

**vstupní vzdělávání následné**

**rozšiřující texty**

**ministerstvo vnitra**

**sekce pro státní službu**

**praha 2024**



MINISTERSTVO VNITRA  
sekce pro státní službu

**Rozšiřující texty**  
v rámci Vstupního vzdělávání následného  
kolektiv autorů

P R A H A

Ú N O R 2 0 2 4



### Vysvětlení piktogramů



definice



citace



literatura

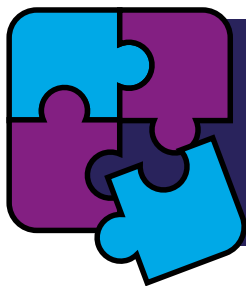


# Obsah

<b>1. Projektové řízení.....</b>	<b>9</b>
Cíl projektového řízení.....	9
Přípravná fáze projektu.....	10
Metoda logického rámce.....	11
WBS - Work Breakdown Structure.....	12
Tvorba harmonogramu projektu.....	12
Plán komunikace.....	13
Realizace (implementace) projektu.....	13
Ukončení projektu.....	13
<b>2. Inovace ve veřejném sektoru.....</b>	<b>15</b>
Definice inovací.....	15
Oslo manuál.....	15
Rozdíl mezi inovacemi ve veřejném a soukromém sektoru.....	16
Kde hledat pomoc a inspiraci.....	18
Mezinárodní úsilí - Deklarace o inovacích ve veřejném sektoru.....	18
<b>3. Umělá inteligence.....</b>	<b>19</b>
Úvod do umělé inteligence.....	19
Počátky umělé inteligence.....	19
Definice umělé inteligence.....	19
Typy a podobory umělé inteligence.....	20
Strojové učení (Machine Learning).....	21
Neuronové sítě (Neural Networks).....	21
Hluboké učení (Deep Learning).....	22
Zpracování přirozeného jazyka (Natural Language Processing, dále také „NLP“ ).....	22
Velké jazykové modely (Large Language Models, dále také „LLM“ ).....	23
Počítačové vidění (Computer Vision).....	23
Robotika (Robotics).....	24
Společenské dopady umělé inteligence.....	24
Přínosy.....	24
Rizika.....	25
AI ve veřejné sféře.....	26
Reakce na dopady AI.....	26
Etika.....	27
Legislativa v oblasti umělé inteligence.....	27
Národní strategie umělé inteligence České republiky.....	27
<b>4. Zvyšování odolnosti státní správy proti nelegitimnímu ovlivňování.....</b>	<b>29</b>
Co to je nelegitimní ovlivňování.....	29
Týká se státních zaměstnanců nelegitimní ovlivňování?.....	30
Jak nelegitimní ovlivňování rozpoznat a jak postupovat.....	31
Je nutné zjišťovat kdo je útočníkem?.....	32
Hlavní zásady.....	32







# Projektové řízení

1

## CÍL PROJEKTOVÉHO ŘÍZENÍ

Cílem projektového řízení<sup>1)</sup> je úspěšná realizace projektu. Projekty jsou prostředkem pro uskutečnění změny, jsou svou povahou jedinečné, a proto se vyznačují vyšší mírou rizika oproti běžným provozním činnostem organizace.

cíl

Projektové řízení je proces, ve kterém jednotlivci nebo organizace využívají své zdroje k realizaci projektů. Jedná se o způsob plánování a realizace aktivit, které je potřeba uskutečnit v požadovaném termínu s plánovanými náklady tak, aby bylo dosaženo nadefinovaných cílů.

## PROJEKT



Projekt je jedinečný **časově** (s jasně ohraničeným začátkem a koncem), **nákladově a zdrojově omezený proces koordinovaných činností realizovaný za účelem vytvoření definovaných výstupů co do kvality, standardů a požadavků.**

projekt

## PROJEKTOVÁ KANCELÁŘ



Projektová kancelář je organizační jednotka určená k centrální koordinaci jí určených projektů.

projektová kancelář

## METODIKA PROJEKTOVÉHO ŘÍZENÍ



Metodika projektového řízení je **interním nástrojem organizace, který popisuje způsob a rozsah nastavení systému projektového řízení v organizaci.** Jedná se o individualizovaný popis řízení projektů dle reálných podmínek organizace. Tato metodika může rámcově vycházet z mezinárodních metodik a standardů.

metodika  
projektového řízení

Cílem metodiky je ukotvení systému projektového řízení v rámci dané instituce veřejné správy, a to prostřednictvím zřízení tzv. projektových týmů jako centrální funkční jednotky, která bude řídit veškeré projekty realizované veřejným subjektem.

Metodika specifikuje požadavky na zapojení zaměstnanců dané instituce veřejné správy v rámci řízení projektů, definuje projektové role včetně způsobu zapojení jednotlivých členů projektových týmů, které jsou nezbytné pro úspěšnou realizaci projektů, a popisuje základní

<sup>1)</sup> Blíže vizte MINISTERSTVO PRO MÍSTNÍ ROZVOJ. Projektové řízení. Metodiky [online]. [cit. 2024-02-24]. Dostupné z: <https://mmr.gov.cz/getmedia/d81c5d81-4793-4c0f-818c-5488d55ae08f/Projektove-řízení-skripta.pdf.aspx?ext=.pdf>

procesy projektového řízení, systém komunikace a sledování kvality procesů. Součástí metodiky je rovněž soubor šablon pro potřeby řízení dokumentace k projektům (přílohy).

## PŘÍPRAVNÁ FÁZE PROJEKTU

Přípravná fáze projektu je stěžejní, protože dochází k vytváření základních předpokladů realizace projektu. Výchozím předpokladem je soulad projektu s vizí a cíli organizace identifikovaných v rámci strategického řízení. V návaznosti na odpovědnost top managementu, která se pohybuje v oblasti strategické, vzniká v této fázi projektu **odpovědnost manažera projektu** (nebo sponzora projektu):

- » stanovit cíle,
- » vytvořit návrh milníků,
- » specifikovat potřeby a požadavky,
- » určit náklady,
- » vytvořit harmonogram.

V případě realizace projektu v součinnosti s dodavatelem vzniká celá oblast dalších odpovědností, které jsou přeneseny na specialisty:

- » návrh ceny dle zadání požadavků,
- » rizika projektu směrem k dodavateli a návrh eliminace,
- » vytvoření návrhu smlouvy v oblasti předmětu a dalších relevantních oblastí, které je možné specifikovat v této fázi.

## ZAKLÁDACÍ LISTINA PROJEKTU/PROJEKTOVÝ ZÁMĚR/PROJEKTOVÁ FIŠE



Projektová fiše je souhrn informací o projektu, která slouží jako první vstupní informace k rozhodování o předběžném výběru projektu k realizaci. Současně dává projektová fiše základní informace o projektu ve větším, přesto však dostatečně přehledném rozsahu (doporučený rozsah je cca 2–10 stran).

Fiše projektu může sloužit jako základ pro přípravu projektu, případně projektové žádosti u projektů žádajících spolufinancování z fondů EU.

Pro realizaci každého projektu je nutno předem zřetelně specifikovat:

- » **zadavatele projektu** – kdo organizuje práce spojené s přípravou a realizací projektu,
- » **investora** – kdo zajistí financování projektu a z jakých zdrojů,
- » **uživatele projektu** – kdo bude uživatel a provozovatel výstupu projektu.

## OBECNÁ STRUKTURA ROZPOČTU

Struktura předběžného rozpočtu projektu závisí na tom, o jaký projekt se jedná, a může se projekt od projektu významně lišit.

Zde uvádíme základní obecnou strukturu předběžného rozpočtu:

- » název projektu,
- » předmět projektu,
- » hodnocení projektu z hlediska ekonomických ukazatelů,
- » rozložení nákladů podle jednotlivých druhů, etap (rozložení v čase) a jednotlivých organizačních jednotek případně dalších zapojených subjektů,
- » rozpis čerpání nákladů,
- » cash-flow včetně návrhu financování,
- » rizika.

## ANALÝZA RIZIK

V přípravné fázi projektu se analýza rizik zaměřuje na dvě úrovně rizik projektu:

- » **globální úroveň** – jedná se o zcela nový a novátorský projekt, a tedy také velmi rizikový projekt, nebo se jedná o projekt, který je podobný projektům již realizovaným, a tedy málo rizikový,
- » **projektová úroveň** – zvážení hlavních projektových rizik, která jsou interního i externího charakteru. Zde je třeba vytvořit soupis těchto rizik (například zajištění finančních prostředků z operačního programu – neschválení žádosti, změna legislativy apod.).

Dále je nezbytné posoudit, zda jsou veškerá identifikovaná rizika přijatelná, či nepřijatelná. V případě nepřijatelných rizik následuje úprava části projektu, která by znamenala hrozbu nepřijatelného rizika. V případě přijatelných rizik následuje vytvoření plánu jejich eliminace.

## METODA LOGICKÉHO RÁMCE

Jednou z metod, jak přehledně zmapovat záměry a očekávání a uvést je do souladu s konkrétními výstupy a činnostmi při realizaci projektu je metoda logického rámce. Je to postup, s jehož pomocí jsme schopni stručně, přehledně a srozumitelně popsat chystaný projekt.

Definování projektu s využitím metodiky logického rámce je základem pro řízení projektu. Logický rámec je vhodný pro identifikaci a analýzu problémů na straně jedné a definování

obecná struktura  
předběžného rozpočtu

analýza rizik

metoda logického  
rámce

cílů a stanovení konkrétních aktivit k řešení těchto problémů na straně druhé. Metodou logického rámce se připravovaný projekt testuje jak z hlediska vhodnosti a přiměřenosti pro řešení daného problému, tak z hlediska jeho proveditelnosti a trvalé udržitelnosti.

Výhody užití logického rámce projektu jsou:

- » celý projekt je jasně a stručně popsán na „jediném“ listu papíru (formulář logického rámce),
- » vypovídá o hlavním účelu projektu, výstupech a také o tom, jak lze těchto výstupů dosáhnout, které vnější vlivy mohou pomoci a které naopak uškodit,
- » z logického rámce lze usoudit, zda má projekt šanci na realizaci.

## WBS - WORK BREAKDOWN STRUCTURE

WBS

Při použití této metody plánování je hlavní otázkou CO chceme v projektu udělat (neřeší se JAK se daná činnost udělá, pouze CO se udělá). WBS definuje hranice projektu a stoprocentní rozsah projektu; tato metoda je vhodná jako obrana proti „přetečení“ projektu (tzv. *Scope Creep* – rozsah projektu nepřetržitě a nekontrolovaně roste, a to kdykoliv po jeho zahájení).

## TVORBA HARMONOGRAMU PROJEKTU

harmonogram

Harmonogram představuje časovou souslednost jednotlivých kroků projektu (tedy všech etap, aktivit, činností, úkolů apod.). Čas projektu je zde zachycen ze dvou hledisek:

- » kdy budou jednotlivé kroky realizovány,
- » jak dlouho budou realizovány.

**Ideální harmonogram** projektu má:

- » přiřazeny zdroje pro jednotlivé kroky,
- » milníky a důležité body projektu,
- » jasnou formu a strukturu, která umožní rychlou a přehlednou orientaci (například forma tabulky),
- » určeno jednotné časové měřítko (například dny, týdny nebo měsíce),
- » stanovení odpovědnosti,
- » uvedeny dílčí výstupy,
- » časové informace nezbytné pro koordinaci činností, které bezprostředně souvisí s projektem (významný prvek v komunikační rovině, vstup v podobě nového softwaru, který bude v projektu dále využíván apod.).

## PLÁN KOMUNIKACE

Plán komunikace projektu se obvykle sestavuje u velkých, rizikových a náročných projektů, kdy je třeba mít jasně určeno:

- » jaké informace budou komunikovány a komu,
- » jak často bude komunikace probíhat (včetně formy a časových limitů pro reakci),
- » odpovědnost při komunikaci,
- » forma komunikace,
- » archivace, bezpečnost informací.

plán komunikace

## REALIZACE (IMPLEMENTACE) PROJEKTU

neboli **fáze vlastní realizace projektu** zahrnuje následující hlavní činnosti:

- » řízení prací a subdodávek,
- » kontrola postupu podle časového plánu a rozpočtu,
- » řízení komunikace,
- » řízení projektové dokumentace,
- » kontrola kvality a účinnosti dosažení jednotlivých dílčích cílů,
- » testování výstupu projektu a komparace s plánovanými hodnotami.

fáze vlastní realizace

Dále následuje PROVOZ PROJEKTU – **fáze vlastního užívání předmětu projektu**, kdy:

- » dochází k začlenění předmětu projektu do existujících organizačních systémů uživatele projektu,
- » probíhá hodnocení technologických, sociálních a ekonomických dopadů realizovaného projektu v rámci předpokladů daných v návrhu projektu,
- » je zpracována zpětná vazba pro plánování dalších projektů,
- » probíhá průběžné vyhodnocení projektu (například na roční bázi).

fáze vlastního užívání

Během této fáze je tedy monitorována realizace, výstupy a výsledky projektu.

## UKONČENÍ PROJEKTU

Ukončením projektu chápeme veškeré činnosti, které vedou k dokončení veškerých aktivit projektu, předání a schválení výstupů projektu a uzavření veškerých administrativních

ukončení projektu

náležitostí, které s realizací projektu souvisely (například archivace, provedení inventury, vyhodnocení projektu apod.).

Prostřednictvím schválení výstupů projektu je realizována závěrečná akceptace projektu, bez níž nemůže dojít k úspěšnému ukončení projektu. U složitých a dlouhodobých projektů jsou běžně schvalovány dílčí akceptační kritéria po dosažení určité fáze projektu. Tento přístup s sebou nese vyšší nároky na zdroje, ale rovněž přináší obrovské snížení rizika projektu, kdy v závěru realizace nemůže nastat nečekaný nesouhlas s projektem.

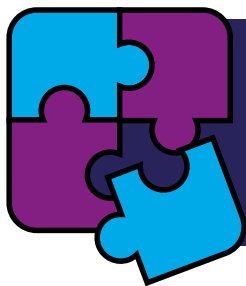
Za úspěšně ukončený projekt je možné považovat projekt, který:

- » naplnil cíle projektu,
- » přinesl realizaci předmětu projektu,
- » má realizovány administrativní úkony a vytvořeny závěrečné dokumenty, které obsahují také hodnocení projektu.



## ROZŠIŘUJÍCÍ LITERATURA

- (1) Projektové řízení (skripta). Dostupné z <https://mmr.gov.cz/getmedia/d81c5d-81-4793-4c0f-818c-5488d55ae08f/Projektove-rizeni-skripta.pdf.aspx?ext=.pdf>



# Inovace ve veřejném sektoru

2

## Definice inovací

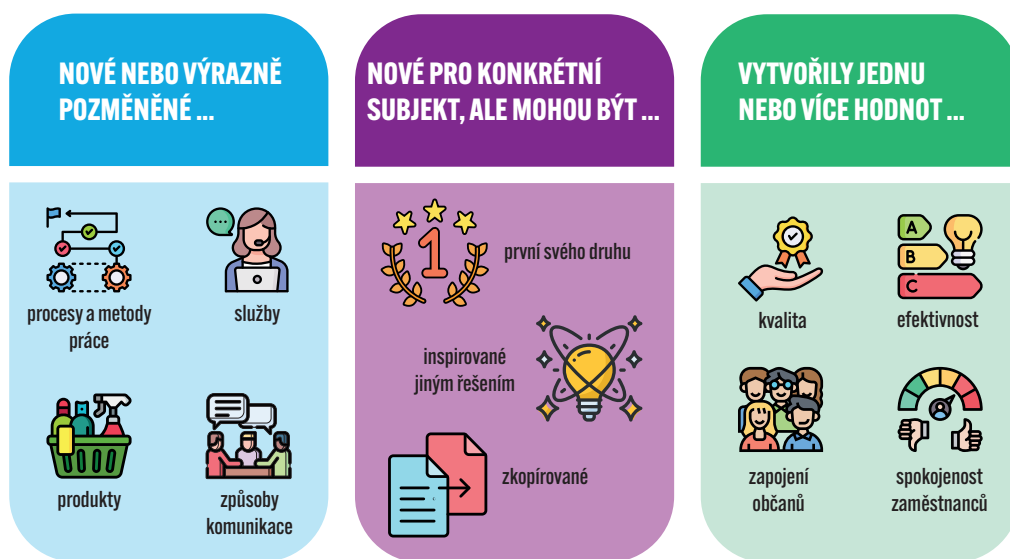
Inovace jsou nástrojem zvyšování kvality a efektivity veřejné správy. Inovacemi se zvyšuje kvalita služeb pro občany a zlepšují se podmínky výkonu práce pro pracovníky veřejné správy.

Inovace je nový nebo podstatně zdokonalený produkt nebo proces (nebo kombinace obou), který se významně liší od předchozího produktu nebo procesu **dané entity** a který je zpřístupněn potenciálním uživatelům (produkt) nebo uveden do používání danou entitou (proces).<sup>1)</sup>



**Inovací je tedy proces, kterým se zlepšuje buď vnitřní chod úřadu nebo se realizuje věcná agenda, a to jak v samotném procesu realizace, tak v jejím výsledku.**

definice inovace



Zdroj: <https://innovationbarometer.org/copenhagen-manual/>

## Oslo manuál

Tzv. *Oslo manuál* je základní metodickou pomůckou Organizace pro hospodářskou spolupráci a rozvoj (OECD), která definuje jednotlivé pojmy v oblasti inovací, takže jsou v zemích OECD používány se stejným významem. To umožňuje realizovat měření inovací a provádět jejich mezinárodní srovnání. Inovace jsou významným parametrem konkurenceschopnosti

Oslo manuál



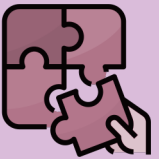





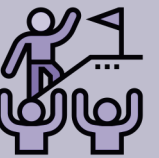

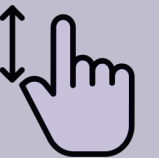

<sup>1)</sup> OECD. Oslo manual 2018. *OECD. The Measurement of Scientific, Technological and Innovation Activities* [online]. 2018, 2018-10-22 [cit. 2024-02-24]. Dostupné z: <https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm>

jednotlivých zemí, rovněž firem a také veřejného sektoru, či veřejné správy. Kvalita a inovativnost veřejné správy je stále více považována za součást konkurenceschopnosti země, proto byla původní definice v OECD manuálu rozšířena také pro veřejný sektor.

Pojem **inovace** je často spojován s termíny **výzkum a vývoj**, protože inovace často bývají výsledkem výzkumné práce, která vede k novým tržním produktům. Neplatí to však obecně. Podobně jsou v současnosti inovace významně spojeny s digitalizací, resp. digitálními službami,<sup>2)</sup> nicméně digitální služby jsou jen částí procesu inovací.

## Rozdíl mezi inovacemi ve veřejném a soukromém sektoru

Rozdíl nejlépe vyjadřuje následující schéma:<sup>3)</sup>

VEŘEJNÝ VERS. SOUKROMÝ SEKTOR	LOGIKA	ÚČEL	KOPÍROVÁNÍ	EXTERNÍ SPOLUPRÁCE	TENDENCE K RIZIKU
 VEŘEJNÝ	 politici	 přínos pro společnost	 volné	 převážně horizontální	 nízká
 SOUKROMÝ	 trh	 konkurenční výhoda	 duševní vlastnictví	 převážně vertikální	 vysoká

Zdroj: Inspirováno Kodaňským manuálem

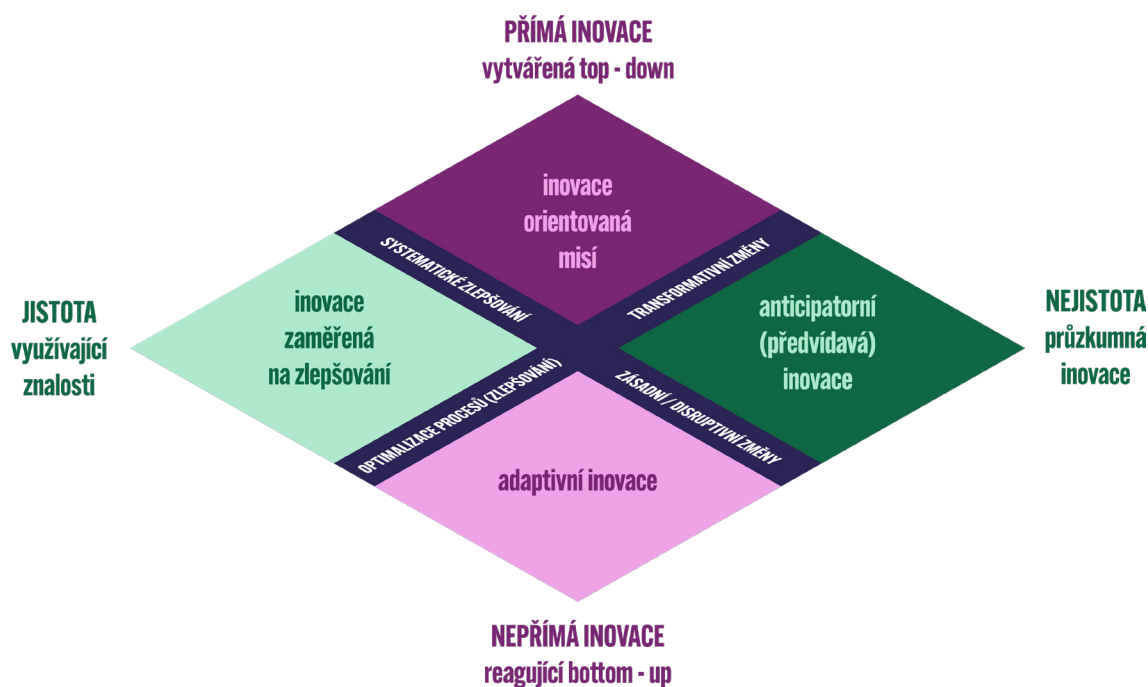
V soukromém sektoru inovují firmy většinou na základě požadavků trhu. Důvodem je konkurenceschopnost, potřeba uspět v soutěži o trh a zákazníka. Proto usilují o nová řešení, která chrání před ostatními a při jejich tvorbě omezují spolupráci s vnějšími subjekty. Rozhodnutím o uvedení inovace na trh riskují neúspěch (se všemi ekonomickými důsledky).

Ve veřejném sektoru, kdy inovace vzniká na základě strategických (politických) rozhodnutí, kde cílem je veřejné dobro a zvyšování kvality veřejných služeb, je naopak žádoucí informace o inovacích šířit, sdílet a s partnery spolupracovat. Riziko neúspěchu je tak malé.

<sup>2)</sup> Viz zejména zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění zákona č. 36/2021, zákona č. 261/2021 Sb., zákona č. 471/2022 Sb. a zákona č. 1/2024 Sb. Dostupné z <https://www.e-sbirka.cz/sb/2020/12/0000-00-00?f=12%2F2020&zalozka=text>

<sup>3)</sup> INNOVATION BAROMETER. *Copenhagen Manual* [online]. 2018-10-22 [cit. 2024-02-24]. Dostupné z: <https://innovationbarometer.org/copenhagen-manual/>





## Typy inovací ve veřejném sektoru<sup>4)</sup>

Observatory of Public Sector Innovation OECD (OPSI), pracoviště OECD zřízené pro podporu inovací ve veřejném sektoru a sdílení dobré praxe, rozlišuje na obrázku uvedené čtyři typy inovací ve veřejném sektoru. Ty se liší ve způsobu řízení a složitostí, zároveň v očekávaném výsledku. Podle toho, jaké typy inovací se ve veřejném sektoru uskutečňují, dochází k (jednorázové) optimalizaci procesů, systematickému zlepšování (k procesu změn), k transformativním nebo zásadním (disruptivním) změnám. Předpokládá se, že stát bude rozvíjet všechny čtyři typy inovací.

**Inovace zaměřená na vylepšení** (*Enhancement-oriented Innovation*) je inovace s vysokou pravděpodobností úspěchu. Je zaměřena na vylepšení stávající praxe, zavřených postupů a metod práce. Z principu je tedy často využívána v interních procesech úřadů.

**Adaptivní inovace** (*Adaptive Innovation*) je reakcí na změnu situace, změnu okolního prostředí, hrozbu nebo nové politické zadání. Znamená testování nového řešení nebo zavádění nových přístupů, např. na základě podnětů občanů nebo jejich zpětné vazby. Občané se takto zapojují do procesu tvorby inovace.

**Inovace orientovaná misí** (*Mission-oriented Innovation*) je koncept, kdy je definována nějaká mise - ambiciózní, měřitelný a časově ohraničený cíl, který přináší celospolečenskou změnu. Předem není jednoznačně definováno, jakými opatřeními lze cíle dosáhnout. K dosažení jsou podporovány všechny možné projekty a iniciativy, které k jeho naplnění přispějí. *Příkladem mise EU v oblasti výzkumu je 100 uhlíkově neutrálních evropských měst do roku 2030, což přispěje k hlavnímu cíli EU – uhlíkové neutralitě do roku 2050.*

<sup>4)</sup> OBSERVATORY OF PUBLIC SECTOR INNOVATION. *Publication Tag: Facets Brief* [online]. 2021, 2021-10-27 [cit. 2024-02-24]. Dostupné z: <https://oecd-opsi.org/publication-tags/facets-brief/>

typy inovací ve veřejném sektoru

inovace zaměřená na vylepšení

adaptivní inovace

inovace orientovaná misí

**Anticipatorní („předvídavá“) inovace** (*Anticipatory Innovation*) reaguje na trend nebo pravděpodobný budoucí problém (např. mění se trh práce z důvodu stárnutí populace). Tato inovace je spojena s vysokou mírou nejistoty a možným rizikem, protože jejím účelem je úprava stávajících procesů tak, aby pomohly eliminovat problém, který v budoucnu nastane, ale zatím není jisté, jak velký bude a jak se bude projevovat.

## Kde hledat pomoc a inspiraci

V rámci OECD existuje od roku 2011 **Observatoř pro inovace ve veřejném sektoru**, mezinárodní platforma pro inovace ve veřejné správě, v jí zřizovaných organizacích a v dalších organizacích financovaných z veřejných zdrojů. Observatoř pro inovace ve veřejném sektoru monitoruje světové trendy, přináší know-how z implementace inovací ve veřejném sektoru a znalostně podporuje vlády v systematickém úsilí o inovace. Shromažďuje a zveřejňuje příklady dobré praxe.

## Mezinárodní úsilí - Deklarace o inovacích ve veřejném sektoru

Na základě spolupráce v Observatoři pro inovace ve veřejném sektoru přijaly v roce 2019 členské státy OECD, včetně České republiky, **Deklaraci o inovacích ve veřejném sektoru**. Členské státy se zavázaly, že budou naplňovat pět hlavních zásad podpory inovací ve veřejném sektoru.

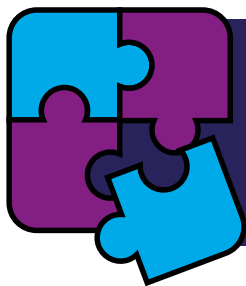
Ve zdůvodnění Deklarace je uvedeno:



*„Vlády a jejich organizace veřejného sektoru působí v nestálých, nejistých, složitých podmínkách a musí se potýkat s řadou problémů, jako je digitální transformace, energetická chudoba, zhoršování životního prostředí, změna klimatu a nerovnost... **Je nepravděpodobné, že by úroveň inovací, ke které dojde automaticky, byla dostatečná nebo udržitelná,**“ proto je potřebné cílené úsilí o inovace ve veřejném sektoru.“*

### Úsilí o inovace zahrnuje pět zásad:

- (1) Přijmout a posílit inovace ve veřejném sektoru (uznat, že inovace, podobně jako jiné hlavní úkoly, vyžadují silnou podporu a významné investice a uvědomit si překážky bránící inovacím).
- (2) Povzbuzovat zaměstnance v inovativním přístupu, poskytnout podmínky (nebrzdit inovace, umožnit zaměstnancům přemýšlet o své práci, učit se z chyb apod.).
- (3) Kultivovat partnerství a zohledňovat různé názory (sdílení informací, spolupráce napříč sektory).
- (4) Podporovat testování a experimentování (uznávat dílčí úspěchy plynoucí z testování a experimentování).
- (5) Rozšiřovat znalosti a zkušenosti a sdílet dobrou praxi (síťování, vzdělávání, databáze inovací apod.).



## Úvod do umělé inteligence

Technologie **umělé inteligence** (*artificial intelligence*, dále také „AI“) se stala v posledních letech automatickým a nezbytným nástrojem pro náš **způsob fungování v rozhodování, plánování a hledání informací v soukromém a pracovním životě**.

Umělá inteligence je postavena na získávání obrovského množství dat a spoléhá na pokročilé algoritmy strojového učení a extrémně vysokou úroveň programování, datové sady, databáze a počítačovou architekturu.

## Počátky umělé inteligence

Během druhé světové války ve Velké Británii představovala práce **Alana Turinga v Bletchley Park** na rozluštění šifrovacího systému Enigma kód používaným nacistickým Německem zásadní vědecký přelom. Jeho průkopnická práce pomohla rozvinout některé základy informatiky.

historický exkurz

V 50. letech 20. století se Turing soustředil na problematiku, **zda mohou stroje myslet samy za sebe**. Tento radikální nápad společně s rostoucími důsledky strojového učení v řešení problémů vedl k mnoha průlomovým výsledkům v oboru. Ve výzkumu se Turing zabýval základními otázkami, zda mohou být stroje řízeny a instruovány k myšlení, porozumění, učení a aplikaci vlastní ‚inteligence‘ při řešení problémů jako lidé.

Počítačové a kognitivní vědci, jako Marvin Minsky a John McCarthy, rozpoznali potenciál umělé inteligence v 50. letech minulého století. Jejich výzkum, který navazoval na Turingovy poznatky, poháněl exponenciální růst v této oblasti. V roce 1956 se účastníci semináře na Dartmouth College ve Spojených státech amerických zabývali problematikou strojového myšlení, otázkou, zda a za jakých okolností by bylo možné sestavit systémy vyznačující se inteligencí. Setkání připravil **matematik John McCarthy, jenž tyto systémy označil souslovím „umělá inteligence“**.

## Definice umělé inteligence

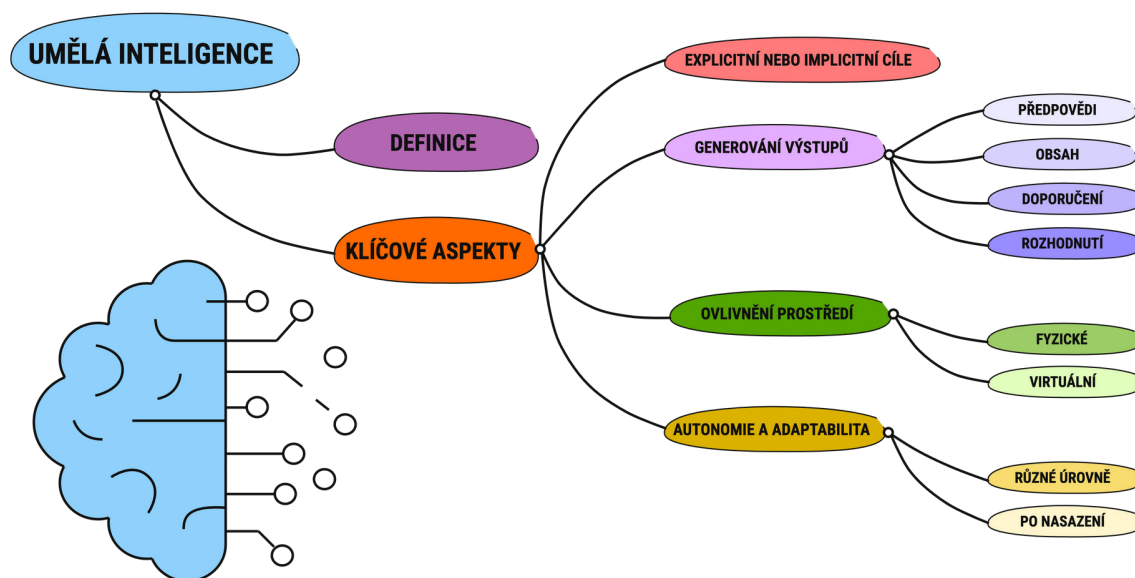
Umělá inteligence je komplexní a rychle se vyvíjející obor, neexistuje ovšem jedna platná definice AI. Různí odborníci, výzkumníci a instituce mají mírně odlišné definice AI, které

odrážejí rozdílné aspekty a aplikace v oboru. Klíčové aspekty AI, které jsou často zahrnuty v jejich definicích, zahrnují schopnost učení, řešení problémů, vnímání, autonomii a zpracování přirozeného jazyka.

Obecně uznávanou definici představila v roce 2019 Organizace pro hospodářskou spolupráci a rozvoj (OECD), která byla v roce 2023 aktualizována:

definice

„Systém umělé inteligence je strojový systém, který pro explicitní nebo implicitní cíle odvozuje ze vstupních údajů, které obdrží, jak generovat výstupy, jako jsou předpovědi, obsah, doporučení nebo rozhodnutí, která [mohou] ovlivnit fyzické nebo virtuální prostředí. Různé systémy AI se po nasazení liší úrovní autonomie a adaptability.“<sup>1)</sup>



Zdroj: Ilustrace/Myšlenková mapa - definice umělé inteligence - vytvořeno OpenAI – Diagrams Show Me,<sup>2)</sup> upraveno ve SketchWow Pro Version 2. 3. 0

## Typy a podobory umělé inteligence

typy a podobory

AI se dělí na několik typů, od úzké/slabé AI, která je navržena pro konkrétní úkoly, až po všeobecnou/silnou AI s obecnou inteligencí srovnatelnou s lidskou. Každý typ má své specifické použití a schopnosti.

<sup>1)</sup> „An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that [can] influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment“ OECD. Updates to the OECD’s definition of an AI system explained. OECD. Policy Observatory [online]. 2023, 2023-11-29 [cit. 2024-02-24]. Dostupné z: <https://oecd.ai/en/wonk/ai-system-definition-update>

<sup>2)</sup> OpenAI (<https://openai.com/>) je přední výzkumná organizace v oblasti umělé inteligence. OpenAI je známá vývojem pokročilých modelů zpracování přirozeného jazyka, jako je GPT (Generative Pre-trained Transformer) a inovativními nástroji jako je např. DALL·E pro generování obrázků z textu.

## Úzká/slabá AI (Narrow/Weak AI)

Je úzce specializovaná, zaměřuje se na přesně definované úkoly, ale postrádá schopnost generalizovat své znalosti nebo dovednosti na úkoly mimo svůj určený rozsah. Slabá AI prokazuje účinnost a přesnost v rámci svých předem určených hranic. Příklady slabé AI zahrnují hlasového asistenta Siri od Apple nebo systémy doporučení, jako jsou ty používané společností Amazon nebo streamovací službou Netflixem. Tyto systémy jsou efektivní v konkrétních oblastech, ale neumí se přizpůsobit novým nebo neznámým situacím.

## Všeobecná/silná AI (General/Strong AGI)

Tento typ AI by měl teoreticky rozumět a učit se jakýmkoliv intelektuálním úkolům, které dokáže člověk. V současnosti je silná AI spíše teoretickým konceptem než skutečností. **Hlavním cílem této AI je vytvořit systémy, které jsou schopny obecného intelektuálního chování, adaptace a učení v libovolném prostředí.** Tato AI by tedy měla být schopna porozumět a naučit se zcela novým a neznámým úkolům. Je v současné době předmětem výzkumu a její zavedení je považováno za jednu z hlavních výzev v oblasti umělé inteligence a předpokládá se, že bude mít dopad na společnost a technologie. Hypoteticky všeobecná/silná AI představuje schopnost inteligentních strojů, které rozumějí a učí se jakémukoliv úkolu nebo procesu, který obvykle provádí člověk.

## Strojové učení (Machine Learning)

**Strojové učení je podoblast umělé inteligence, zabývá se algoritmy a technikami, které umožňují počítačovým systémům učit se a zlepšovat se zkušenostmi bez potřeby jejich přímého naprogramování.** Pracuje s velkým množstvím dat, které analyzuje, uspořádává do souvislostí a následně vyhodnocuje. Vychází ze své předešlé zkušenosti, kterou na základě nových informací dále vylepšuje, a rozšiřuje si tak své znalosti. Strojové učení má široké spektrum využití, včetně překladu jazyků, předpovídání preferencí spotřebitelů a lékařských diagnóz. Je to klíčový prvek mnoha dalších podoborů AI, jako je zpracování přirozeného jazyka, neuronové sítě a hluboké učení.

## Neuronové sítě (Neural Networks)

Neuronové sítě představují klíčovou technologii v AI, inspirovanou strukturou a funkcí lidského mozku. Jsou základem mnoha moderních způsobů využití AI a umožňují komplexní zpracování dat. **Neuronové sítě jsou nezbytné pro AI programy, protože umělé inteligenci pomáhají provádět samostatné kompetentní rozhodnutí bez mnoha lidských zásahů.** Učí se a modelují vztahy mezi nelineárními, komplexními daty, což umožňuje aplikacím správně reagovat na různé požadavky. Vývoj a výzkum v oblasti neuronových sítí bude i nadále rychle postupovat, což otevírá nové příležitosti pro jejich aplikaci ve všech

úzká/slabá umělá  
inteligence

všeobecná / silná  
umělá inteligence

strojové učení

neuronové sítě

oblastech lidské činnosti. Neuronové sítě, zvláště ty hluboké (deep learning), jsou využívány v řadě oblastí, kde se ukázaly být velmi účinné. Např. Google Translate je online překladač, který používá neuronové sítě pro strojový překlad textu z jednoho jazyka do druhého. Díky hlubokým neuronovým sítím dokáže poskytovat mnohem přesnější a plynulejší překlady než předchozí metody strojového překladu.

## Hluboké učení (Deep Learning)

**Hluboké učení, podkategorie strojového učení, používá rozsáhlé neuronové sítě s mnoha vrstvami k modelování složitých vzorců v datech.** Je to motor mnoha pokročilých AI aplikací. Hluboké učení přichází na řadu, pokud je třeba řešit složitější problémy a pracovat s větším množstvím dat. Mezi nejvýznamnější oblasti hlubokého učení patří mj. rozpoznávání obrazů a zpracování vizuálních dat a také zpracování přirozeného jazyka. Hluboké učení je využíváno pro vývoj pokročilých technik komprese videa, což umožňuje ukládat a přenášet videa s vysokým rozlišením efektivněji.



## Zpracování přirozeného jazyka (Natural Language Processing, dále také „NLP“)

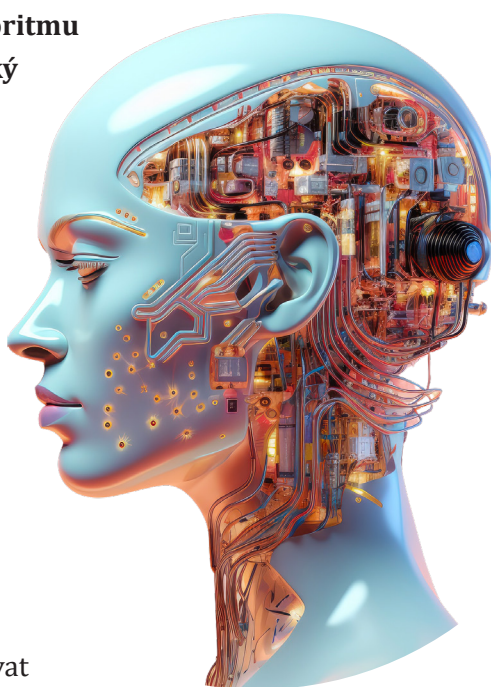
**Zpracování přirozeného jazyka je klíčovou součástí mnoha AI systémů od základní analýzy textu po složité chatboty, umožňuje strojům číst, rozumět a interpretovat lidský jazyk.** Příkladem nejčastěji využívanou aplikací NLP jsou chatboti pro zákaznickou podporu. Dalším příkladem mohou být systémy pro rozpoznávání a generování řeči. Tyto systémy umožňují uživatelům mluvit s technologií přirozeným způsobem, ať už jde o zadávání příkazů, dotazů nebo žádostí o informace. NLP technologie umožňují těmto asistentům rozumět mluvenému slovu a reagovat přirozeně a inteligentně. Tzv. Grammarly

je nástroj pro kontrolu pravopisu a gramatiky v anglickém jazyce, který používá zpracování přirozeného jazyka k tomu, aby pomohl lidem psát lépe. Tento produkt může být integrován do různých textových editorů a webových prohlížečů. Analyzuje psaný text a nabízí návrhy na opravy chyb v pravopisu, gramatice a slovní zásobě.

## Velké jazykové modely (Large Language Models, dále také „LLM“)

**Velké jazykové modely jsou typem algoritmu hlubokého učení, který využívá obrovský počet parametrů a rozsáhlá tréninková data k porozumění a generování textu.**

Tyto modely se zvláště zaměřují na úkoly zpracování přirozeného jazyka. Termín „velký“ u LLM se vztahuje jak na velikost modelu z hlediska jeho parametrů, tak na masivní množství dat použitých pro trénink, které se mohou pohybovat od milionů až do stovek miliard. LLM mají různá využití, jako je generování textu, překlad, shrnutí obsahu, přepisování, klasifikace, kategorizace, analýza emocionálního zabarvení textu a pohánění konverzační AI a chatbotů.<sup>3)</sup> Jsou schopny generovat odpovědi na výzvy, odpovídat na otázky, a dokonce vést konverzaci přirozeným způsobem.



velké jazykové modely

## Počítačové vidění (Computer Vision)

**Jedná se o oblast umělé inteligence a počítačových věd, která se zabývá tím, jak umožnit počítačům zpracovávat a interpretovat vizuální data ze světa kolem nás, obvykle pomocí digitálních kamer, videa a hloubkových senzorů.** Cílem počítačového vidění je umožnit počítačům provádět složité úkoly vizuálního vnímání, jako je rozpoznávání objektů, tváří, prostředí, dokonce i porozumění vizuálním scénám na úrovni, která se přibližuje lidskému vnímání. Používá se v různých aplikacích, od rozpoznávání obličejů při odemykání zařízení a ve fotografickém softwaru pro označování osob až po autonomní auta v navigaci, detekci překážek a rozhodování v reálném čase.

počítačové vidění

<sup>3)</sup> Mezi významné příklady LLM náleží modely GPT (*General Pre-Trained Transformer*) společnosti OpenAI (jako jsou GPT-3.5 a GPT-4, používané v ChatGPT), modely PaLM a Gemini společnosti Google, Copilot společnosti Microsoft, rodina otevřených modelů LLaMA společnosti Meta a modely Claude společnosti Anthropic.

## Robotika (Robotics)

robotika

**Robotika kombinuje AI s mechanickými těly k vytvoření autonomních nebo kolaborativních robotů.** Tyto systémy mohou provádět složité úkoly v průmyslových, lékařských, nebo domácích prostředích.

Robotika v tomto kontextu zahrnuje širokou škálu variant robotů.

kolaborativní roboti

**Kolaborativní roboti** – jsou vybaveni bezpečnostními prvky umožňujícími bezpečnou spolupráci s lidmi. Tito roboti jsou schopni automatizovat rutinní a opakující se úkoly, čímž umožňují lidským pracovníkům věnovat se složitějším a kreativnějším činnostem.

autonomní roboti

**Autonomní roboti** – využívají strojové vidění pro navigaci a provádění úkolů bez lidského dohledu. Tito roboti mohou zefektivnit širokou škálu průmyslových úkolů, které bylo tradičně obtížné automatizovat.

## Společenské dopady umělé inteligence

V posledních letech byl rozvoj umělé inteligence velice dynamický a její využití v praxi se rozšířilo do mnoha oblastí, od zemědělství přes průmysl až po služby, ale i veřejnou správu.

Technologické firmy jako je Apple, Google, Meta, Amazon, Microsoft do této technologie směřují své investice a výzkum. Pro globální komunikaci a propojenost v podnikání se stala umělá inteligence důležitou oblastí.

## Přínosy

přínosy

Společenské dopady umělé inteligence jsou komplexní a mají významný vliv na mnoho aspektů naší ekonomiky a společnosti. **AI zvyšuje efektivitu a přesnost v rozhodování díky schopnosti analyzovat velké objemy dat a přináší výhody při využití napříč různými sektory.**

V medicíně umožňuje přesnější diagnostiku a personalizované léčebné postupy. Dále přináší značné pokroky ve zlepšení bezpečnosti dopravy, kvality a životnosti produktů a služeb. Může také usnadnit přístup k informacím, vzdělání a školení, což bylo zvláště důležité během pandemie COVID-19. V pracovním prostředí může AI zvýšit bezpečnost tím, že převezme za člověka některé nebezpečné úkoly. Jako příklad může uvést stavebnictví. Na staveništích dochází k velkému počtu úrazů, mnohdy se závažnými následky. Proto je nezbytné využívat všechny dostupné nástroje a technologie pro zvýšení bezpečnosti práce, včetně umělé inteligence a automatizace. Ve vzdělávání může AI identifikovat potřeby a preferované učební styly jednotlivých studentů, umožňuje personalizované učební plány.



V průmyslu může AI predikovat potenciální poruchy zařízení nebo strojů, což umožňuje provádět údržbu dříve, než dojde k výpadkům zařízení v provozu.

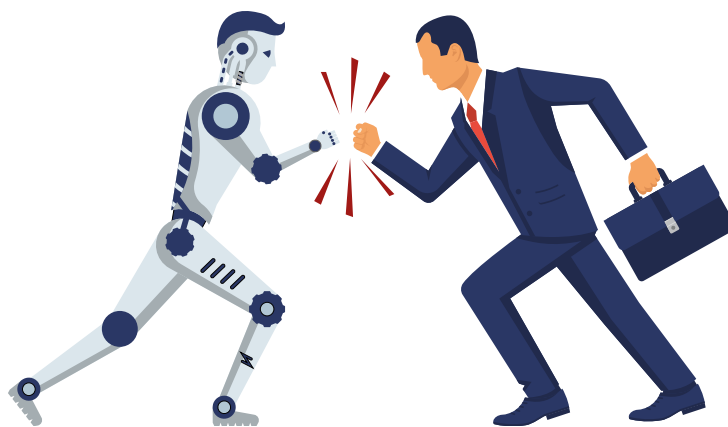
Podnikům AI umožňuje vývoj nové generace produktů a služeb v sektorech, jako je zelená a cirkulární ekonomika, strojírenství, zemědělství, móda a cestovní ruch. AI může zvýšit prodej, zlepšit údržbu strojů, zvýšit výrobní výstupy a kvalitu zboží, zlepšit zákaznický servis a ušetřit energii. Nedostatečné využití AI může vést k zmeškání příležitostí, ekonomické stagnaci a vyšší nezaměstnanosti.

## Rizika

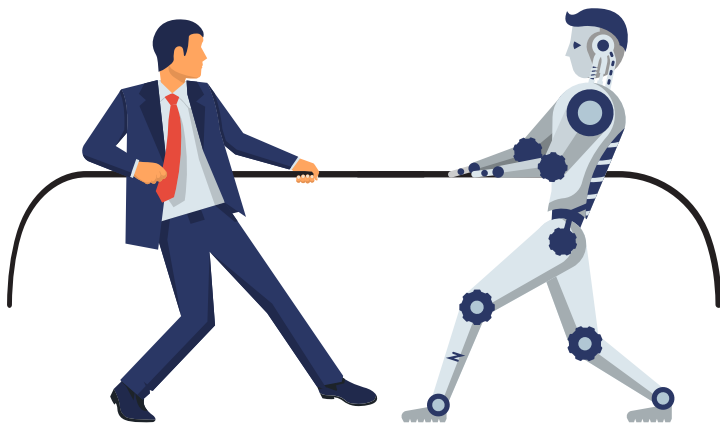
Na druhou stranu narůstající spoléhání se na AI systémy rovněž představuje **potenciální rizika**.



Aktuálně v poslední fázi schvalování **nařízení Evropské unie o umělé inteligenci** (*Artificial Intelligence Act, AIA*) se soustřeďuje na klasifikaci technologií podle způsobu využití a zavedení různých úrovní omezení podle toho, jaké s sebou nesou riziko. Některé systémy chce Evropská unie zcela zakázat. Zakázané AI systémy se týkají například identifikace emocí na pracovišti nebo ve vzdělávacích institucích, dále biometrických kategorizačních systémů, které třídí lidi na základě „citlivých“ rysů, jako je rasa nebo sexuální orientace, a v neposlední řadě i sociální kreditní systém obyvatelstva (*social scoring*), který hodnotí občany na základě jejich chování a sociálních interakcí.



Na světě totiž existuje obava z možného **zneužití AI pro škodlivé účely, jako například šíření dezinformací a falešných zpráv**. AI přináší vážná rizika a nebezpečí, zejména v souvislosti s tvorbou tzv. deep fake videí. Ty jsou digitálními výtvoři, které využívají pokročilé metody strojového učení



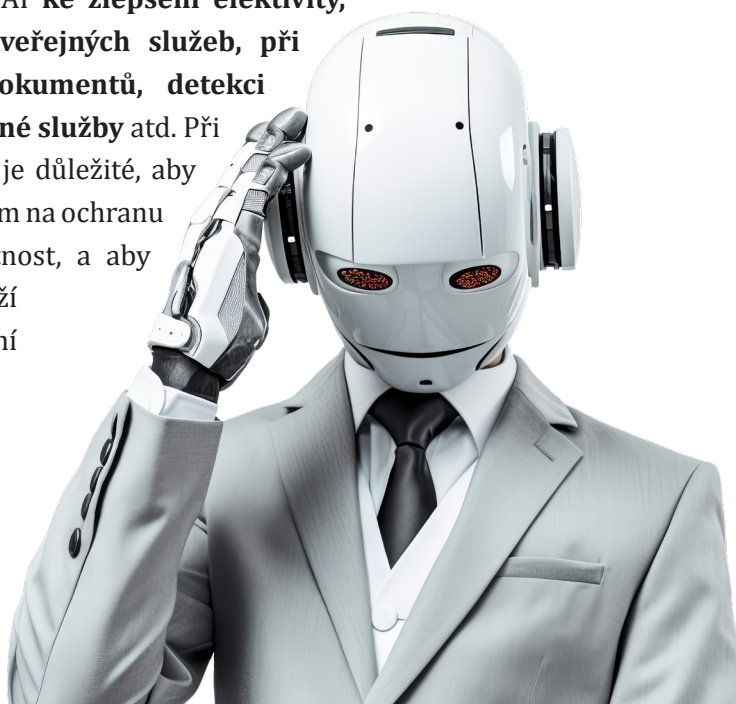
a umělé inteligence, především technologie známé jako generativní soupeřící sítě (*Generative Adversarial Networks, GANs*), k vytváření velmi přesvědčivých falešných videí. Tato videa mohou měnit obsah originálních záznamů tak, že vyměňují tváře osob, modifikují jejich výrazy,

rizika

mění jejich řeč nebo dokonce vytvářejí úplně nové videozáznamy, které vypadají realisticky, ale ve skutečnosti se nikdy nestaly. AI systémy mohou obsahovat zkreslení (bias), která mohou vést k diskriminaci lidí, například v oblasti nábory zaměstnanců nebo poskytování úvěrů. AI systémy mohou být zranitelné vůči kybernetickým útokům, což může mít vážné důsledky v kritických sektorech, jako je zdravotnictví nebo doprava. Rozšířené používání AI ve sledovacích systémech může vést k narušení soukromí a zvýšenému dohledu nad jednotlivci. Zneužití AI může ovlivnit voliče a narušit spravedlivý a demokratický průběh voleb.

## AI ve veřejné sféře

Zaměstnanci mohou využívat AI ke zlepšení efektivity, transparentnosti a kvality veřejných služeb, při analýze dat, zpracování dokumentů, detekci podvodů a pro personalizované služby atd. Při zavádění AI ve veřejné správě je důležité, aby státní úřady zavedly AI s ohledem na ochranu osobních údajů a transparentnost, a aby zajistily, že technologie slouží ku prospěchu občanů a zlepšení veřejných služeb.



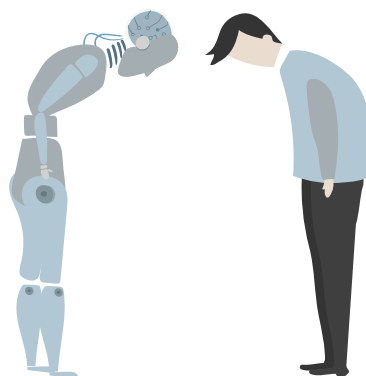
## Reakce na dopady AI

Je zřejmé, že AI nabízí řadu výhod, ale také přináší výzvy, které vyžadují pozornost a regulaci ze strany vládních a mezinárodních institucí, aby se zajistilo, že jejich vývoj a využití bude prospěšné pro společnost jako celek. **Řešení rizik kromě přijetí regulace také obnáší zavedení etických kodexů/směrnic, transparentnost a spolupráci mezi výzkumníky, vývojáři, vládami a dalšími zúčastněnými stranami.** Vývoj v oblasti legislativy a etiky AI je dynamický, aby dokázal reflektovat rychlý technologický pokrok a měnící se společenské názory na tyto technologie.

**Etika a legislativa v oblasti umělé inteligence jsou klíčové pro formování způsobu, jakým je AI využívána a rozvíjena.** Obě disciplíny řeší široké spektrum otázek od ochrany osobních údajů, přes vyváženost a transparentnost algoritmů, až po odpovědnost za rozhodnutí učiněná AI.

## Etika

V etickém kontextu se klade důraz na zajištění, aby AI technologie byla využívána způsobem, který respektuje lidská práva, je spravedlivý a transparentní, brání zkreslení a diskriminaci v AI systémech. V roce 2019 vydala Organizace pro hospodářskou spolupráci a rozvoj doporučení k principům inovativní umělé inteligence, která respektují lidská práva a demokratické hodnoty.



etické dopady

## Legislativa v oblasti umělé inteligence



Evropská unie přistupuje k umělé inteligenci s cílem stát se globálním lídrem v bezpečném využívání této technologie. Její politiky a programy jsou zaměřeny na rozvoj AI, která je bezpečná, transparentní, sledovatelná, nediskriminační a šetrná k životnímu prostředí. V roce 2021 představila Evropská unie **návrh nařízení o umělé inteligenci (AIA)**, který je považován za **jeden z prvních komplexních právních rámců pro AI na světě a klade důraz na bezpečnost, transparentnost a základní práva**.

nařízení EU o umělé inteligenci

Spojené státy americké nemají na federální úrovni komplexní legislativu o AI, ale několik států, jako je Kalifornie, přijalo vlastní zákony o ochraně soukromí a etickém používání AI. Na federální úrovni existují různé iniciativy a směrnice, které řídí používání AI v určitých sektorech, jako je zdravotnictví a obrana.

## Národní strategie umělé inteligence České republiky

V roce 2019 Česká republika jako jedna z prvních zemí na světě přijala **Národní strategii umělé inteligence v České republice**, která je v gesci Ministerstva průmyslu a obchodu ČR. **Strategie se zaměřuje na podporu rozvoje AI v rámci akademické, veřejné i soukromé sféry**. Strategie zahrnuje cíle a nástroje pro domácí i mezinárodní spolupráci v oblasti AI a je rozdělena do sedmi klíčových oblastí.

Národní strategie umělé inteligence v ČR

7 klíčových oblastí

- (1) podpora a koncentrace vědy, výzkumu a vývoje,
- (2) financování výzkumu a vývoje, podpora investic a rozvoj AI ekosystému v ČR,
- (3) AI v průmyslu, službách a veřejné správě,
- (4) lidský kapitál a vzdělávací systém spolu s celoživotním vzděláváním,
- (5) opatření k řešení dopadů AI na trh práce a sociální systém,

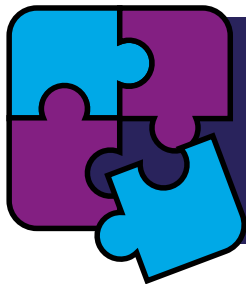
- (6) právní a společenské aspekty AI, etická pravidla, ochrana spotřebitele a bezpečnostní otázky,
- (7) mezinárodní spolupráce.

Cíle strategie jsou časově odstupňovány s důrazem na konkrétní opatření splnitelná v daném časovém horizontu, v návaznosti na finanční rámec EU a implementační plány koncepce **Digitální ekonomika a společnost**.



## ROZŠIŘUJÍCÍ LITERATURA

- (1) *Kolektiv autorů: JEDNODUŠE: Umělá inteligence.* Praha, Universum, První vydání, 2023. ISBN 978-80-242-9293-9
- (2) Ministerstvo průmyslu a obchodu. Národní strategie umělé inteligence ČR (2019). Dostupné z [https://www.mpo.cz/assets/cz/podnikani/2023/1/NAIS\\_kveten\\_2019.pdf](https://www.mpo.cz/assets/cz/podnikani/2023/1/NAIS_kveten_2019.pdf)
- (3) *Ministerstvo průmyslu a obchodu.* Umělá inteligence. Dostupné z <https://www.mpo.cz/cz/podnikani/digitalni-ekonomika/umela-inteligence/>
- (4) *Ministerstvo průmyslu a obchodu.* Výsledky veřejné konzultace k aktualizaci Národní strategie umělé inteligence. Dostupné z: <https://www.mpo.cz/cz/podnikani/digitalni-ekonomika/umela-inteligence/vysledky-verejne-konzultace-k-aktualizaci-narodni-strategie-umele-inteligence--277259/>
- (5) *Evropská komise.* Evropský přístup k umělé inteligenci. Dostupné z <https://digital-strategy.ec.europa.eu/cs/policies/european-approach-artificial-intelligence>
- (6) *OECD.* Artificial intelligence. Dostupné z <https://www.oecd.org/digital/artificial-intelligence>
- (7) *UNESCO.* Artificial intelligence. Dostupné z <https://www.unesco.org/en/artificial-intelligence>
- (8) Další internetové zdroje: <https://umelligence.cz>, <https://aidetem.cz>, <https://asociace.ai/>, <https://prg.ai/en/>, <https://www.brno.ai>



# Zvyšování odolnosti státní správy proti nelegitimnímu ovlivňování

# 4


Audit národní bezpečnosti schválený usnesením vlády č. 1125 ze dne 14. prosince 2016<sup>1)</sup> popsal deset hlavních bezpečnostních hrozeb pro Českou republiku, přičemž jednou z nich je tzv. „**působení cizí moci**“. Na základě doporučení Auditů probíhá od roku 2018 školení vybraných státních zaměstnanců a dalších zaměstnanců veřejné správy zaměřené na zodolnění vůči pokusům o nelegitimní ovlivňování, které pořádá Ministerstvo vnitra spolu se zpravodajskými službami (Bezpečnostní informační službou a Úřadem pro zahraniční styky a informace). Svým usnesením č. 794 z 25. října 2023 vláda České republiky rozhodla o pokračování těchto školení.

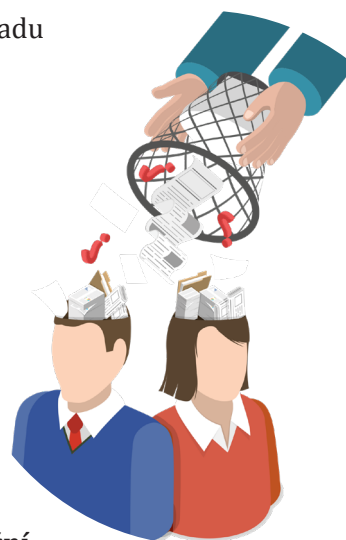
audit národní  
bezpečnosti

Většina těchto zaměstnanců absolvuje toto školení formou e-learningu. Ti, kteří mají přístup k většímu množství citlivých informací anebo disponují zvýšenými rozhodovacími pravomocemi, mohou být na základě rozhodnutí služebního orgánu vysláni na školení prezenční.

## CO TO JE NELEGITIMNÍ OVLIVŇOVÁNÍ

Nelegitimní ovlivňování je souhrnné označení pro celou řadu zpravidla cílených aktivit a činností, které jsou svojí povahou protiprávní anebo nežádoucí. Původcem nelegitimního ovlivňování je útočník, který se všemi jemu dostupnými prostředky snaží o prosazení svých zájmů, a to tak, že pomocí svého aktivního jednání zasahuje do zájmů někoho jiného (cíle nelegitimního ovlivňování).

 Nelegitimní ovlivňování je **nežádoucí působení na lidi, rozhodování, či procesy**. Zahrnuje jak vlivové působení cizí moci,<sup>2)</sup> tak i kriminální (např. korupční) jednání a nežádoucí lobbování. **Obvykle jde o aktivity, které jsou skryté, klamavé, vynucující či korupční, a které útočník (cizí moc, korupčník, lobbista postupující v rozporu se**



nelegitimní  
ovlivňování

definice

<sup>1)</sup> Podrobnosti k Auditů národní bezpečnosti viz <https://www.mvcr.cz/chh/soubor/audit-narodni-bezpecnosti.aspx>

<sup>2)</sup> Český právní řád obsahuje definici pojmu „cizí moc“ v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů v § 2, písm. g) takto: „Cizí mocí se rozumí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán.“ Pro účely tohoto textu definici rozšíříme i o jakékoliv další fyzické osoby bez ohledu na jejich státní příslušnost, či právnické osoby bez ohledu na jejich sídlo anebo místo působení, pokud se podílí, byť i jen částečně, na prosazování zájmů cizí moci formou nelegitimního ovlivňování.za

zákonem, případně obecně uznávanými společenskými etickými pravidly) vykonává **sám** anebo **prostřednictvím třetí strany**, a které **ohrožují** či **poškozují** naše zájmy.

## TÝKÁ SE STÁTNÍCH ZAMĚSTNANCŮ NELEGITIMNÍ OVLIVŇOVÁNÍ?

Ano týká. **Existují subjekty prosazující svoje zájmy v rozporu s demokratickými principy, právním řádem**, ale i dobrými mravy, a ty v tomto kontextu označujeme za útočníky.

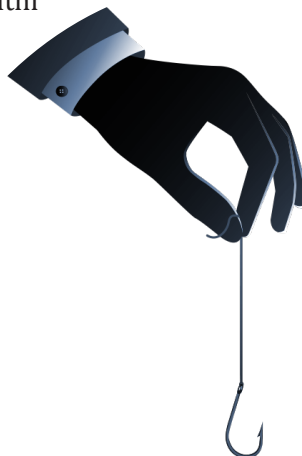
Útočníci se snaží najít co možná nejjednodušší cestu

k prosazování svých zájmů, přičemž v absolutní

většině případů takové aktivity směřují

vůči nějaké fyzické osobě (v tomto

případě státnímu zaměstnanci).



Celá řada státních zaměstnanců

(a nejen jich) má dojem, že

jejich práce je pro jiné osoby

(potenciální útočníky)

nezajímavá, nemá přístup

k informacím, které by mohly

být pro někoho zajímavé nebo

mít nějakou hodnotu, a že nemá

žádnou anebo jen minimální

rozhodovací pravomoc. Takové

presvědčení je ale nesprávné,

a naopak zvyšuje pravděpodobnost

úspěchu útočníka, pokud svoje zájmy

zkusí prosazovat právě prostřednictvím

fyzické osoby, která je přesvědčená, že je pro

potenciálního útočníka nezajímavá. Právě u takového člověka

je vysoká pravděpodobnost, že signály naznačující, že by mohl být cílem nelegitimního ovlivňování, přehlédne, nebo je bude podceňovat.



V konečném důsledku může takový přístup a nesprávná nebo žádná reakce státního zaměstnance na nelegitimní ovlivňování či pokus o něj způsobit poškození politických, ekonomických, bezpečnostních, reputačních, ale i dalších zájmů České republiky.

Je třeba si uvědomit, že kterýkoli státní zaměstnanec **se může stát cílem nelegitimního ovlivňování kvůli tomu:**

- » **K čemu má přístup** – přichází do styku s různými interními dokumenty, pracuje s databázemi obsahujícími osobní údaje či jiné citlivé anebo interní informace; má interní informace vztahující se k zadávání veřejných zakázek, má přístup k interní počítačové síti apod.

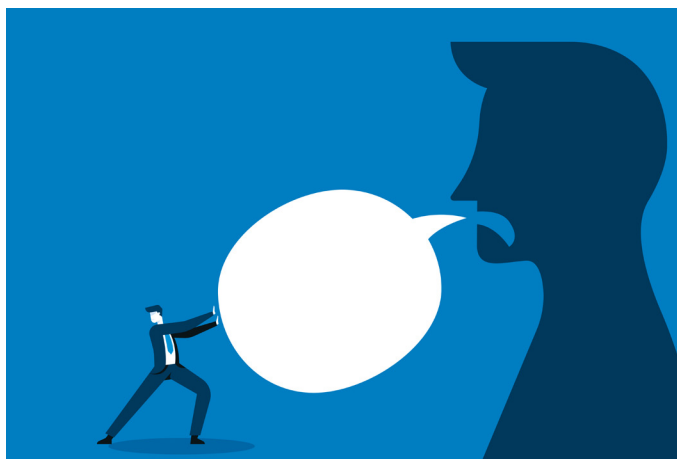
státní zaměstnanec  
jakožto cíl  
nelegitimního  
ovlivňování

- » **Kam má přístup** – jako zaměstnanec má fyzický přístup do prostor, kam nemůže veřejnost, v některých případech i do míst, kam nesmí ani většina dalších zaměstnanců úřadu; umí popsat bezpečnostní opatření fyzické, administrativní, ale i režimové povahy
- » **Ke komu má přístup** – nejde jen o kolegy, ale i představené a zaměstnance jiných úřadů a dalších státních i nestátních subjektů, se kterými spolupracuje
- » **Co ví** – je schopen popsat dynamiku vztahů na pracovišti, ví kdo má přístup k jakým informacím anebo do jakých prostor, zná řadu velice osobních informací o lidech, se kterými spolupracuje

V některých případech nemusí být cílem přímo konkrétní státní zaměstnanec, ale může se stát nástrojem útočníka k ovlivňování někoho jiného, tj. třetí osoby či subjektu.

## JAK NELEGITIMNÍ OVLIVŇOVÁNÍ ROZPOZNAT A JAK POSTUPOVAT

Identifikace jednotlivých forem a metod útoku a způsobu obrany proti nim se v zásadě neliší podle toho, zda je útočníkem zástupce cizí moci, korupčník či lobbista postupující v rozporu se zákony či dobrými mravy. Aktérem útoku je vždy „člověk“, bez ohledu na to, zda jedná sám či ve prospěch nějakého státu, firmy, organizace apod. Je tak velmi pravděpodobné, že v absolutní většině případů se útočník, stejně jako každý jiný člověk, dopustí řady větších či menších chyb, kterých si lze všimnout.



Zkušenosti ze zjištěných případů nelegitimního ovlivňování, ať již u nás anebo v zahraničí, ukazují, že v absolutní většině případů bylo lidem, kteří se stali cílem nelegitimního ovlivňování či jejich nejbližšímu okolí, zcela zřejmé, že **je „něco špatně“, případně „jinak“, než je v obdobných situacích běžné.**

Pokud má zaměstnanec pocit, že se děje něco zvláštního, podivného, či se někdo v nějaké situaci chová či jedná neodpovídajícím způsobem, **je vhodné informovat svého představeného či odpovědného zaměstnance bezpečnostního odboru/oddělení úřadu** a konkrétní podezření s ním prodiskutovat. V krajním případě je pak možné obrátit se cestou e-mailu [prevence@bis.cz](mailto:prevence@bis.cz) přímo na Bezpečnostní informační službu.

Bezprostředně nadřízený představený či zaměstnanec bezpečnostního odboru/oddělení se státním zaměstnancem podezření prodiskutuje a navrhne další postup. V některých případech se může rozhodnout, že bude vhodné informovat o celé situaci i Policii České republiky či Bezpečnostní informační službu.

postup při podezření

## JE NUTNÉ ZJIŠŤOVAT KDO JE ÚTOČNÍKEM?

Nehraje roli, zda je útočníkem cizí moc, nějaká kriminální skupina snažící se např. korupčními aktivitami přimět zaměstnance k tomu, aby nějakým způsobem konal, či někdo jiný. Důležité je, nenechat si informaci o možném probíhajícím pokusu o nelegitimní ovlivňování pro sebe.

Pro správné vyhodnocení konkrétní situace, v níž může docházet k nelegitimnímu ovlivňování, je velmi užitečné, zapamatovat si co možná největší množství detailů, které by mohly pomoci odpovědět na šest základních otázek: Kdo? Co? Kdy? Kde? Jak? a Proč?

hlavní zásady

## HLAVNÍ ZÁSADY

### TŘI PILÍŘE PRO ZVÝŠENÍ ODOLNOSTI

- I.** každý má přístup k citlivým informacím, které se mohou stát cílem zájmu útočníka (jinými slovy: informace, které jsou pro někoho bezcenné, mohou mít velkou cenu pro někoho jiného)
- II.** každý se může stát předmětem zájmu (nelegitimního ovlivňování) - rozhodnutí, zda se zaměří přímo na zaměstnance, je na útočnickovi, zaměstnanec sám jej nemůže nijak ovlivnit
- III.** každý se může bránit - jsou k dispozici nástroje, jak nelegitimní ovlivňování rozeznat a jak se v takových situacích zachovat => každý se může na někoho obrátit