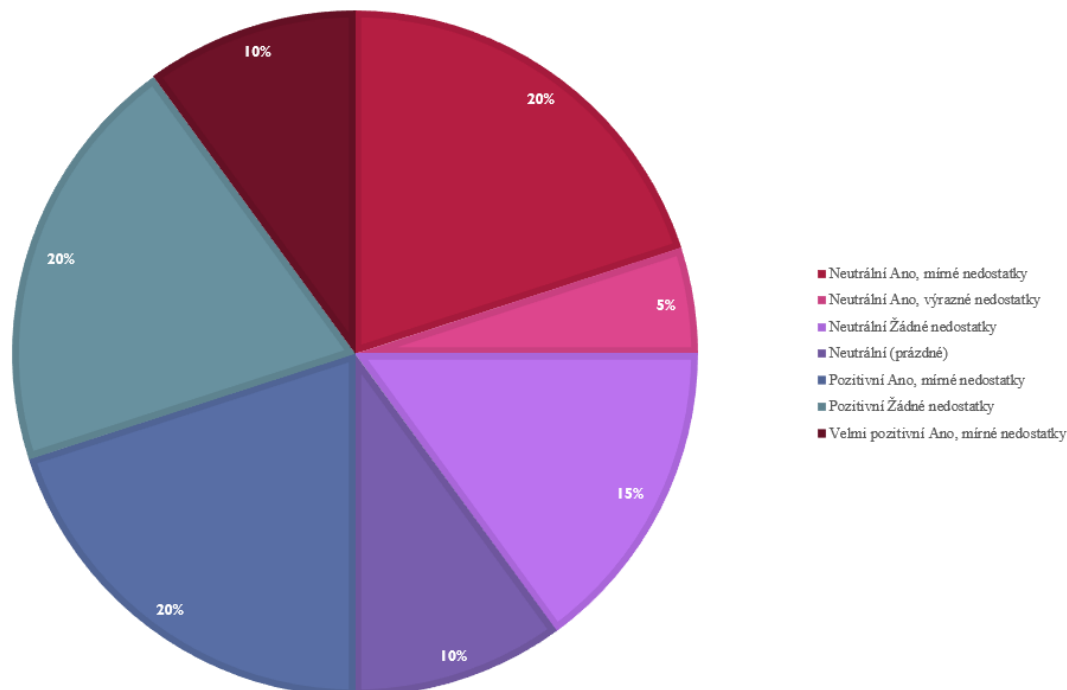
Obrázek 28 – Graf závislosti mezi zavedením digitálních technologií a jejich znovuzavedením (vlastní)

Graf zobrazuje vztah mezi prvotním zavedením digitalizačních technologií v organizaci a jejich následným znovuzavedením či ochotou k další digitalizaci. Je zřejmé, že prvotní pozitivní zkušenost s implementací digitálních prvků má výrazný vliv na ochotu organizace pokračovat v tomto trendu. Nejpočetnější skupinu tvoří organizace, které již digitální technologie implementovaly a zároveň deklarují připravenost pokračovat v dalším zavádění (7 organizací). Významná je také skupina 6 organizací, které zatím digitalizaci nezavedly a zároveň nemají zájem o její zavedení. Tento výsledek poukazuje na fakt, že bez jakékoliv zkušenosti s digitalizací zůstává postoj spíše rezervovaný, a že absenci prvního impulsu může být obtížné překonat. Menší počet organizací (5) uvedl, že i přes implementaci další rozšiřování neplánují, což ukazuje, že ne každá prvotní zkušenost musí být jednoznačně pozitivní, nebo že narážejí na bariéry (např. finanční, personální či systémové). Pouze jediná organizace, která dosud žádné technologie nezavedla, uvedla, že další digitalizaci zvažuje, což jen potvrzuje význam úvodního impulsu pro další strategické směřování organizace.

Výsledky potvrzují významné zjištění: první krok v oblasti digitalizace je pro organizace klíčový a může ovlivnit celý budoucí vývoj v této oblasti.

Je mezi mírou aplikace digitálních technologií a výskytem procesních nedostatků v organizaci identifikovatelný vztah?

Závislost mezi hodnocením dopadů aplikace digitálních technologií a procesními nedostatky při jejich zavádění



Obrázek 29 – Graf závislost mezi hodnocením dopadů aplikace digitálních technologií a procesních nedostatků při jejich zavádění (vlastní)

Tento kruhový graf znázorňuje souvislost mezi hodnocením dopadu zavádění digitálních technologií v organizacích a výskytem procesních nedostatků. Ukazuje, jak různé kombinace těchto dvou faktorů byly zastoupeny mezi respondenty.

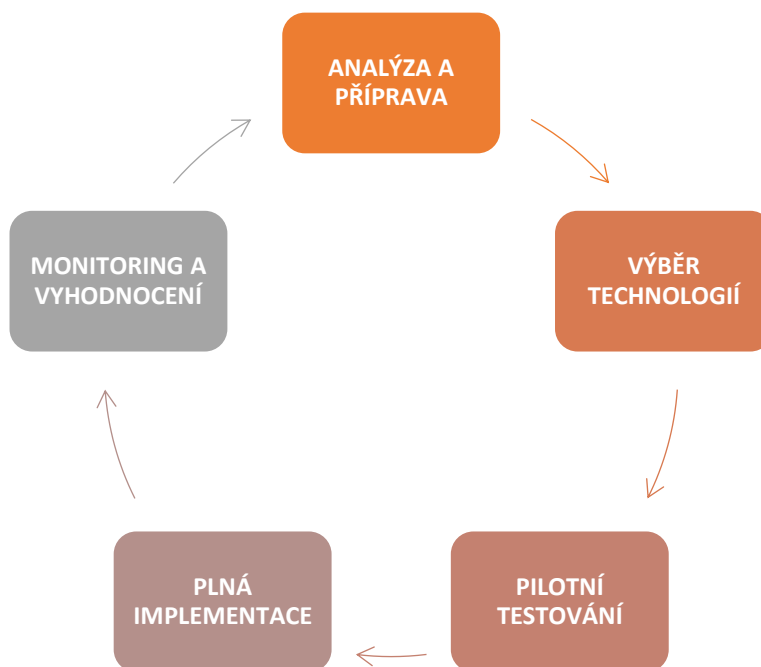
Největší podíly, každá po 20 %, patří třem kategoriím: neutrálnímu hodnocení s mírnými nedostatky, pozitivnímu hodnocení bez nedostatků a velmi pozitivnímu hodnocení s mírnými nedostatky. To naznačuje, že většina organizací buď nezaznamenala zásadní problémy, nebo je považovala za zvládnutelné. Naopak jen malé procento (5 %) uvedlo výskyt výrazných procesních nedostatků při zavádění digitálních technologií.

Celkově lze říci, že existuje identifikovatelný vztah mezi pozitivním hodnocením dopadů digitalizace a nižším výskytem procesních problémů v organizaci.

12 NÁVRH PODROBNÉHO ROADMAP K DIGITALIZACI BOZP

Tato roadmapa slouží jako přehledný návod pro organizace, které zvažují nebo plánují zavedení prvků digitalizace v oblasti bezpečnosti a ochrany zdraví při práci. Jednotlivé fáze postupu zachycují celý proces od úvodní analýzy přes výběr technologií a pilotní testování až po finální implementaci a dlouhodobé vyhodnocování. Součástí Roadmapy jsou také shrnuté hlavní benefity a možná rizika, která s jednotlivými kroky souvisejí. Cílem je poskytnout firmám praktický nástroj pro systematické, efektivní a bezpečné zavádění digitálních technologií s důrazem na prevenci rizik a ochranu zdraví zaměstnanců.

Roadmap pro zavádění digitalizace v oblasti BOZP — podrobný popis fází



Obrázek 30 – Fáze Road Map (vlastní)

FÁZE 1: ANALÝZA A PŘÍPRAVA

Cíl: Zmapovat aktuální stav, definovat potřeby a možnosti organizace v oblasti digitalizace BOZP.

Kroky:

- Provést **interní audit BOZP**, zjistit, kde jsou slabá místa, typické příčiny úrazů a nedostatků.
- Zhodnotit **současné procesy, systémy a evidenci BOZP**.
- Analyzovat incidenty a úrazovost za poslední období.

- Definovat **cíle digitalizace** (např. snížení počtu úrazů o 20 % za 2 roky, digitalizace evidence).
- Ověřit **legislativní požadavky** a standardy pro dané technologie (např. GDPR u AI a nositelných zařízení).
- Stanovit **rozpočet a dostupné personální kapacity**.
- Připravit návrh, **které oblasti a technologie mají největší potenciál pro zlepšení**.

Benefity:

- Odhalení slabých míst v aktuálním BOZP.
- Nastavení jasných cílů digitalizace.
- Přesné plánování rozpočtu a personálních kapacit.
- Předjetí zbytečným nákladům díky efektivnímu výběru priorit.

Rizika:

- Nedostatečná analýza může vést ke špatným rozhodnutím.
- Podcenění legislativních a etických aspektů (GDPR, bezpečnost dat).
- Nedostatek zapojení zaměstnanců do přípravy.

FÁZE 2: VÝBĚR TECHNOLOGIÍ

Cíl: Vybrat vhodné digitální technologie a nástroje pro implementaci.

Kroky:

- Vyhodnotit možnosti na trhu (AI nástroje, VR školení, nositelné technologie, senzory, digitální evidence).
- Posoudit **přínosy a náklady jednotlivých technologií**.
- Zaměřit se na technologie jako:
 - **AI systémy** (predikce rizik, rozpoznávání nebezpečných situací)
 - **Senzorická zařízení a IoT** (monitoring prostředí)
 - **Nositelné technologie** (sledování fyziologických parametrů)
 - **Digitální školení a simulace**
 - **Platformy pro vzdálené řízení BOZP**

- Vybrat dodavatele, kteří splňují bezpečnostní a legislativní požadavky.
- Připravit implementační plán a zvolit **pilotní provoz**.

Benefity:

- Možnost porovnat více řešení a vybrat nejvhodnější.
- Přesné zacílení investice na technologie s největším přínosem.
- Získání know-how od dodavatelů a odborníků.

Rizika:

- Nevhodný výběr technologie pro konkrétní pracoviště.
- Podcenění nároků na provoz, údržbu a školení.
- Riziko vysokých nákladů na technologie s omezeným efektem.

FÁZE 3: PILOTNÍ TESTOVÁNÍ

Cíl: Otestovat vybrané technologie na vybraném pracovišti nebo v části provozu.

Kroky:

- Implementovat vybrané technologie v omezeném rozsahu.
- Proškolit zaměstnance, kteří s nimi budou pracovat.
- Sběr dat a zpětné vazby od uživatelů.
- Sledování:
 - změny v úrazovosti
 - reakční dobu při incidentech
 - efektivitu školení
- Identifikovat problémy, nedostatky, odpor zaměstnanců.
- Provést potřebné úpravy před plošným zavedením.

Benefity:

- Ověření funkčnosti technologií v reálném provozu.
- Získání zpětné vazby od zaměstnanců.
- Možnost upravit nastavení před plošným zavedením.

Rizika:

- Odpor zaměstnanců vůči změnám.
- Neodhalení všech problémů v pilotní fázi.
- Ztráta důvěry, pokud testování selže.

FÁZE 4: PLNÁ IMPLEMENTACE

Cíl: Nasadit technologie v celém provozu a zajistit jejich efektivní využití.

Kroky:

- Postupné zavádění technologií na všech pracovištích.
- Organizace školení a workshopů pro zaměstnance.
- Nastavení **procesů pro správu, údržbu a aktualizaci technologií.**
- Zajištění **technické podpory a servisu.**
- Pravidelná kontrola dodržování nových postupů a jejich efektivity.

Benefity:

- Sjednocení postupů napříč celou organizací.
- Zvýšení bezpečnosti a prevence rizik.
- Efektivnější školení a evidence BOZP.
- Vyšší motivace zaměstnanců díky moderním nástrojům.

Rizika:

- Přetížení personálu a technické podpory.
- Vyšší finanční náklady při nečekaných komplikacích.
- Riziko nesouladu s legislativou nebo interními procesy.

FÁZE 5: MONITORING A VYHODNOCENÍ

Cíl: Vyhodnotit přínosy digitalizace a naplánovat další rozvoj.

Kroky:

- Sledování klíčových ukazatelů (úrazovost, počet incidentů, efektivita školení, spokojenost zaměstnanců).

- Pravidelné reporty a analýzy dat z digitálních systémů.
- Vyhodnocení dopadu na BOZP.
- Identifikování možností pro další rozšíření digitalizace.
- Aktualizování systémy a metodiku dle nových trendů a technologií.
- Příprava na **další fázi rozvoje digitalizace**.

Benefits:

- Přesná data pro řízení BOZP.
- Možnost rychle reagovat na změny a rizika.
- Plánování dalšího rozvoje a inovací.
- Posílení kultury bezpečnosti ve firmě.

Rizika:

- Nedostatečné vyhodnocování a zpracování dat.
- Přehlížení drobných problémů, které mohou přerůst v závažné.
- Riziko nevyužití potenciálu nasazených technologií.

13 DISKUZE

Digitalizace v oblasti BOZP je stále proměnlivým a vyvíjejícím se tématem. Teoretická část této práce ukazuje, že digitalizační prvky – ať už jde o inteligentní senzory, nositelné technologie nebo vzdělávací platformy – mohou výrazně zefektivnit prevenci rizik, zlepšit monitoring prostředí a zvýšit bezpečnost zaměstnanců. V praxi je ale situace často složitější.

Z výsledků dotazníkového šetření je zřejmé, že velikost firmy sama o sobě nehraje zásadní roli při rozhodování o implementaci digitalizace. Mnohé menší firmy se aktivně snaží o modernizaci, zatímco některé větší subjekty zůstávají konzervativní. Významnou roli zde hraje přístup vedení, firemní kultura i motivace ke změně.

Zajímavým zjištěním je výrazný zájem o digitální školení zaměstnanců, a to i přesto, že jde o finančně náročnější řešení. Firmy vnímají, že dlouhodobě se jim tato investice může vyplatit, zejména z hlediska prevence chyb a rizik vyplývajících z neinformovanosti.

Pozitivní je také to, že většina respondentů vnímá dopad digitalizačních nástrojů buď neutrálně, nebo pozitivně. Žádná firma neuváděla negativní dopady, což potvrzuje, že správně zavedené technologie mohou být přijímány bez odporu – zejména pokud jsou zaměstnanci zapojeni do procesu změny a mají dostatek podpory.

Na druhé straně však firmy stále čelí zásadním překážkám – vysokým nákladům, nedostatku odborníků, slabé technické podpoře nebo vnitrofiremním komunikačním bariérám. Teoretické poznatky zde korespondují s realitou – zavádění technologií není jen otázkou vybavení, ale i lidí, plánování a schopnosti změnu řídit.

Nedostatky se projevují také v oblasti vyhodnocování přínosů – mnoho firem nemá dostatek údajů k objektivnímu posouzení efektivity zavedených opatření. To brzdí další rozvoj a znesnadňuje rozhodování o dalších investicích.

Celkově se ukazuje, že firmy vnímají potenciál digitalizace pozitivně, ale její využití je zatím opatrné a často dílčí. Největší výzvou tak zůstává nejen technologie samotná, ale schopnost ji smysluplně a strategicky implementovat do reálného prostředí a propojit ji s firemní vizí a bezpečnostní kulturou.

ZÁVĚR

Digitalizace bezpečnosti a ochrany zdraví při práci představuje významný nástroj, jak reagovat na současné výzvy pracovního prostředí. Tato diplomová práce ukázala, že technologický rozvoj v oblasti BOZP není pouze otázkou zavádění nových nástrojů, ale především proměny způsobu uvažování o bezpečnosti jako takové – více datově podložené, proaktivní a systémově řízené.

Z dotazníkového šetření vyplynulo, že digitální technologie jsou v organizacích stále zaváděny selektivně a v omezeném rozsahu. Překvapivě však nezávisí míra implementace přímo na velikosti firmy. I menší organizace mohou být v digitalizaci aktivní, pokud existuje vůle vedení a prostor pro inovace. Za pozornost stojí i rostoucí zájem o digitální školení zaměstnanců, které si firmy vybírají navzdory jejich vyšší finanční náročnosti – což svědčí o důrazu na dlouhodobou udržitelnost a prevenci.

Řízené rozhovory přinesly cenný vhled do vývoje digitalizačních řešení a zároveň upozornily na řadu bariér, které v praxi brzdí rozvoj – zejména jde o vysoké náklady, nedostatek odborníků a odpor k organizačním změnám. Zároveň se však ukazuje, že první krok směrem k digitalizaci může hrát zásadní roli v tom, zda bude organizace ochotna pokračovat dál. Pozitivní zkušenost s prvotním zavedením technologií totiž významně ovlivňuje připravenost k jejich dalšímu rozšiřování.

Výsledky také poukázaly na to, že i přes obecně kladné vnímání přínosů digitalizace, organizace často postrádají nástroje pro její objektivní vyhodnocení. Chybějící data, nejednotná evidence úrazů nebo nedostatečné zapojení zaměstnanců do změnových procesů zůstávají faktory, které mohou oslabit účinnost zavedených technologií.

Závěrem lze říct, že digitalizace má v oblasti BOZP značný potenciál – avšak její úspěšné zavedení závisí nejen na technologiích samotných, ale především na komplexním přístupu organizace, její kultuře, připravenosti zaměstnanců a schopnosti pracovat s daty. Pro budoucnost tak zůstává klíčovou výzvou propojit technické inovace s efektivním řízením, lidským faktorem a dlouhodobou strategií bezpečnosti práce.

SEZNAM POUŽITÉ LITERATURY

, Úřad vlády ČR - Oddělení strategie a trendů EU, 2015. Dopady digitalizace na trh práce v ČR a EU. Online. *OSTEU Discussion paper*. Č. 12, s. 20. Dostupné z: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://vlada.gov.cz/assets/evropske-zalezitosti/analyzy-EU/Dopady-digitalizace-na-trh-prace-CR-a-EU.pdf>. [cit. 2025-02-13].

„Noční oči“ českých vrtulníků: Historie a současnost použití NVG na našich vojenských vrtulnících, © 2025. Online. Czech Air Force. Dostupné z: <https://czechairforce.com/news/nocni-oci-ceskych-vrtulnikaru-historie-a-soucasnost-pouziti-nvg-na-nasich-vojenskych-vrtulnicich/>?. [cit. 2025-04-13].

2019. Toward understanding the impact of artificial intelligence on labor. *PNAS*. No. 14, s. 6531-6539. ISSN 1091-6490.

3 typy cloud computingu: SaaS, PaaS, IaaS, © 2025. Online. In: Algotech. Dostupné z: <https://www.cestadocloudu.cz/blog/3-typy-cloud-computingu-saas-paas-iaas/>. [cit. 2025-04-11].

3M Worker Health and Safety, © 3M 2025. Online. Dostupné z: https://www.3m.co.uk/3M/en_GB/worker-health-safety-uk/safety-solutions/industry-solutions/defence-ppe/?utm_term=sibg-psd-le_d-en_eu-eng-defence-website-osm-amp-amp-learn-na-ne24-63210. [cit. 2025-04-20].

A Brief Overview of Digital Military Systems Used in the Armies of NATO Member Countries, 2021. I.

Advanced robotics and automation: implications for occupational safety and health, © 2025 EU-OSHA. Online. *European Agency for Safety and Health at Work*. S. 45. ISSN 1831-9343. Dostupné z: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://osha.europa.eu/sites/default/files/2022-06/Advanced_robotics_automation_implications.pdf. [cit. 2025-03-12].

AI ve službách BOZP. Co nám ukázala studie REDECA o umělé inteligenci?, 2023. Online. Bezpečnost práce.info. 2.11. 2023. Dostupné z: <https://www.bezpecnostprace.info/umela-intelligence-ai/studie-redeca/>. [cit. 2025-03-12].

An OSH smart control centre: smart digital systems for improving workers' safety and health, 2024. Online. *European Agency for Safety and Health at Work*. S. 9. Dostupné

z: <https://healthy-workplaces.osha.europa.eu/en/publications/osh-smart-control-centre-smart-digital-systems-improving-workers-safety-and-health?>. [cit. 2025-03-30].

Analýza možných dopadů Průmyslu 4.0 na nemoci z povolání, 2021. Online. *Časopis výzkumu a aplikací v profesionální bezpečnosti (JOSRA)*. Roč. 14, s. 7. Dostupné z: <https://vubp.cz/soubory/vyzkum/projekty/01-2020-VUBP/Priloha-6-Jost-Analyza-moznych-dopadu-Prumyslu-4-0-na-nemoci-z-povolani.pdf?>. [cit. 2025-03-17].

ARTIFICIAL INTELLIGENCE - BASED VEHICULAR AUTOMATION FITTED TO EXCAVATORS TO AUTOMATE TRENCHING (ID6), 2023. Online. *European Agency for Safety and Health at Work*. S. 10. Dostupné z: <https://osha.europa.eu/en/publications/artificial-intelligence-based-vehicular-automation-fitted-excavators-automate-trenching-id6>. [cit. 2025-03-30].

Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends, and Directions, 2020. Online. *Sustainability*. No. 12, s. 26. Dostupné z: <https://www.mdpi.com/2071-1050/12/2/492>. [cit. 2025-04-11].

Automation of cognitive and physical tasks in the health and social care sector: implications for safety and health, 2024. Online. *European Agency for Safety and Health at Work*. S. 54. ISSN 978-92-9402-327-8. Dostupné z: <https://doi.org/10.2802/692689>. [cit. 2025-03-13].

Bezpečnost v systémech Internetu věcí (IoT), 2020. Online. *Elektroprůmysl.cz*. Dostupné z: <https://www.elektroprumysl.cz/automatizace/bezpecnost-v-systemech-internetu-veci-iot?>. [cit. 2025-03-17].

Bude v budoucnu BOZP řešit i naši duševní pohodu? Trendy bezpečnosti a ochrany zdraví při práci tomu nasvědčují, 2020. Online. *SECURITY Magazin*. Dostupné z: <https://www.securitymagazin.cz/security/bude-v-budoucnu-bozp-resit-i-nasi-dusevni-pohodu-trendy-bezpecnosti-a-ochrany-zdravi-pri-praci-tomu-nasvedcuji-1404065517.html?>. [cit. 2025-03-17].

Co je cloud computing, jak funguje a proč ho zavést do firmy, 2024. Online. *Rascasone*. 3.7. 2024. Dostupné z: <https://www.rascasone.com/cs/blog/co-je-cloud-podnikani>. [cit. 2025-02-17].

Co je Internet věcí (IoT)? Online. In: *SAP*. Dostupné z: <https://www.sap.com/cz/products/artificial-intelligence/what-is-iot.html#main>. [cit. 2025-02-17].

Co je to strojové učení?, © 2025 SAP. Online. SAP. Dostupné z: <https://www.sap.com/cz/products/artificial-intelligence/what-is-machine-learning.html>. [cit. 2025-03-31].

COGNITIVE AUTOMATION: IMPACT, RISKS AND OPPORTUNITIES FOR OCCUPATIONAL SAFETY AND HEALTH, 2022. Online. *European Agency for Safety and Health at Work*. S. 6. Dostupné z: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://osha.europa.eu/sites/default/files/documents/policy_brief_based_systems_cognitive_tasks_en.pdf. [cit. 2025-03-12].

Cybersecurity for Industry 4.0 in the current literature: A reference framework, Copyright © 2025 Elsevier B.V. All. Online. *Computers in Industry*. S. 14. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0166361518303658>. [cit. 2025-04-11].

Digital Twins in Industry 5.0, 2023. Online. Research. Dostupné z: <https://spj.science.org/doi/full/10.34133/research.0071>. [cit. 2025-04-11].

Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age, 2023. I.

Digitalizace a bezpečnost a ochrana zdraví při práci (BOZP), 2020. I. Výzkumný program EU-OSHA.

Digitalizace a dynamické hodnocení rizik jako vize budoucnosti, 2022. Online. Bezpečnost a hygiena práce. 13. 1. 2022. Dostupné z: <https://www.bhp.cz/clanky/14803/digitalizace-a-dynamicke-hodnoceni-rizik-jako-vize-budoucnosti?>. [cit. 2025-03-17].

Dlouhodobý výhled pro obranu 2035, 2019. Online. I. Ministerstvo obrany.

EEP-100 EU 3M PELTOR, Copyright 2025. Online. In: 3Market. Dostupné z: <https://www.3market.cz/eep-100-eu-3m-peltor-elektronicke-usni-zatky--nabijeci/>. [cit. 2025-03-27].

Elektronická identifikace, 2024. Online. Evropská komise. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/policies/electronic-identification>. [cit. 2025-04-11]. *Bezpečnostní politika*, 2019. Online. Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D>. [cit. 2025-04-11].

Elektronické nástroje v oblasti BOZP, © 2025 EU-OSHA. Online. Evropská agentura pro bezpečnost a ochranu zdraví při práci. Dostupné z: <https://osha.europa.eu/cs/themes/osh-e-tools>. [cit. 2025-03-17].

Empatica, 2020. Online. Dostupné z: <https://www.empatica.com/>. [cit. 2025-04-13].

Event recognition for improved safety management: smart digital systems for improving workers' safety and health, 2024. Online. *European Agency for Safety and Health at Work*. S. 8. Dostupné z: <https://healthy-workplaces.osha.europa.eu/en/publications/event-recognition-improved-safety-management-smart-digital-systems-improving-workers-safety-and-health?>. [cit. 2025-03-30].

Hexoskin Smart Shirts, Hexoskin © 2025. Online. Dostupné z: <https://hexoskin.com/>. [cit. 2025-04-13].

How to Prepare and Guide Employees for VR Training?, © 2025 Visartech. Online. In: Visartech. Dostupné z: <https://www.visartech.com/blog/how-to-prepare-and-guide-employees-for-vr-training/>. [cit. 2025-03-26].

HOWARD, John, 2019. *Artificial intelligence: Implications for the future of work*. Online. I. Dostupné z: <https://doi.org/10.1002/ajim.23037>. [cit. 2025-03-12].

CHAKRAVORTI, Nirjhar. *Digital Transformation*. Boca Raton: Productivity Press, 2022. ISBN 978-1-032-22019-2.

Impact of Industry 4.0 on Operations, 2022. Online. In: Brightly. Dec 02, 2022. Dostupné z: <https://www.brightlysoftware.com/blog/impact-industry-4-point-0-operations>. [cit. 2025-03-24].

Industry 4.0 – Digitální dvojčata, 2022. Online. Svět průmyslu. Dostupné z: <https://svetprumyslu.cz/industry-4-0-digitalni-dvojcata/>. [cit. 2025-04-11]. *Blockchain Faks: What Is, How It works, and How It Can Be Used*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/terms/b/blockchain.asp>. [cit. 2025-04-11].

Industry 4.0 – The Global Industrial Revolution, 2023. Online. I. MDPI. Dostupné z: chrome-extension://efaidnbmninnibpcapjcgclcfndmkaj/https://mdpi-res.com/bookfiles/book/8462/Industry_40_The_Global_Industrial_Revolution_Achievements_Obstacles_and_Research_Needs_for_the_Digital_Transformation_of_Industry.pdf?v=1743041294. [cit. 2025-03-27].

Internet věcí je budoucnost. V čem je jeho největší výhoda a nebezpečí, 2022. Online. ŽIVĚ. 9. srpna 2022. Dostupné z: <https://www.zive.cz/clanky/internet-veci-je-budoucnost/sc-3-a-217765/default.aspx>. [cit. 2025-02-17].

Koncepce výstavby Armády České republiky 2035: (KVAČR 2035), 2024. Online. In: *Ministerstvo obrany ČR. Česká republika*, s. 49. ISBN 978-80-7278-873-6. ISSN 978-80-7278-873-6. Dostupné z: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://mocr.mo.gov.cz/images/id_40001_50000/46088/KVA_R_2035_Final.pdf. [cit. 2025-02-26].

Kybernetická bezpečnost počítačových systémů AČR, 2024. Diplomová práce. Česká republika: Vysoká škola logistiky o.p.s.

Kybernetická bezpečnost ve firmách. Tři pilíře pro efektivní ochranu před kyberútoky, 2022. Online. BOZP.cz. 14. 03. 2022. Dostupné z: <https://www.bozp.cz/aktuality/kyberneticka-bezpecnost-ve-firmach/>. [cit. 2025-03-13].

Kybernetická bezpečnost ve firmách. Tři pilíře pro efektivní ochranu před kyberútoky, 2022. Online. BOZP.cz. 14. 03. 2022. Dostupné z: <https://www.bozp.cz/aktuality/kyberneticka-bezpecnost-ve-firmach/>. [cit. 2025-03-13].

Machine learning in manufacturing and industry 4.0 applications, 2021. Online. *International Journal of Production Research*. Vol. 59, no. 16, s. 6. Dostupné z: <https://www.tandfonline.com/doi/epdf/10.1080/00207543.2021.1956675?needAccess=true>. [cit. 2025-03-31].

MAŘÍK, Vladimír. *Průmysl 4.0: výzva pro Českou republiku*. Praha: Management Press, 2016. ISBN 978-80-7261-440-0.

Moderní a efektivní přístup ke školení BOZP prostřednictvím virtuální reality, 2021. Výzkumný ústav bezpečnosti práce.

NEUGEBAUER, Tomáš, 2016. *Bezpečnost a ochrana zdraví při práci v kostce*. 2. Česká republika: Wolters Kluwer. ISBN 978-80-7552-107-1.

Prediktivní údržba: definice, výhody, příklady ... to vše jedním kliknutím!, © igus, 2025. Online. Igus. Dostupné z: <https://www.igus.cz/smart-maintenance/predictive-maintenance/definice-vhod-a-priklady?>. [cit. 2025-03-17].

Prediktivní údržba: definice, výhody, příklady ... to vše jedním kliknutím!, © igus, 2025.

Online. Igus. Dostupné z: <https://www.igus.cz/smart-maintenance/predictive-maintenance/definice-vhod-a-priklady?>. [cit. 2025-03-17].

Průmysl 4.0, Copyright © 2016 - 2025. Online. Znalostní systém prevence rizik v BOZP. Dostupné z: <https://zsbozp.vubp.cz/prumysl-4-0-uvod-do-problematiky>. [cit. 2025-03-17].

Reaper Drones: The new close Air Support Weapon, 2017. Online. In: Breaking Defense. Dostupné z: <https://breakingdefense.com/2017/05/reaper-drones-the-new-close-air-support-weapon/>. [cit. 2025-03-26].

Ripsaw M5: Robotická hvězda akčních filmů pro americkou armádu, 2019. Online. In: Armádní noviny. Dostupné z: <https://www.armadninoviny.cz/ripsaw-m5-roboticka-hvezda-akcnich-filmu-pro-americkou-armadu.html>. [cit. 2025-03-26].

Robotic system for palletising and depalletising products, 2023. Online. *European Agency for Safety and Health at Work*. S. 11. Dostupné z: <https://healthy-workplaces.osha.europa.eu/en/publications/robotic-system-palletising-and-depalletising-products-id7>. [cit. 2025-03-30].

Robotizace a automatizace: Klíč k budoucnosti, 2024. Online. TGS. Dostupné z: <https://tgs.cz/blog/robotizace-a-automatizace-klic-k-budoucnosti-n468465.htm?>. [cit. 2025-03-17].

RQ-11B Raven, © 2025 Military Advantage. Online. In: MILITARY.COM. Dostupné z: <https://www.military.com/equipment/rq-11b-raven>. [cit. 2025-03-26].

Ruská armáda zavedla do výzbroje bojové roboty Uran-9, © 2018 - 2025 Armadninoviny.cz. Online. In: Armádní noviny. Dostupné z: <https://www.armadninoviny.cz/ruska-armada-zavedla-do-vyzbroje-bojove-roboty-uran-9.html>. [cit. 2025-03-26].

Security and Military Relevancies of Digitisation, Globalisation and Cyberspace, 2021. Online. *Security and Military Relevancies of Digitisation, Globalisation and Cyberspace*. Vol. 20, no. 1, s. 81-93. Dostupné z: http://epa.niif.hu/04200/04298/00023/pdf/EPA04298_AARMS_2021_1.pdf#page=83. [cit. 2025-04-12].

SMART DIGITAL SYSTEMS FOR IMPROVING WORKERS' SAFETY AND HEALTH, 2023-2025. Online. *European Agency for Safety and Health at Work*. S. 14. Dostupné z: <https://healthy-workplaces.osha.europa.eu/cs/publications/smart-headband-fatigue-risk-monitoring-smart-digital-systems-improving-workers-safety-and-health>. [cit. 2025-04-12].

SMART DIGITAL SYSTEMS FOR IMPROVING WORKERS' SAFETY AND HEALTH, 2024. Online. *European Agency for Safety and Health at Work*. S. 10. Dostupné z: https://healthy-workplaces.osha.europa.eu/en/publications/smart-armband-real-time-data-analysis-health-and-safety-smart-digital-systems-improving-workers-safety-and-health?utm_source=chatgpt.com. [cit. 2025-03-30].

Smart digital systems: implications for occupational safety and health, 2025. Online. In: Evropská agentura pro bezpečnost a ochranu zdraví při práci. Dostupné z: <https://osha.europa.eu/cs/publications/smart-digital-systems-implications-occupational-safety-and-health>. [cit. 2025-03-13].

STANĚK, Peter, Vladimír MAŘÍK, Dušan DOLIAK a Adrián ONDROVIČ. *Fakta a mýty o společnosti 5.0: zamyslenie se nad budúcnosťou*. Bratislava: Wolters Kluwer, 2019. ISBN 978-80-571-0057-7.

Study on artificial intelligence: The state of the art and future prospects, 2021. Online. *Nature Medicine*. No. 23, s. 8. ISSN Journal of Industrial Information Integration. Dostupné z: <https://www.sciencedirect.com/science/article/abs/pii/S2452414X21000248?via%3Dihub>. [cit. 2025-03-31].

Systémy C4ISTAR pozemních sil. Online. In: SKUPINA ICZ. Dostupné z: <https://www.iczgroup.com/produkty-a-sluzby/obrana/systemy-c4istar-pozemnich-sil/>. [cit. 2025-03-26].

Školení BOZP a PO ve virtuální realitě, © 2025 VR Education. Online. VR Education. Dostupné z: <https://vreducation.cz/skoleni-bozp-a-po-ve-virtualni-realite/>. [cit. 2025-03-17].

TACTICAL COMMUNICATION AND PROTECTIVE SYSTEM, 2019. Online. In: Program Executive Office Soldier. Dostupné z: <https://www.peosoldier.army.mil/News/Photos/igphoto/2002299767/>. [cit. 2025-03-27].

Tactix® Delta - Solar Edition with Ballistics. Online. Garmin. Dostupné z: <https://www.garmin.com/cs-CZ/p/733535>. [cit. 2025-04-14].

The future of work: How innovation and digitalization re-shape the workplace. Online. *Journal of Innovation & Knowledge*. S. 7. ISSN 2444-569X. [cit. 2025-04-12].

Types of cloud computing, 2022. Online. Red Hat. July 25, 2022. Dostupné z: <https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud>. [cit. 2025-02-17].

Umělá inteligence v bojových simulacích: Jak AI mění výcvik vojáků NATO a AČR. Online. *CZ Defence*. S. 2024. Dostupné z: <https://www.czdefence.cz/clanek/umela-inteligence-v-bojovych-simulacich-jak-ai-meni-vycvik-vojaku-nato-a-acr>. [cit. 2025-02-27].

Velká data (big data): definice, výhody a výzvy (infografika), 2021. Online. Evropský parlament. 2023. Dostupné z: <https://www.europarl.europa.eu/topics/cs/article/20210211STO97614/velka-data-big-data-definice-vyhody-a-vyzvy-infografika>. [cit. 2025-04-11].

Virtual Battlespace 2 (VBS2), Copyright © 2025. Online. In: Andrew Barron. Dostupné z: <https://andrewbarron.net/projects/vbs2/>. [cit. 2025-03-26].

Vše, co potřebujete vědět o cloudu, Copyright © 2025 - Algotech a.s.. Online. Algotech. Dostupné z: <https://www.algotech.cz/novinky/vse-co-potrebuje-vedet-o-cloudu>. [cit. 2025-02-17].

What is Big Data? Online. Google Cloud. Dostupné z: <https://cloud.google.com/learn/what-is-big-data>. [cit. 2025-04-11].

What is blockchain? Online. IBM – United States. Dostupné z: <https://www.ibm.com/think/topics/blockchain>. [cit. 2025-04-11].

What is the Internet of Things (IoT)?, 2022. Online. In: LinkedIn. Dostupné z: <https://www.linkedin.com/pulse/what-internet-things-iot-juan-camilo-arce-garc%C3%ADa>. [cit. 2025-04-11]. Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion, Copyright © 2025. Online. *Government Information Quarterly*. Roč. 38, č. 2, s. 15. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0740624X21000046>. [cit. 2025-04-11].

WINTER, Johannes, 2023. *Industry 4.0 - The Global Industrial Revolution*. CC BY-NC-ND license. ISBN 978-3-0365-9663-1.

SEZNAM OBRÁZKŮ

Obrázek 1 – Školení zaměstnanců pomocí VR (How to Prepare and Guide Employees for VR Training?, © 2025 Visartech).....	22
Obrázek 2 – Internet věcí (What is the Internet of Things (IoT)?, 2022).....	26
Obrázek 3 – Cloud computing (3 typy cloud computingu: SaaS, PaaS, IaaS, © 2025).....	30
Obrázek 4 – Strojové učení (Co je to strojové učení?, © 2025 SAP).....	33
Obrázek 5 – Systémy C4ISTAR pozemních sil (Systémy C4ISTAR pozemních sil).....	51
Obrázek 6 – RQ-11 Raven (RQ-11B Raven, © 2025 Military Advantage).....	53
Obrázek 7 – MQ-9 Reaper (Reaper Drones: The new close Air Support Weapon, 2017)..	54
Obrázek 9 – Ripsaw M5 (Ripsaw M5: Robotická hvězda akčních filmů pro americkou armádu, 2019).....	55
Obrázek 8 – Ruský Uran-9 (Ruská armáda zavedla do výzbroje bojové roboty Uran-9, © 2018 - 2025 Armadninoviny.cz).....	55
Obrázek 10 – Virtual Battlespace System (Virtual Battlespace 2 (VBS2), Copyright © 2025).....	58
Obrázek 11 – 3M PELTOR (EEP-100 EU 3M PELTOR, Copyright 2025).....	60
Obrázek 12 – Taktický komunikační a ochranný systém (TACTICAL COMMUNICATION AND PROTECTIVE SYSTEM, 2019).....	61
Obrázek 13 – QR kód Dotazníkového šetření	86
Obrázek 14 – Grafické znázornění otázky týkající se působnosti firmy (zdroj Microsoft Forms).....	87
Obrázek 15 – Grafické znázornění týkající se počtu zaměstnanců ve firmě (zdroj Microsoft Forms).....	87
Obrázek 16 – Grafické znázornění otázky týkající se působnosti firmy (zdroj Microsoft Forms).....	88
Obrázek 17 – Grafické znázornění otázky týkající se digitálních technologií zavedené ve firmě (zdroj Microsoft Forms).....	88
Obrázek 18 – Grafické znázornění otázky týkající se dopadu digitálních technologií na BOZP (zdroj Microsoft Forms)	89
Obrázek 19 – Grafické znázornění otázky týkající se zlepšení prevence rizik (zdroj Microsoft Forms).....	89
Obrázek 20 – Grafické znázornění otázky týkající se evidování úrazů před a po zavedení digitálních technologií (zdroj Microsoft Forms)	90
Obrázek 21 – Grafické znázornění otázky týkající se přínosů digitalizace BOZP (zdroj Microsoft Forms).....	90
Obrázek 22 – Grafické znázornění otázky týkající se hlavních problémů a výzev spojené se zavedením digitálních prvků (zdroj Microsoft Forms).....	91
Obrázek 23 – Grafické znázornění otázky týkající se procesních nedostatků po implementaci (zdroj Microsoft Forms).....	91

Obrázek 24 – Grafické znázornění otázky týkající se konkrétních nedostatků (zdroj Microsoft Forms)	92
Obrázek 25 – Grafické znázornění otázky týkající se zavedení dalších prvků digitalizace (zdroj Microsoft Forms).....	92
Obrázek 26 – Grafické znázornění otázky týkající se zavedení dalších konkrétních prvků digitalizace (zdroj Microsoft Forms)	93
Obrázek 27 – Graf závislosti digitálních technologií vůči velikosti organizace (vlastní) ..	94
Obrázek 28 – Graf závislosti mezi zavedením digitálních technologií a jejich znovuzavedením (vlastní)	95
Obrázek 29 – Graf závislost mezi hodnocením dopadů aplikace digitálních technologií a procesních nedostatků při jejich zavádění (vlastní)	96
Obrázek 30 – Fáze Road Map (vlastní)	97

SEZNAM TABULEK

Tabulka 1 – Porovnání prvků digitalizace (vlastní).....	45
---	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Umělá inteligence
AR	Rozšířená realita
BankID	Bankovní identita
BIM	Construction and Building Management
BOZP	Bezpečnost a ochrana zdraví při práci
CT	Výpočetní tomografie
ČR	Česká republika
DL	Hluboké učení (Deep Learning)
eID	Elektronická identifikace
EW	Elektronický boj
FMN	Federated Mission Network
GDPR	Obecné nařízení o ochraně osobních údajů
GPS	Global Positioning System
IAM	Identita a správa přístupu
IoT	Internet věcí
IT	Informační technologie
KHS	Krajská hygienická stanice
MFA	Multifaktorová autentizace
ML	Strojové učení
MRI	Magnetická rezonance
NCKO	Národní centrum kybernetických operací
OIP	Oblastní inspektorát práce
OOPP	Osobní ochranné pracovní prostředky
PoW	Proof of Work
RFID	Radiofrekvenční identifikace

RPA	Robotická automatizace procesů
SAP	Vývoj programu systémové analýzy
SÚIP	Státní úřad inspekce práce
TMS	Systém řízení dopravy
VOSS	Verbeterd Operationeel Soldaat System
VR	virtuální realita

SEZNAM PŘÍLOH

Příloha P I: Dotazníkové šetření

Příloha P II: Road Map

PŘÍLOHA P I: DOTAZNÍKOVÉ ŠETŘENÍ

Dotazník

Vážený/á pane/paní, ráda bych Vás požádala o vyplnění tohoto průzkumu, který se zaměřuje na implementaci digitálních technologií v oblasti bezpečnosti a ochrany zdraví při práci (BOZP) ve vaší organizaci. Cílem průzkumu je získat přehled o tom, jaké digitální technologie jsou využívány k zajištění bezpečnosti na pracovišti, jaké přínosy přinášejí a jaké výzvy související s jejich implementací firmy čelí. Vaše odpovědi mi pomohou lépe pochopit aktuální stav digitalizace v oblasti BOZP a přispějí k optimalizaci bezpečnostních procesů. Dotazník je anonymní a jeho vyplnění Vám zabere přibližně 5 minut. Veškeré informace budou využity výhradně pro účely analýzy a výzkumu pro praktický podklad diplomové práce, která se zabývá „Prvky digitalizace a jejich vliv na zajištění bezpečnosti a ochrany zdraví při práci zaměstnanců“. Děkuji za Vaši ochotu se zapojit do tohoto průzkumu a za váš čas.

Úvodní informace



1. 1. Působnost vaší firmy se nachází na území:

- ☐ České republiky
- ☐ Slovenské republiky

2. Kolik má vaše organizace zaměstnanců?

- ☐ Méně než 50
- ☐ 50-99
- ☐ 100-249
- ☐ 250-499
- ☐ 500-999
- ☐ 1000 a více

3. V jakém průmyslovém odvětví působí vaše organizace? 

- ☐ Výroba
- ☐ Stavebnictví
- ☐ Doprava a logistika
- ☐ Zdravotnictví
- ☐ IT a telekomunikace
- ☐ Služby
- ☐ Energetika
- ☐ Zemědělství
- ☐ Jiné

4. Jaké digitální technologie jsou ve vaší organizaci implementovány? (Vyberte všechny relevantní možnosti.) 

- ☐ Kolaborativní roboti
- ☐ Senzory pro prevenci rizik
- ☐ Nositelné technologie (chytré přilby, náramky – sledování zdravotního stavu, přetížení nebo vyčerpání, upozornění na vystavení nebezpečným materiálům)
- ☐ Digitální školení zaměstnanců (VR, online simulace)
- ☐ Digitální platformy pro možnost práce z domova
- ☐ Inteligentní systémy pro monitoring pracovního prostředí
- ☐ Nemáme implementovány žádné digitální technologie
- ☐ Jiné

5. Jak hodnotíte dopad těchto digitálních technologií na zajištění bezpečnosti a ochrany zdraví při práci (BOZP) ve vaší organizaci? 

- ☐ Velmi pozitivní
- ☐ Pozitivní
- ☐ Neutrální
- ☐ Negativní
- ☐ Velmi negativní

6. Zaznamenali jste po zavedení digitálních technologií zlepšení v oblasti prevence rizik na pracovišti? 

- ☐ Ano, výrazné zlepšení
- ☐ Ano, mírné zlepšení
- ☐ Žádná změna
- ☐ Došlo ke zhoršení
- ☐ Nedokážu posoudit

7. Evidujete ve vaší organizaci počet pracovních úrazů před a po zavedení digitálních technologií? 

- ☐ Ano, máme údaje za obě období
- ☐ Máme údaje pouze za období před zavedením
- ☐ Máme údaje pouze za období po zavedení
- ☐ Ne, údaje neevidujeme / nejsou k dispozici
- ☐ Jiné

8. Jaké konkrétní přínosy v oblasti BOZP přinesla digitalizace ve vaší organizaci? (Vyberte všechny relevantní možnosti.) 

- ☐ Zvýšení bezpečnosti pracovníků
- ☐ Lepší monitoring a analýza rizik
- ☐ Snižování počtu pracovních úrazů
- ☐ Zvýšení efektivity školení BOZP
- ☐ Rychlejší reakce na mimořádné situace
- ☐ Jiné

9. Jaké hlavní výzvy nebo problémy jste při implementaci digitálních technologií v oblasti BOZP zaznamenali? (Vyberte všechny relevantní možnosti.) 

☐ Vysoké náklady na implementaci

☐ Odpor zaměstnanců ke změnám

☐ Nedostatečná technická podpora

☐ Legislativní a regulační překážky

☐ Nedostatek interních odborníků

☐ Jiné

10. Setkali jste se při implementaci digitálních technologií s procesními nedostatky? 

☐ Ano, výrazné nedostatky

☐ Ano, mírné nedostatky

☐ Žádné nedostatky

☐ Ne, došlo k mírnému zlepšení

☐ Ne, došlo k výraznému zlepšení

11. Jaké konkrétní procesní nedostatky jste zaznamenali při implementaci digitálních technologií? (Vyberte všechny relevantní možnosti.) 

- ☐ Nedostatečné proškolení zaměstnanců
- ☐ Nízká míra zapojení zaměstnanců do změn
- ☐ Nedostatečné plánování a příprava implementace
- ☐ Špatná komunikace mezi odděleními
- ☐ Nedostatečná technická podpora nebo zázemí
- ☐ Nepřesné nebo neaktuální data
- ☐ Zdlouhavé rozhodovací procesy
- ☐ Jiné

12. Plánujete implementovat další prvky digitalizace? 

- ☐ Ano, v nejbližších 12 měsících
- ☐ Ano, v horizontu 1-3 let
- ☐ Ano, ale zatím bez konkrétního časového plánu
- ☐ Ne, v současnosti neplánujeme

13. Pokud plánujete zavedení dalších digitálních technologií, o jaké konkrétní prvky se jedná? (Vyberte všechny relevantní možnosti.) 

- ☐ Kolaborativní roboti
- ☐ Senzory pro monitoring rizik
- ☐ Nositelné technologie pro ochranu zdraví a bezpečnost (chytré přilby, náramky apod.)
- ☐ Pokročilá data analýza a prediktivní modely
- ☐ Digitální školení zaměstnanců (např. VR)
- ☐ Rozšířená a virtuální realita pro simulaci rizik
- ☐ Digitální nástroje pro řízení BOZP
- ☐ Digitální platformy pro flexibilní práci (home office)
- ☐ Neplánujeme zavedení dalších digitálních technologií

PŘÍLOHA P II: ROAD MAP



Prvky Digitalizace



Digitální školení zaměstnanců



Kolaborativní roboti



Senzory pro prevenci rizik



Home office



Intelligentní systémy na monitoring pracovního prostředí

TIME LINE

1

Zmapování aktuálního stavu

➤ Audit technologií a úrazovosti

2

Výběr vhodných technologií

➤ Zhodnocení přínosu a nákladů

3

Pilotní testování

➤ Workshops, školení

4

Implementace do celé organizace

➤ Rozšíření ověřených prvků

5

Průběžné vyhodnocení

➤ Monitoring, aktualizace

PŘÍNOSY DIGITALIZACE



Vyšší efektivita



Uspadnění komunikace



Neujede Vám vlak



Standardizace procesu



Podklady pro rozhodování



Prevence rizik