**Katalóg rizík pre mládež, jej zákonných zástupcov a pedagógov v kybernetickom priestore**

**vedomostná báza**

Obrázok, na ktorom je text, snímka obrazovky, osoba, ľudská tvár

Obsah vygenerovaný pomocou AI môže byť nesprávny.

|  |  |
| --- | --- |
| **Verzia:** | 3f |
| **Dátum:** | 09.07.2025 |
| **Vlastník:** | Ministerstvo školstva, výskumu, vývoja a mládeže SR |
| **Autor:** | RNDr. Michal Danilák |

**História dokumentu**

|  |  |  |
| --- | --- | --- |
| **Verzia** | **Dátum verzie** | **Popis verzie a zmien** |
| 1 | 15.02.2025 | Prvá pracovná verzia dokumentu |
| 2-2d | 19.03.2025 | Pracovné verzie dokumentu na review / pripomienkovanie, pridaný prehľad aktív a vybraných hrozieb so zraniteľnosťami, identifikácia potrieb, priebežné zapracovanie podnetov. |
| 2e-2f | 31.03.2025 | Pridaná analýza potrieb, vekovo špecifické hrozby, analýza školského IKT prostredia, zapracovanie čiastkových pripomienok. |
| 2g-2k | 13.05.2025 | Verzie na review / pripomienkovanie v širšej skupine pripomienkujúcich, zapracúvanie pripomienok a dopĺňanie špecifických hrozieb, zraniteľností, dopadov, opatrení. |
| 2l | 20.05.2025 | Verzia rozposlaná Digitálnou koalíciou na širšie pripomienkovanie |
| 2m-2q | 20.06.2025 | Zapracúvanie pripomienok v rámci Digitálnej koalície |
| 3-3d | 25.6.2025 | Verzie so zapracovanými pripomienkami a pre-review |
| 3e | 02.07.2025 | Verzia na review v internom tíme, zladenie textovej a tabuľkovej časti |

Obsah

[1 Úvodné informácie 7](#_Toc202940124)

[**1.1** **Zhrnutie** 7](#_Toc202940125)

[1.1.1 Úloha Akčného plánu 7](#_Toc202940126)

[1.1.2 Zmysel vytvorenia Katalógu rizík 7](#_Toc202940127)

[1.1.3 Hlavné oblasti rizík pre mládež v kybernetickom priestore 8](#_Toc202940128)

[1.1.4 Závislosti medzi vybranými rizikami 9](#_Toc202940129)

[1.2 Možná spolupráca a podpora 10](#_Toc202940130)

[1.3 Využitie Katalógu rizík 10](#_Toc202940131)

[1.4 Zoznam skratiek a vysvetlenie pojmov 12](#_Toc202940132)

[1.5 Definícia základných pojmov v oblasti kybernetickej bezpečnosti 13](#_Toc202940133)

[1.6 Vecný rámec základných pojmov v oblasti bezpečnosti 14](#_Toc202940134)

[1.7 Stručný úvod do manažmentu bezpečnosti 15](#_Toc202940135)

[2 Katalóg rizík – vnútorné členenie a prístup 16](#_Toc202940136)

[2.1 Štruktúra Katalógu 16](#_Toc202940137)

[2.2 Členenie oblastí hrozieb a zraniteľností 17](#_Toc202940138)

[2.3 Členenie podľa špecifických skupín 20](#_Toc202940139)

[2.4 Členenie vplyvov / dopadov 22](#_Toc202940140)

[2.5 Výber prístupu k analýze rizík 24](#_Toc202940141)

[2.6 Spôsob určenia miery rizika 25](#_Toc202940142)

[3 Aktíva 28](#_Toc202940143)

[3.1 Aktíva priamo súvisiace s IKT 28](#_Toc202940144)

[3.1.1 Aktíva súvisiace v IKT v domácnosti 28](#_Toc202940145)

[3.1.2 Aktíva mobilného IKT 34](#_Toc202940146)

[3.1.3 IKT aktíva školy 35](#_Toc202940147)

[3.2 Aktíva dieťaťa ako fyzickej osoby 41](#_Toc202940148)

[3.3 Aktíva rodičov vo vzťahu k dieťaťu a kybernetickému priestoru 44](#_Toc202940149)

[3.4 Finančné aktíva 45](#_Toc202940150)

[3.5 Aktíva populácie mládeže ako celku 45](#_Toc202940151)

[3.6 Aktíva štátu ako celku 46](#_Toc202940152)

[4 Hrozby a zraniteľnosti, dopady a riziká 46](#_Toc202940153)

[4.1 Domáce IKT prostredie 46](#_Toc202940154)

[4.1.1 Hrozby 46](#_Toc202940155)

[4.1.2 Zraniteľnosti 53](#_Toc202940156)

[4.1.3 Možné dopady / následky 54](#_Toc202940157)

[4.1.4 Analýza rizík 56](#_Toc202940158)

[4.2 Školské IKT prostredie 60](#_Toc202940159)

[4.2.1 Hrozby 61](#_Toc202940160)

[4.2.2 Zraniteľnosti 66](#_Toc202940161)

[4.2.3 Možné dopady / následky 68](#_Toc202940162)

[4.2.4 Analýza rizík 70](#_Toc202940163)

[4.3 Mobilné / externé IKT prostredie 74](#_Toc202940164)

[4.3.1 Hrozby 74](#_Toc202940165)

[4.3.2 Zraniteľnosti 80](#_Toc202940166)

[4.3.3 Možné dopady / následky 81](#_Toc202940167)

[4.3.4 Analýza rizík 83](#_Toc202940168)

[4.4 Analýza dopadov (BIA) pre školské IKT prostredie 87](#_Toc202940169)

[4.4.1 Legislatívny a vecný rámec BIA 87](#_Toc202940170)

[4.4.2 Klasifikačné schémy pre posúdenie dopadov 89](#_Toc202940171)

[4.4.3 Časové limity výpadku 89](#_Toc202940172)

[4.4.4 Klasifikácia dopadov podľa kvantitatívnej škály 89](#_Toc202940173)

[4.4.5 Klasifikácia dopadov podľa kvalitatívnej škály 90](#_Toc202940174)

[4.4.6 Dopady na školy 92](#_Toc202940175)

[4.4.7 Dopady na žiaka 94](#_Toc202940176)

[4.5 Špecifické oblasti hrozieb, zraniteľností, rizík 95](#_Toc202940177)

[4.5.1 Hrozby pre vzdelávací proces 95](#_Toc202940178)

[4.5.2 Hrozby týkajúce sa porušenia ochrany osobných údajov na škole 96](#_Toc202940179)

[4.5.3 Hrozby pre finančné aktíva 97](#_Toc202940180)

[4.5.4 Hrozby pre reputáciu a osobnú integritu 99](#_Toc202940181)

[4.5.5 Hrozby pre zdravie 101](#_Toc202940182)

[4.5.6 Hrozby pre časový fond 105](#_Toc202940183)

[4.5.7 Vekovo špecifické hrozby 106](#_Toc202940184)

[4.5.8 Hrozby vo virtuálnych prostrediach 110](#_Toc202940185)

[4.5.9 Hrozby súvisiace s digitálnym vylúčením 114](#_Toc202940186)

[4.5.10 Hrozby súvisiace s možnosťami poznania 118](#_Toc202940187)

[4.5.11 Hrozby v špecifických životných situáciách 122](#_Toc202940188)

[4.5.12 Hrozby súvisiace so sociálno-spoločenskou kontinuitou 124](#_Toc202940189)

[4.5.13 Hrozby súvisiace s AI (umelá inteligencia) 128](#_Toc202940190)

[4.5.14 Nové oblasti zdrojov hrozieb a zraniteľností 131](#_Toc202940191)

[4.5.15 Štandardné hrozby pre mládež ovplyvnené kybernetickým priestorom 141](#_Toc202940192)

[4.5.16 Špecifické riziká pre dievčatá 143](#_Toc202940193)

[4.5.17 Špecifické riziká pre chlapcov 148](#_Toc202940194)

[4.6 Závislosti medzi vybranými rizikami 152](#_Toc202940195)

[4.6.1 Najvýznamnejšie riziká pre mládež v kybernetickom priestore 152](#_Toc202940196)

[4.6.2 Analýza závislostí medzi vybranými rizikami a ich opis 153](#_Toc202940197)

[4.7 Scenáre 156](#_Toc202940198)

[4.7.1 Najhoršie scenáre 156](#_Toc202940199)

[4.7.2 Nepriaznivé scenáre 156](#_Toc202940200)

[5 Analýza potrieb a očakávaní 159](#_Toc202940201)

[5.1 Úvodné informácie o potrebách a očakávaniach 159](#_Toc202940202)

[5.2 Rodič 161](#_Toc202940203)

[5.3 Dieťa / žiak 162](#_Toc202940204)

[5.4 Pedagóg 163](#_Toc202940205)

[5.5 Vedenie školy 164](#_Toc202940206)

[5.6 Štát ako celok 164](#_Toc202940207)

[6 Možné opatrenia a odporúčania 165](#_Toc202940208)

[6.1 Rodičia 165](#_Toc202940209)

[6.2 Dieťa / žiak 169](#_Toc202940210)

[6.3 Škola / zriaďovateľ školy 170](#_Toc202940211)

[6.4 MŠVVaM 171](#_Toc202940212)

[6.5 Ďalšie štátne orgány 172](#_Toc202940213)

[6.6 Ďalšie subjekty 173](#_Toc202940214)

[7 Prílohy 174](#_Toc202940215)

[7.1 Legislatívny rámec pre riadenie identifikovaných rizík 174](#_Toc202940216)

[7.1.1 Kompetencie v oblasti starostlivosti o mládež 174](#_Toc202940217)

[7.1.2 Kompetencie v oblasti implementácie ďalších opatrení 176](#_Toc202940218)

[7.1.3 Kompetencie v oblasti ochrany zdravia mládeže 177](#_Toc202940219)

[7.2 Stratégia Slovenskej republiky pre mládež na roky 2021 – 2028 178](#_Toc202940220)

[7.2.1 Vecný rámec 178](#_Toc202940221)

[7.2.2 Prioritné oblasti 179](#_Toc202940222)

[7.2.3 Vybrané ciele 180](#_Toc202940223)

[7.3 Národná koncepcia ochrany detí v digitálnom priestore 183](#_Toc202940224)

[7.3.1 Vecný rámec 183](#_Toc202940225)

[7.3.2 Členenie ohrození 183](#_Toc202940226)

[7.3.3 Participujúce subjekty 186](#_Toc202940227)

[7.3.4 Strategické zámery a priority 187](#_Toc202940228)

[7.3.5 Akčný plán 188](#_Toc202940229)

[7.4 Legislatívny rámec Trestného zákona 190](#_Toc202940230)

[7.4.1 Vymedzenie dôležitých pojmov 190](#_Toc202940231)

[7.4.2 Tresty pre mladistvých 192](#_Toc202940232)

[7.4.3 Ďalšie dôležité pojmy 193](#_Toc202940233)

[7.4.4 Špecifické trestné činy realizovateľné v kybernetickom priestore 195](#_Toc202940234)

[7.4.5 Trestné činy špecifické pre kybernetický priestor 197](#_Toc202940235)

[7.4.6 Ďalšie relevantné trestné činy 198](#_Toc202940236)

[7.5 Hodnotenie vekovo podmienených rizík digitálnych technológií 203](#_Toc202940237)

[7.5.1 Škála pre hodnotenie času stráveného s digitálnymi technológiami 203](#_Toc202940238)

[7.5.2 Vek a odporúčané časy 204](#_Toc202940239)

[7.5.3 Vek a riziká digitálnych aktivít 205](#_Toc202940240)

[7.5.4 Inšpirácia pre škálu 206](#_Toc202940241)

[7.6 Klasifikačné schémy pre riziká v digitálnom prostredí 207](#_Toc202940242)

[7.6.1 OECD 207](#_Toc202940243)

[7.6.2 EÚ 209](#_Toc202940244)

[7.7 Globálne riziká súvisiace s kybernetickým priestorom 211](#_Toc202940245)

[7.8 Riziká digitálnych technológií v oblasti základných práv a slobôd 215](#_Toc202940246)

[7.9 Monetarizácia zdravotných dopadov 224](#_Toc202940247)

[7.10 Populačná dynamika – podklady 226](#_Toc202940248)

# Úvodné informácie

V tejto kapitole sú uvedené úvodné informácie súvisiace s tvorbou a využitím Katalógu rizík pre deti, žiakov, študentov, ich zástupcov, pedagogických a odborných zamestnancov v kybernetickom priestore.

## **Zhrnutie**

### Úloha Akčného plánu

Jednou z úloh Akčného plánu pre Program informatizácie š kolstva do roku 2030 [[1]](#footnote-1) je:

„Vytvoriť katalóg rizík pre deti, žiakov, študentov (v závislosti od veku), ich zástupcov, pedagogických a odborných zamestnancov v kybernetickom priestore a jeho pravidelná ročná aktualizácia. Súčasťou Katalógu rizík je aj BIA a návrh možných opatrení na ich mitigáciu.“

Katalóg bude obsahovať prehľad hrozieb, zraniteľností, možných následkov a posúdenie miery rizika; ako aj návrh možných opatrení pre zníženie miery rizík. Bude v podrobnej textovej a zhutnenej tabuľkovej forme.

### Zmysel vytvorenia Katalógu rizík

Digitálne technológie a kybernetický priestor okrem nesporných pozitív priniesli aj veľa nových hrozieb a rizík. Ako príklad môžeme uviesť:

* nové závislosti (na mobiloch, sociálnych sieťach, hrách, pornografický obsah na internete, a pod.)
* kyberšikana
* sexting a grooming
* šírenie toxických výziev na sociálnych sieťach (napr. na lízanie WC, prehltnutie tužkových batérií, konzumácia liekov)
* šírenie dezinformácií, nenávistného obsahu
* nové formy okrádania (napr. cez phising a pharming)
* nové formy vydierania (napr. ransomvér)
* podvádzanie pri vypracovaní domácich úloh a prác využitím AI
* zníženie schopností fyzického sociálneho kontaktu u mladých
* nedostatok pohybu a spánku
* obmedzenie kognitívnych schopností

Nové hrozby v kybernetickom priestore majú množstvo negatívnych zdravotných, psychosociálnych a aj ekonomických dopadov vo všetkých vyspelých krajinách najmä pre mládež, ale aj ich rodičov a pedagógov. Preto sa všade vo svete pristupuje k systémovým opatreniam na úrovni legislatívy (nové trestné činy, obmedzenia prístupu k sociálnym sieťam), metodických usmernení (napr. obmedzenia mobilov v škole), programov a projektov bezpečnosti mládeže.

Informácie o hrozbách pre mládež sú uvedené v množstve informačných zdrojov a prinášajú veľa podnetných myšlienok. Chýba však systematický prehľad všetkých relevantných hrozieb a súvisiacich zraniteľnosti a odhad ich možných negatívnych dopadov. Túto medzeru má za cieľ zaplniť Katalóg rizík pre deti / žiakov / študentov, ich rodičov, pedagogických a odborných zamestnancov v kybernetickom priestore.

Katalóg rizík bude jedným z kľúčových podkladom pre ďalšie systémové riešenie problematiky bezpečnosti mládeže v kybernetickom priestore na úrovni štátu, rezortu, škôl; detto aj pre ich rodičov a pedagógov v jeho zjednodušenej verzii.

Tento dokument je aj referenčným podkladom pre tvorbu špecializovaných verzií Katalógu rizík a ďalších súvisiacich dokumentov.

### Hlavné oblasti rizík pre mládež v kybernetickom priestore

V tejto podkapitole je uvedený prehľad najvýznamnejších rizík pre mládež v súvislosti s kybernetickým priestorom. Bude predmetom širšej spoločenskej diskusie a následne revízie.

1. **Časovo nadmerné využívanie digitálnych technológií**
   1. Nezdravý životný štýl
   2. Ohrozenie fyzického zdravia
   3. Vznik nelátkových závislostí u časti mládeže nadmerným využívaním digitálnych technológií.
2. **Nesprávne resp. škodlivé používanie digitálnych technológií** mládežou a z toho vyplývajúce negatívne dopady *(napr. sledovanie mobilov počas vyučovania, sledovanie krátkych Tik Tok videí či negatívne pôsobiacich influencerov, flameware na sociálnych sieťach)*, najmä:
   1. Negatívne vplyvy mobilných technológií (mobil, inteligentné hodinky).
   2. Negatívne vplyvy sociálnych sietí na duševné zdravie mládeže.
   3. Toxický obsah v kybernetickom priestore dostupný mládeži.
   4. Negatívne vplyvy digitálnych technológií (najmä pornografie) na vývoj sexuality mládeže [[2]](#footnote-2).
3. Rizikové využívanie digitálnych technológií mládežou a z toho vyplývajúce negatívne dopady *(napr. minimálne zabezpečenie počítača / mobilu, nevhodné heslá, návštevy rizikových webových stránok, zdieľanie citlivého obsahu, žiadne zálohovanie)*
   1. Kybernetické útoky (najnovšie aj s využitím AI).
   2. Malvér napádajúci digitálne zariadenia.
   3. Strata digitálneho obsahu (napr. čo má dieťa na mobile – kontakty, videá, fotografie, texty)
4. Páchanie trestnej činnosti v kybernetickom priestore (obeť / páchateľ), najmä
   1. Kyberšikana
   2. Porušovanie ochrany osobných údajov
   3. Porušovanie autorských práv
   4. Detská pornografia
5. Negatívne vplyvy AI, najmä
   1. Nahrádzanie vlastnej tvorivej práce žiaka v škole nevhodným využitím AI.
   2. Závislosť na AI aplikáciách.
   3. Nárast psychických ťažkostí – porovnávanie sa s „dokonalými“ AI-generovanými avatarmi alebo obsahom môže prispieť k nízkemu sebavedomiu, frustrácii a úzkostiam.
   4. Zníženie hodnoty ľudskej tvorby – vnímanie, že „AI to spraví lepšie alebo rýchlejšie“, môže viesť k znevažovaniu vlastnej práce a znižovaniu motivácie.
   5. AI v škodlivých aplikáciách a aktivitách (hacking, sociálne inžinierstvo).
   6. Obmedzenie rozvoja mentálnych schopností a zručností dieťaťa.
   7. Obmedzenia pracovných príležitostí v mnohých profesiách.
   8. Stále vyššia miera závislosti na digitálnych technológiách.
   9. Zneistenie v oblasti pravdy a reality – rastúci výskyt deepfake videí, textov a obrázkov generovaných AI môže spôsobiť zmätok v rozlišovaní medzi skutočnosťou a manipuláciou.

### Závislosti medzi vybranými rizikami

Medzi jednotlivými rizikami sú závislosti. Grafické znázornenie (podrobnejšie v prílohe v Kap. 7.5):

Obrázok, na ktorom je snímka obrazovky, text, diagram, rad

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.

**Príklady kvantifikácie najčastejších rizík podľa prieskumov a výskumných správ** [[3]](#footnote-3)

* Dospievajúci so svojimi smartfónmi v ruke strávia v priemere viac než štyri hodiny denne. Na smartfón pozrú v priemere 78 krát denne. Najviac ich zaujíma Instagram, YouTube, TikTok a hry [[4]](#footnote-4).
* Z pätnásťročných má 25 percent nadváhu a obezitu [[5]](#footnote-5). Medzi jedenásťročnými chlapcami má až 40 percent nadváhu a obezitu. Až 80 percent týchto detí si obezitu prenáša do dospelosti. S obezitou je spojených 236 ochorení.
* V SR je cca. 360.000 diabetikov (2024). Prediabetes má 140.000 ľudí. Náklady na ich zdravotnú starostlivosť sú ročne vyše 800 mil. € [[6]](#footnote-6)V slovenskej detskej populácii ročne pribúda 120 – 130 nových pacientov [[7]](#footnote-7)
* Podľa najnovšieho prieskumu na jednoznačnú guľatosť Zeme verí menej ako polovica (49,4 %) respondentov vo veku 18-29 rokov. [[8]](#footnote-8)
* Podľa prieskumov sa s kyberšikanou na Slovensku stretlo až 60 % stredoškolákov. [[9]](#footnote-9)
* Podľa prieskumov má skúsenosti s prijímaním intímnych fotografií, videí alebo správ so sexuálnym obsahom tretina slovenských detí a dospievajúcich (33 %) vo veku od 11 do 17 rokov. [[10]](#footnote-10)

## Možná spolupráca a podpora

Do tvorby Katalógu rizík je žiadúce zapojiť čo najširšie spektrum relevantných subjektov v oblasti kybernetickej bezpečnosti, práce s mládežou či riešenia duševného zdravia a nelátkových závislostí.

Spolupráca je možná na viacerých úrovniach:

* Pripomienkovanie jednotlivých verzií Katalógu.
* Námety, podnety a zlepšenia.
* Samostatné vstupy do Katalógu.
* Konzultácie špecifických rizík (napr. nelátkové závislosti, trestné činy, psychosociálne dopady).

## Využitie Katalógu rizík

Katalóg rizík bude možné využiť viacerými spôsobmi:

* Pre žiakov a ich rodičov bude spracovaná zjednodušená forma Katalógu, ktorá im bude verejne prístupná a poslúži ako primárny zdroj informácií o tejto problematike.
* Pre pedagógov bude určená verzia s podrobnejšími informáciami o možných opatreniach na zníženie rizík v školskom prostredí a reakcii na konkrétne udalosti.
* Pre odbornú verejnosť bude podkladom pre návrhy a realizáciu konkrétnych opatrení na zmiernenie rizík.

## Zoznam skratiek a vysvetlenie pojmov

Nakoľko v dokumente sú často používané skratky a pojmy aj mimo kybernetickej bezpečnosti, v úvode uvádzame ich prehľad.

|  |  |
| --- | --- |
| **Skratka** | **Plné znenie** |
| HW | Hardvér, technické vybavenie počítača |
| IS | Informačný systém |
| IT VS | Informačné technológie verejnej správy |
| KB | Kybernetická bezpečnosť |
| KP | Kybernetický priestor |
| MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| MS SR | Ministerstvo spravodlivosti Slovenskej republiky |
| MŠVVaM | Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky |
| MV SR | Ministerstvo vnútra Slovenskej republiky |
| NBÚ | Národný bezpečnostný úrad |
| SW | Softvér, programové vybavenie počítača |
| Zákon o KB, ZoKB, ZKB | Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov |
|  |  |
| Dieťa | Podľa § 127 Trestného zákona dieťaťom sa rozumie osoba mladšia ako osemnásť rokov |
| Mladistvý | Podľa § 94 Trestného zákona osoba, ktorá v čase spáchania trestného činu dovŕšila štrnásty rok a neprekročila osemnásty rok svojho veku, sa považuje za mladistvú. |
| Osoba blízka veku mladistvých | Podľa § 127 Trestného zákona osobou blízkou veku mladistvých sa rozumie osoba, ktorá dovŕšila osemnásty rok svojho veku a neprekročila dvadsaťjeden rokov svojho veku. |
| Mládežník, mládež | Podľa zákona č. 282/2008 o podpore práce s mládežou v znení neskorších predpisov, §2, písm. a)  mládežník je osoba, ktorá dovŕšila vek najviac 30 rokov,  mládež je skupina najmenej troch mládežníkov |
|  |  |
| Digitálny wellbeing | Digitálny wellbeing vo vzdelávaní sa chápe ako pocit fyzickej, kognitívnej, sociálnej a emocionálnej spokojnosti, ktorý umožňuje všetkým jednotlivcom pozitívne sa zapájať do všetkých digitálnych vzdelávacích prostredí, a to aj prostredníctvom nástrojov a metód digitálneho vzdelávania a odbornej prípravy (The council of the European  Union, 2022). |
| Deep fake | Tento pojem vznikol kombináciou slov „deep learning“ (hĺbkové učenie) a „fake“ (falošný)’; označuje techniku vytvárania zmanipulovaných, veľmi realistických multimediálnych obsahov (najmä videí a zvukov) pomocou umelej inteligencie. |

## Definícia základných pojmov v oblasti kybernetickej bezpečnosti

**Podľa zákona o kybernetickej bezpečnosti [[11]](#footnote-11)**

Na účely tohto zákona sa rozumie

b) **informačným systémom** funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,

c) **kybernetickým priestorom** globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

d) **kontinuitou** strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

e)  **dôvernosťou záruka**, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

f) **dostupnosťou** záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované,

g) **integritou** záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené,

h) **kybernetickou bezpečnosťou** stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

i) **rizikom** potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu,

j) **kybernetickou hrozbou** kybernetická hrozba podľa čl. 2 bodu 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881“),

m) **kybernetickým bezpečnostným incidentom** udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov,

q) **zraniteľnosťou** akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou,

**Podľa zákona o informačných technológiách vo verejnej správe (95/2019 Z. z)**

Na účely tohto zákona sa ďalej rozumie

u) **aktívom**

* programové vybavenie,
* technické zariadenie,
* poskytovaná služba,
* kvalifikovaná osoba,
* dobré meno orgánu riadenia a
* informácia,
* dokumentácia,
* zmluva
* a iná skutočnosť, ktorú považuje orgán riadenia za citlivú.

**Slovník pojmov kybernetickej a informačnej bezpečnosti – metodický materiál MIRRI [[12]](#footnote-12)**

**Hrozba**

[threat] je objektívne existujúca potenciálna možnosť priamo alebo nepriamo narušiť systém, informácie, ktoré sa v ňom spracovávajú alebo iné aktíva organizácie.

**Riziko**

[risk] je veličina závisiaca od závažnosti (možného dopadu) →hrozby a pravdepodobnosti, že sa hrozba naplní.

**Zraniteľnosť**

[vulnerability] vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej hrozby. Napr. pripojenie nechráneného počítača k Internetu umožňuje hackerský útok, neaktuálna databáza vírusov je zraniteľnosťou umožňujúcou napadnutie počítača zlomyseľným softvérom.

## Vecný rámec základných pojmov v oblasti bezpečnosti

Aktíva

Nad rámec definície uvedenej v kap. 1.1 v tomto dokumente pod aktívom chápeme všetko, čoho narušením, poškodením, zničením utrpí osoba alebo spoločnosť škodu alebo ujmu.

*Aktívom je okrem IKT napr. zdravie dieťaťa, jeho rodina, sociálne vzťahy, zamestnanie, obydlie, auto, finančné príjmy; ale aj napr. dobre vychované deti, čistý register trestov, postavenie v zamestnaní, vnútorný pocit spokojnosti, duševná pohoda.*

Hrozba

Pod pojmom hrozba chápeme potenciálnu udalosť, jav, aktivitu, činnosť - ktorá môže narušiť aktívum a spôsobiť škodu alebo ujmu.

*Príkladom hrozby je úder blesku, požiar, záplava, ukradnutie počítača, hackerský útok, technická porucha zariadenia, chyba používateľa pri práci s IKT, strata USB, zneužitie dieťaťa, finančný podvod, šikana, vydieranie, hrubý nátlak, dostať infarkt a pod.*

**Zraniteľnosť**

Pod pojmom zraniteľnosť chápeme vlastnosť aktíva alebo stav jeho okolia, ktorý zvyšuje možnosť realizácie hrozby alebo rozsah možnej škody.

*Príkladom zraniteľnosti je dom v záplavovej oblasti, neuzamknutý byt, viditeľne položený notebook na sedadle zaparkovaného auta, neaktualizovaný softvér, USB ponechané na pracovnom stole, zálohy údajov na tom istom mieste ako samotné údaje, jednoduché heslo, ponechanie liekov alebo chemikálií na mieste dostupnom dieťaťu, horľaviny uskladnené v byte, slabá znalosť rizík kybernetického priestoru.*

*Poznámka: Častá otázka je - aký je rozdiel medzi hrozbou a zraniteľnosťou? Realizácia zraniteľnosti nespôsobuje škodu, na rozdiel od realizácie hrozby.*

**Riziko**

Pod pojmom riziko chápeme v zmysle definície uvedenej v kap. 1.1 mieru, ktorá nám hovorí nakoľko máme brať hrozbu vážne. Závisí od miery dopadov hrozby a od pravdepodobnosti realizácie hrozby. Riziko je vyššie, ak je možná škoda väčšia, alebo sa zvyšuje pravdepodobnosť realizácie hrozby.

*Napr. riziko zrážky so zverou sa zvyšuje podvečer – vyššia pravdepodobnosť prebiehania zveri cez cestu. Riziko je vyššie, ak nie som v aute sám, ale sú tam aj deti – možná ujma v dôsledku zranení je vyššia.*

*Poznámka: riziko vyhodnocuje neustále každý mnohobunkový organizmus a táto schopnosť je stará stovky miliónov rokov. Podceňovanie rizika (mne sa to nemôže stať) je časté u detí, ale aj niektorých dospelých. Darwinovská evolúcia eliminuje nositeľov tohto prístupu (viď aj sarkastické Darwinove ceny).*

*Príklady podceňovania rizika: plnenie hlúpych výziev Tik-toku, prebehovanie cez cestu na červenú, „super výnosné“ investície do kryptomien, obiehanie v neprehľadnej zákrute, zasielanie sexuálne citlivého obsahu iným osobám, provokácia do bitky, ignorovanie potreby anti-malware softvéru, skok hlavičkou do neznámej vody, odmietanie poistenia pri ceste do zahraničia (veď zatiaľ sa mi nič nestalo).*

## Stručný úvod do manažmentu bezpečnosti

V tejto kapitole je uvedený stručný úvod do problematiky manažmentu bezpečnosti.

**Možný zjednodušený prístup k riešeniu problémov**, vrátane problémov s bezpečnosťou:

*(vhodný prístup pre rodičov v domácom prostredí)*

1. V čom je problém?
2. Aký veľký je problém?
3. Čo s tým vieme spraviť?
4. Riešme ho v rámci svojich možností!
5. Vyhodnoťme úspešnosť riešenia!

**Prístup k systémovému riešeniu bezpečnosti**

Systémové riešenie bezpečnosti v ľubovoľnej oblasti je realizované na rovnakých princípoch a základných postupoch:

1. Analytická fáza
   1. Identifikácia aktív, ktoré sú predmetom ochrany.
   2. Identifikácia vlastníkov aktív, ktorí zodpovedajú za ich ochranu.
   3. Identifikácia možných hrozieb pre tieto aktíva.
   4. Identifikácia zraniteľností, ktoré môžu zvyšovať pravdepodobnosť realizácie hrozby, alebo možnú škodu.
   5. Identifikácia a posúdenie miery možných dopadov, následkov resp. škôd, ktoré môže realizovaná hrozba spôsobiť.
   6. Identifikácia a posúdenie doteraz realizovaných bezpečnostných opatrení.
   7. Identifikácia možných scenárov rizík resp. realizácie hrozieb.
   8. Posúdenie pravdepodobnosti resp. možnosti realizácie hrozby.
   9. Určenie miery rizika pre jednotlivé scenáre.
   10. Vytvorenie Katalógu rizík.
2. Realizačná fáza
   1. Rozhodnutie o spôsobe riadenia rizík na úrovni zodpovedných osôb a organizačných štruktúr.
   2. Návrh možných vhodných opatrení na zníženie miery rizika.
   3. Posúdenie primeranosti navrhovaných opatrení (s ohľadom na náklady a mieru rizika).
   4. Implementácia schválených opatrení na zníženie miery rizika.
   5. Posúdenie miery rizika po implementácii bezpečnostných opatrení.
   6. Plánovanie kontinuity činností v prípade úspešnej realizácie hrozby.
3. Kontrolná fáza
   1. Testovanie dosiahnutej úrovne bezpečnosti.
   2. Pravidelná kontrola a aktualizácia výstupov horeuvedených aktivít.

# Katalóg rizík – vnútorné členenie a prístup

V tejto kapitole sú uvedené podklady k návrhu štruktúry Katalógu rizík.

## Štruktúra Katalógu

Katalóg bude mať viacero relatívne samostatných častí, uvádzame ich navrhovanú štruktúru:

1. **Aktíva (text, tabuľka)**
   1. ID aktíva
   2. Oblasť aktív
   3. Názov aktíva
   4. Opis aktíva
2. **Hrozby a riziká (text, tabuľka)**
   1. ID hrozby
   2. Oblasť hrozieb
   3. Podoblasť hrozieb (voliteľné)
   4. Názov hrozby
   5. Opis hrozby
   6. Typické scenáre realizácie rizika
   7. Možné dopady hrozby
   8. Pravdepodobnosť naplnenia scenára rizika
   9. Zraniteľnosti
   10. Miera rizika
   11. Zdroje informácií o hrozbe (voliteľné)
   12. Možné opatrenia
   13. Doplnkové informácie (voliteľné)
3. **Dopady (text)**
   1. ID dopadu
   2. Oblasť dopadu
   3. Názov dopadu
   4. Opis dopadu
   5. Klasifikácia miery dopadu
   6. Zdroje informácií o dopade (voliteľné)
   7. Doplnkové informácie (voliteľné)
4. **Zraniteľnosti (text)**
   1. ID zraniteľnosti
   2. Oblasť zraniteľnosti
   3. Názov zraniteľnosti
   4. Opis zraniteľnosti
   5. Scenáre zneužitia zraniteľnosti
   6. Zdroje informácií o zraniteľnosti (voliteľné)
   7. Doplnkové informácie (voliteľné)
5. **Možné opatrenia (text)**
   1. ID opatrenia
   2. Oblasť opatrení
   3. Názov opatrenia
   4. Opis opatrenia
   5. Zdroje informácií o opatrení
   6. Doplnkové informácie

## Členenie oblastí hrozieb a zraniteľností

V tejto kapitole je uvedený návrh členenia hrozieb a zraniteľností týkajúcich sa mládeže a jej aktivít súvisiacich s kybernetickým priestorom a vplyvom kybernetického priestoru na ňu.

1. **Štandardné hrozby pre IKT (v zmysle metodiky NBÚ a MIRRI)**
   1. Domáce prostredie
   2. Školské prostredie
   3. Mobilné prostredie (najmä mobily a inteligentné hodinky mimo domova)
2. **Hrozby súvisiace s páchaním trestnej činnosti (TČ)**
   1. špecifické pre kybernetický priestor (obeť)
   2. špecifické pre kybernetický priestor (páchateľ)
   3. s využitím kybernetického priestoru (obeť)
   4. s využitím kybernetického priestoru (páchateľ)
3. **Psychosociálne hrozby, najmä:**
   1. Nelátkové závislosti dieťaťa, rodičov
      1. Mobil
      2. Sociálne siete
      3. Počítačové hry
      4. Virtuálny gambling (online kasína)
      5. Digitálna erotika a pornografia
      6. Iné (napr. nakupovanie na internete, digitálne médiá)
   2. Nadmerné používanie digitálnych technológií – dieťa, rodičia, sociálne okolie
      1. Mobil
      2. Sociálne siete
      3. Počítačové hry
      4. Konzumácia internetového obsahu
      5. AI
      6. Iné
   3. Nevhodné používanie digitálnych technológií
      1. Sociálne siete
      2. Počítačové hry
      3. Konzumácia internetového obsahu, najmä
         1. Pornografia
         2. Násilie
         3. Podnecovanie k nenávisti
         4. Podnecovanie k diskriminácii
   4. Narušenie sociálnych väzieb
      1. V rodine
      2. V školskom prostredí
      3. Priatelia a známi
   5. Nezdravý sociálny rozvoj
      1. Radikalizácia
      2. Jednostranné názory
      3. Znížené kognitívne schopnosti
      4. Poškodená emočná inteligencia
   6. Negatívne emócie
      1. Frustrácia
      2. Stres
      3. Depresia
      4. Pocity menejcennosti
   7. Diskriminácia
   8. Útoky voči osobe v KP
      1. Ohováranie
      2. Podnecovanie k nenávisti k osobe
      3. Vyhrážanie
      4. Kyberšikana
4. **Digitálne vylúčenie, najmä:**
   1. Osoby zo sociálne znevýhodneného prostredia
   2. Zdravotne znevýhodnené osoby
   3. Osoby s nižšou mierou psychosociálnej odolnosti
5. **Stratené príležitosti (v dôsledku spotreby času na aktivity v KB), najmä:**
   1. Rozvoj pracovných schopností
   2. Šport
   3. Kultúra
   4. Rozvoj sociálnych vzťahov priameho kontaktu v rodine, s rovesníkmi, v škole
   5. Zábava vo fyzickom svete (s priateľmi, známymi)
   6. Budovanie partnerských vzťahov
6. **Zdravotné hrozby a súvisiace dopady, najmä:**
   1. Nezdravý životný štýl
      1. Narušenie spánku
         1. Nedostatok spánku
         2. Nekvalita spánku
      2. Chýbajúce pohybové aktivity
      3. Nadmerné / nevhodné sedenie
         1. Nevhodná stolička
         2. Dlhé neprerušované sedenie bez ďalšieho pohybu
      4. Záťaž očí
         1. Dlhodobé sledovanie mobilu, tabletu, monitora
         2. Malé písmo v mobile
         3. Nevhodná vzdialenosť od zobrazovacieho zariadenia"
         4. Nesprávne nastavenie zobrazenia
         5. Zastaralá zobrazovacia jednotka
         6. Modré svetlo v noci
      5. Problémy s chrbticou
      6. Problémy so zápästiami
      7. Sluch
         1. Nesprávna vzdialenosť od zdroja a vysoká hlasitosť počúvania hudby
      8. Nezdravé stravovanie počas pobytu v KB
      9. Dlhodobý vplyv negatívnych emócií
      10. Narušenie prirodzeného dopamínového cyklu
      11. Neurologické zmeny mozgu
      12. Dlhodobý stres
   2. Zranenia
      1. Pri prechode cez cestu, železničnú trať so slúchadlami, mobilom
   3. Možné epigenetické vplyvy na dieťa od závislých rodičov.
7. **Ekonomické hrozby pre žiaka a rodinu, najmä:**
   1. Nadmerné náklady na digitálne technológie
   2. Hrozby pre finančné aktíva rodiny / žiaka
   3. Dočasné alebo celoživotné zníženie príjmov
8. **Hrozby pre štát ako celok, najmä:**
   1. Zníženie úrovne pracovných schopností mladej populácie vstupujúcej na trh práce
   2. Zníženie konkurencieschopnosti SR
   3. Predčasné úmrtie / Invalidita dieťaťa
   4. Náklady na liečenie (závislosti) dieťaťa
   5. Nepriaznivá demografická situácia

## Členenie podľa špecifických skupín

Členenie slúži pre identifikáciu rizík špecifických pre jednotlivé kategórie mládeže zohľadňujúce osobitné zraniteľnosti a znevýhodnenia.

1. **Vekovo špecifické** 
   1. Pred počatím (budúca mamička)
   2. Prenatálne obdobie (plod)
   3. Novorodenec (0 – 28 dní)
   4. Dieťa (právne)
      1. Dojča (29 dní – 1 rok)
      2. Batoľa (od 1 roka do 3 rokov)
      3. Predškolský vek (3 - 6 rokov)
      4. Mladší školský vek (6 – 12 rokov)
      5. Starší školský vek (12 – 15 rokov), začiatok puberty
   5. Adolescent (15 – 18 rokov, trestná zodpovednosť)
   6. Osoba blízka veku mladistvých (18-21, právny pojem)
   7. Mladšia dospelosť (21 – 30) - obdobie mladého muža a ženy;

Pre úplnosť uvádzame pokračovanie členenia:

* 1. *Stredná dospelosť (30 – 45) - obdobie zrelého muža a zrelej ženy*
  2. *Staršia dospelosť (45 – 60) - stredný vek; prechodný vek*
  3. *Ranná staroba (60 – 75)*
  4. *Pokročilá staroba (75 – 90)*
  5. *Krajná staroba (90+)*

1. **Inteligencia**
   1. genialita
   2. vysoko nadpriemerná inteligencia
   3. nadpriemerná inteligencia
   4. priemerná inteligencia
   5. podpriemerná inteligencia
   6. hraničná duševná zaostalosť
   7. ľahká duševná zaostalosť (staršie: debilita)
   8. stredná duševná zaostalosť (staršie: imbecilita)
   9. ťažká duševná zaostalosť (staršie: imbecilita)
   10. hlboká duševná zaostalosť (staršie: idiocia)

Podľa MKCH 10:

Obrázok, na ktorom je text, snímka obrazovky, písmo, číslo

Automaticky generovaný popis

1. **Psychické - p**oruchy učenia
   1. Špecifická porucha čítania - dyslexia F81.0
   2. Špecifická porucha hláskovania - dysortografia F81.1
   3. Špecifická porucha aritmetických schopností - dyskalkúlia F81.2
   4. Zmiešaná porucha školských zručností - F81.3
   5. Iná vývinová porucha školských zručností - dysgrafia F81.8
   6. Vývinová porucha školských zručností, bližšie neurčená - F81.9
2. **Sociálne** 
   1. Osoba zo sociálne znevýhodneného prostredia (NIVAM [[13]](#footnote-13)), rodina
      1. ktorej sa poskytuje pomoc v hmotnej núdzi a príjem rodiny je najviac vo výške životného minima,
      2. v ktorej aspoň jeden z rodičov alebo osoba, ktorej je dieťa zverené do osobnej starostlivosti patrí do skupiny znevýhodnených uchádzačov o zamestnanie,
      3. v ktorej najvyššie ukončené vzdelanie rodičov je základné, alebo aspoň jeden z rodičov nemá ukončené základné vzdelanie,
      4. ktorá má neštandardné bytové a hygienické podmienky (napr. žiak nemá vyhradené miesto na učenie, nemá vlastnú posteľ, nie je zavedená elektrická prípojka a pod.)
3. **Digitálne vylúčenie**
   1. Chýbajúci alebo obmedzený prístup k digitálnym technológiám vedúci k možnému čiastočnému alebo plnému vylúčeniu v rámci reálnych aj virtuálnych komunít:
      1. k mobilu
      2. k počítaču
      3. k hernej konzole
      4. k tlačiarni
      5. k 3D tlačiarni
      6. k virtuálnej realite (v blízkej budúcnosti)
      7. k populárnym aplikáciám
      8. na internet
      9. na sociálne siete
      10. možnosť internetových platieb
   2. Chýbajúce znalosti a zručnosti
      1. všeobecné použitie
         1. počítača
         2. mobilu
      2. použitie kancelárskych aplikácií
      3. použitie špecializovaných aplikácií
      4. využívanie služieb na internete
      5. vyhľadávanie
      6. Využívanie sociálnych sietí
      7. Využívanie AI

## Členenie vplyvov / dopadov

V kapitole je uvedený prehľad možných negatívnych vplyvov, ktoré môžu byť spôsobené digitálnymi technológiami, alebo ku ktorým digitálne technológie prispievajú.

1. Zdravotné
   1. Nezdravý životný štýl
      1. Nedostatočné pohybové aktivity
         1. Nadváha
         2. Obezita
         3. Zvýšenie rizika následných civilizačných chorôb
      2. Znížené pohybové schopnosti
      3. Nadmerné / nevhodné sedenie
      4. Nadmerná záťaž očí
      5. Problémy s chrbticou
      6. Problémy so zápästiami
      7. Dopady nadmerného počúvania hudby na sluch
      8. Nezdravé stravovanie a pitný režim počas dlhodobého pobytu v KB
      9. Dlhodobý vplyv negatívnych emócií
      10. Narušenie prirodzeného dopamínového cyklu
      11. Neurologické zmeny mozgu
   2. Civilizačné choroby
   3. Duševné choroby
   4. Narušená plodnosť
   5. Non well-being
   6. Nárast rozsahu invalidity
2. Psychosociálne
   1. Digitálne a následne sociálnej vylúčenie
      1. Kvôli chýbajúcim technológiám (mobil, PC, Internet)
      2. Kvôli chýbajúcim zručnostiam
      3. Z virtuálnych komunít
   2. Komunikácia
      1. Fyzická izolovanosť vedúca k nižšej miere fyzickej komunikácie
      2. Znižovanie schopnosti kvalitnej fyzickej komunikácie
      3. Komunikácia v „bublinách“ – virtuálnych komunitách
      4. Nárast počtu virtuálnych „priateľov“ na úkor znižovania počtu reálnych
      5. Vytváranie nezdravých vzťahov s umelou inteligenciou (chatboty, virtuálne bytosti)
         1. Emocionálna závislosť od chatbotu
      6. Problémy v komunikácii s budúcim partnerom / partnerkou
   3. Motorika
      1. Zníženie úrovne jemnej motoriky v dôsledku obmedzenia ručného písania
      2. Jednostranný rozvoj motoriky palca
   4. Mentálne schopnosti
      1. Znižovanie schopnosti a možnosti odlíšiť pravdu od fikcie
      2. Znižovanie schopnosti dlhodobo si udržať pozornosť (napr. pri učení)
3. Ekonomické
   1. Na osobu
      1. Nižšia úroveň pripravenosti na začlenenie sa do pracovného procesu
      2. Pokles záujmu o kariérny rast
      3. Preferencia virtuálnych aktivít na úkor ekonomických
      4. Preferencie pre „mama hotel“ s nedostatočným záujmom o ekonomickú samostatnosť
   2. Na štát
      1. Znižovanie konkurencieschopnosti štátu
      2. Zníženie rastu DPH
      3. Zvýšené zaťaženie vyplácania sociálnych dávok
4. Spoločenské
   1. Demografické, príspevok ku:
      1. Vysokému percentu mladých žijúcich v spoločnej domácnosti s rodičmi (58 % [[14]](#footnote-14))
      2. Vysokej rozvodovosti
      3. Znižovaniu úrovne fertility
      4. Nárastu rozsahu bezdetnosti
         1. Osoby, ktoré nemôžu mať deti
         2. Osoby, ktoré chcú deti, ale nemajú vhodného partnerku / partnera
         3. Osoby, ktoré nechcú deti
      5. Preferencii štúdia v zahraničí bez návratu po škole
      6. Preferencii migrácie u mladej generácie
   2. Sociálna kohézia, príspevok ku:
      1. Významnému narušeniu sociálnej kohézie
      2. Nárastu polarizácie a antagonizmov v spoločnosti
      3. Rastúcej názorovej polarizácii v oblasti dôležitých spoločenských tém
      4. Rastúcej miery agresie voči názorovým oponentom
      5. Narúšaniu medzigeneračnej solidarity
   3. Obranyschopnosť, príspevok ku:
      1. Zníženiu úrovne fyzických schopností u mladých s dopadom na obranu krajiny v prípade vojnového konfliktu
      2. Neochote brániť krajinu v prípade vojnového konfliktu (len 27 % by bolo ochotných brániť svoju krajinu [[15]](#footnote-15)).
   4. Odolnosť spoločnosti
      1. Rastúca závislosť spoločnosti a osobitne mladej generácie  na digitálnych technológiách tak, že bez nich nie je schopná vykonávať stále väčší rozsah bežných činností.
      2. Rastúca závislosť spoločnosti na digitálnej infraštruktúre tak, že pri jej narušení dochádza k významnému narušeniu fungovania spoločnosti (viď prípad Španielska a jeho výpadku energie – blackoutu [[16]](#footnote-16)). Triviálny prípad - vypadne platobný systém a mladí nemajú hotovosť.
      3. Rastúci dopad závažných kybernetických bezpečnostných incidentov na spoločnosť, vrátane mladej generácie.

## Výber prístupu k analýze rizík

V zmysle metodiky NIST / NBÚ[[17]](#footnote-17) sú odporúčané 3 možné prístupy k analýze rizík:

1. Prístup orientovaný na hrozby (z angl. Threat oriented)
   1. Identifikuje zdroje hrozieb a udalosti
   2. Umožňuje rozvinúť scenáre a modely hrozieb
   3. Identifikuje zraniteľnosti v kontexte hrozieb
2. Prístup orientovaný na aktíva a dopady (z angl. Asset-Impact oriented)
   1. Identifikuje aktíva kritické pre činnosti (z angl. business critical / mission critical) –
   2. Umožňuje analýzu dôsledkov hrozieb a udalostí
   3. Identifikuje zraniteľnosti voči udalostiam ohrozenia kritických aktív so závažným nepriaznivý vplyvom
3. Prístup orientovaný na zraniteľnosti (z angl. Vulnerability-oriented)
   1. Identifikuje predispozičné podmienky
   2. Identifikujte zneužiteľné zraniteľnosti
   3. Identifikujte hrozby v kontexte známych/identifikovaných zraniteľnosti

Obrázok, na ktorom je text, snímka obrazovky, písmo, vizitka

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Pre účel nášho dokumentu sme si zvolili nasledovné prístupy:

* Pre hodnotenie rizík v školskom, domácom a externom IKT prostredí sme zvolili prístup orientovaný na hrozby. Zoznam možných hrozieb je uvedený v metodike NBÚ a MIRRI.
* Pre hodnotenie rizík mimo IKT sme zvolili prístup orientovaný na aktíva a dopady. Je to preto, lebo interakcia mládeže s kybernetickým priestorom má významné dopady aj na jej zdravie, ktoré je kritické aktívum dieťaťa.
  + Preto v kap. 3 sú detailne analyzované aktíva, relevantné pre posúdenie rizík pre dieťa v interakcii s kybernetickým priestorom.

Viaceré medzinárodné inštitúcie vypracovali klasifikačné schémy pre riziká mládeže v digitálnom resp. online prostredí (mimo klasických IKT hrozieb). V zmysle našej terminológie je nimi chápané digitálne alebo online prostredie časťou kybernetického priestoru.

Klasifikácie vychádzajú z prístupov orientovaných na hrozby, viď príloha 7.2.

V nasledujúcich verziách dokumentu bude realizované premapovanie medzi klasifikačnými schémami založenými na zdrojoch hrozieb a klasifikačnými schémami založenými na aktívach (viď kap. 3).

## Spôsob určenia miery rizika

Ako bolo uvedené v kap. 1.6 - v definícii základných pojmov:

„rizikom sa rozumie potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu“.

Aby sme tento potenciál resp. mieru rizika posúdili, potrebujeme:

* ohodnotiť mieru možnej straty / narušenia / dopadu / následku pre aktíva v dôsledku bezpečnostného incidentu resp. realizácie hrozby,
* ohodnotiť pravdepodobnosti výskytu bezpečnostného incidentu resp. realizácie hrozby.

Ohodnotenie je možné:

* Kvantitatívne: napr. strata 12.000 €, pravdepodobnosť incidentu 30 % v priebehu roka.
* **Kvalitatívne**: pomocou definovanej škály (prístup podľa metodiky MIRRI a NBÚ).

**Hodnotenie v kvalitatívnej škále rozšírené o aktíva dieťaťa**

Hodnotiaca škála v zmysle metodiky MIRRI je rozšírená nielen pre IKT aktíva, ale aj ostatné aktíva dieťaťa.

**Ohodnotenie dopadov / následkov**

*Klasifikácia následkov vyjadrená stupňom v zmysle metodiky MIRRI, rozšírená pre účely dokumentu.*

**K** – katastrofický

**S** – stredný

**Z** – závažný

**M** – malý

**ZN** – zanedbateľný

**K:** katastrofický – strata alebo výrazné poškodenie kritických aktív IKT, dlhodobé prerušenie služieb poskytovaných IKT;

významné dočasné alebo trvalé poškodenie zdravia dieťaťa alebo jeho psychosociálnej pohody, zásadné ohrozenie výkonu a funkčnosti primárnych procesov výchovy a rozvoja dieťaťa, finančné škody ohrozujúce existenciu rodiny.

**Z:** závažný – narušenie alebo poškodenie aktív IKT, strednodobé prerušenie služieb poskytovaných IKT,

spôsobenie preukázateľného narušenia IKT bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie následkov realizovanej hrozby;

dočasné poškodenie zdravia dieťaťa alebo jeho psychosociálnej pohody, ohrozenie výkonu a funkčnosti niektorých procesov výchovy a rozvoja dieťaťa, finančné škody vážne narúšajúce rozpočet rodiny.

**S**: stredný – isté narušenie IKT aktív alebo ich bezpečnosti. Následok neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných schopností rodiny, generuje isté personálne a finančné nároky;

možné ohrozenie zdravia dieťaťa alebo jeho psychosociálnej pohody, možné narušenie výkonu a funkčnosti niektorých procesov výchovy a rozvoja dieťaťa, finančné škody narúšajúce rozpočet rodiny.

**M**: malý – následok neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi;

možné narušenie psychosociálnej pohody dieťaťa, možné malé narušenie výkonu a funkčnosti niektorých procesov výchovy a rozvoja dieťaťa, finančné škody nenarúšajúce rozpočet rodiny;

**Zn**: zanedbateľný - následok akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných schopností a povinností bez potreby dodatočných zdrojov na odstránenie následkov.

**Ohodnotenie pravdepodobnosti / očakávania / možnosti realizácie hrozby**

*Klasifikácia pravdepodobnosti je vyjadrená stupňom ohodnotenia v zmysle metodiky MIRRI rozšírená pre účely dokumentu.*

**VV:** veľmi vysoká - je takmer isté, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú súvisiace zneužiteľné zraniteľnosti a nie sú zavedené žiadne bezpečnostné opatrenia na ochranu;

prevalencia negatívneho javu v detskej populácii je viac ako 15 %.

**V:** Vysoká - je pravdepodobné, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú súvisiace zneužiteľné zraniteľnosti a zavedené bezpečnostné opatrenia sú neefektívne alebo zastarané;

prevalencia negatívneho javu v detskej populácii je viac ako 5 %.

**S:** stredná - je potenciálne možné, že v stanovenom čase nastane naplnenie scenára rizika, pretože existujú zneužiteľné zraniteľnosti a zavedené bezpečnostné opatrenia by mohli byť vylepšené

prevalencia negatívneho javu v detskej populácii je viac ako 1 %.

**N:** nízka - je nepravdepodobné, že v stanovenom čase nastane naplnenie scenára rizika, pretože súvisiace zraniteľnosti boli pokryté vhodnými bezpečnostnými opatreniami

prevalencia negatívneho javu v detskej populácii je menej ako 1 %.

**VN**: veľmi nízka - je vysoko nepravdepodobné, že by v stanovenom čase malo nastať naplnenie

scenára rizika, pretože súvisiace zraniteľnosti boli pokryté efektívnymi bezpečnostnými opatreniami

prevalencia negatívneho javu v detskej populácii je menej ako 0,1 %.

**Klasifikácia závažnosti rizika**

*Klasifikácia závažnosti rizík vyjadrená stupňom v zmysle metodiky MIRRI, rozšírená pre účely dokumentu.*

**VV** – Veľmi vysoké

**V** – Vysoké

**S** – Stredné

**N** – Nízke

**VN** – Veľmi nízke / zanedbateľné

**VV –** veľmi vysoké: riziko nie je akceptovateľné, riziko bezprostredne a závažne ohrozuje primárne aktíva dieťaťa a IKT aktíva IS v ktorom pracuje, jeho bezpečnosť, ako aj procesy jeho zdravého rozvoja. (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, závažné následky na pre zdravie a život, atď.) Riziko si vyžaduje bezpodmienečné prijatie ďalších bezpečnostných opatrení na jeho zmiernenie.

**V –** vysoké: nie je akceptovateľné, riziko závažne ohrozuje primárne aktíva dieťaťa a IKT aktíva IS v ktorom pracuje, jeho bezpečnosť, ako aj procesy jeho zdravého rozvoja.

Bezpečnostné opatrenia na jeho zmiernenie by mali byť prijaté, avšak deti nie sú ním akútne ohrozená vo veľkom rozsahu.

**S –** stredné: riziko nie je akceptovateľné, riziko potenciálne ohrozuje primárne aktíva dieťaťa a IKT aktíva IS v ktorom pracuje, jeho bezpečnosť, ako aj procesy jeho zdravého rozvoja.

Bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dobe, ktorú určí vlastník rizika (rodič, spoločnosť).

**N:** nízke – riziko je akceptovateľné, ale musí byť ďalej priebežne monitorované, riziko neohrozuje primárne aktíva dieťaťa a IKT aktíva IS v ktorom pracuje, ohrozuje výkon niektorých podporných procesov zdravého fungovania a rozvoja dieťaťa v digitálnom prostredí.

V niektorých prípadoch môže byť pre toto riziko navrhnuté bezpečnostné opatrenie,

**VN**: veľmi nízke – riziko je akceptovateľné, nie sú vyžadované žiadne ďalšie bezpečnostné opatrenia, riziko neohrozuje aktíva dieťaťa a IKT aktíva IS v ktorom pracuje.

**Určenie výsledného rizika (podľa metodiky MIRRI) [[18]](#footnote-18)**

**Obrázok, na ktorom je text, snímka obrazovky, číslo

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.**

# Aktíva

Aktívom pre účely tohto dokumentu chápeme to, čo je pre nás (dieťa, rodič, pedagóg, škola, štát) dôležité a čoho narušením utrpíme škodu alebo ujmu[[19]](#footnote-19). Právna definícia pre IKT je uvedená v kap. 1.1.

Vymedzenie aktív je dôležité pre špecifikáciu hrozieb a zraniteľností. Hrozba a zraniteľnosť sa týka konkrétneho aktíva (napr. financie na účte, mobil, osobná integrita dieťaťa, jeho zdravie).

Členenie aktív, ktoré sú brané do úvahy pri tvorbe Katalógu rizík pre mládež v kybernetickom priestore je navrhované nasledujúco:

## Aktíva priamo súvisiace s IKT

V tejto kapitole je uvedený prehľad aktív pre jednotlivé IKT prostredia, aj aktíva mimo IKT (napr. aktíva dieťaťa ako fyzickej osoby, finančné aktíva).

Nakoľko v textovej forme je veľký zoznam aktív pomerne neprehľadný, je k dispozícii aj tabuľková verzia prehľadu.

### Aktíva súvisiace v IKT v domácnosti

Sú to aktíva, ktoré sa týkajú IKT bežnej domácnosti, kde predpokladáme existenciu domáceho PC pripojeného na Internet. V  komunitách so sociálne znevýhodneným prostredím to nemusí platiť.

1. **Činnosti a agendy podporované domácim** IKT (primárne aktívum v zmysle metodiky MIRRI)
   1. ***Dieťa / Žiak / Študent***
      1. Dištančná výučba (typicky počas COVIDu, individuálny študijný plán)
      2. Príprava do školy, školské úlohy
      3. Všeobecné vzdelávanie / práca s informačnými zdrojmi
      4. Komunikácia so školou (typicky cez EduPage a maily)
      5. Realizácia platobných operácií (ak má kompetenciu)
      6. Virtuálne sociálne aktivity
         1. SMS komunikácia
         2. Chatovanie
         3. Mailová komunikácia
         4. Video komunikácia
         5. Sociálne siete
            1. Influencer
            2. Lajkovanie (klik na „páči sa mi“) a diskusie
            3. Šírenie obsahu
            4. Pasívny používateľ (prezeranie obsahu)
      7. Voľnočasové digitálne aktivity
         * 1. IKT krúžky
           2. Tvorba vlastného digitálneho obsahu
           3. Vývoj vlastného SW
           4. Počítačové hry
   2. ***Rodičia*** 
      1. Aktivity súvisiace so starostlivosťou o dieťa
      2. Práca s informačnými zdrojmi pri podpore dieťaťa
      3. Komunikácia so školou (typicky EduPage)
      4. Realizácia platobných operácií v prospech dieťaťa / rodiny
      5. Sociálne aktivity (ktoré dieťa vníma a inšpiruje sa nimi)
         1. SMS komunikácia
         2. Chatovanie
         3. Mailová komunikácia
         4. Video komunikácia
         5. Sociálne siete
      6. Ďalšie digitálne aktivity
         1. Tvorba vlastného digitálneho obsahu
         2. Vývoj vlastného SW
         3. Počítačové hry
   3. Vlastné pracovné aktivity
2. **Priestory**
   1. Objekt (obydlie dieťaťa, pri striedavej starostlivosti aj dve)
   2. Miestnosti umiestnenia informačných aktív (router, stolné PC, tlačiareň)
   3. Pracovisko
      1. Stôl
      2. Stolička
      3. Vonkajšie osvetlenie
      4. Vnútorné osvetlenie
   4. Vhodné prostredie
      1. Vhodná teplota
      2. Vhodná vlhkosť
      3. Minimálna prašnosť
3. **Sieťová infraštruktúra**
   1. Kabeláž (optika, metalická po obydlie)
   2. Interná kabeláž
   3. Switch
   4. Router
      1. CPE ktoré dodáva ISP
   5. Rádiový priestor (RF) a priestor pre iné typy bezdrôtových pripojení (IR)
   6. Samostatné zariadenia technológie IEEE 802.11
      1. Access point, ktorý nie je súčasťou WiFi routera.
      2. WiFi Repeater
      3. WiFi Mash systémy
   7. Technológie IEEE 802.15.1 (Bluetooth)
4. **Hardvér**, najmä
   1. Počítač
      1. Klávesnica
      2. Monitor
      3. Myš
      4. Prepojovacie káble
   2. Ďalšie periférne zariadenia
      1. Tlačiareň
      2. Multifunkčné zariadenie
      3. Reproduktory
      4. Slúchadlá a mikrofón
         1. Bezdrôtové
      5. Kamera
      6. Iné (napr. 3D tlačiareň)
   3. Mobilné zariadenia
      1. Notebook
      2. Tablet
      3. Smartfón
      4. Inteligentné hodinky
   4. Špecializovaný HW (napojený na Internet)
      1. Smart TV
      2. Digitálne rádiá
      3. Inteligentné hračky
      4. Domáce spotrebiče
      5. Prvky inteligentnej domácnosti
      6. Bezpečnostné komponenty domácnosti
      7. Telemedicínske zariadenia
   5. v. Dátové úložiská
      1. Externý disk
      2. USB
      3. Pamäťové karty
      4. Cloudové úložisko
5. **Softvér**, najmä
   1. Vlastníctvo
      1. SW dodávaný s počítačom
      2. Zakúpené licencie
      3. Open licencie
      4. Iné (napr. Freeware, Addware, Demo)
   2. Inštalovaný SW
      1. OS (MacOS, Windows, Linux, Android)
      2. Systémový SW
      3. Internetový prehliadač (najčastejšie Google Chrome)
      4. Kancelársky SW (najmä MS Office)
      5. AI aplikácie (napr. ChatGPT)
      6. Aplikačný SW (napr. pre prácu s grafikou)
      7. Bankové a platobné aplikácie
      8. Komunikačný SW
         1. MS Teams
         2. WhatsApp
         3. Telegram
         4. Discord
         5. Iné
      9. Bezpečnostný SW
         1. Antimalware
         2. Personálny FW
         3. IaM SW
         4. Rodičovský zámok
         5. Iné
      10. Sociálne siete
          1. Facebook
          2. Instagram
          3. Youtube
          4. TikTok
          5. Iné (X, Snapchat, Pinterest, Redit)
      11. Počítačové hry (klasifikácia [[20]](#footnote-20))
          1. Detské počítačové hry (predškolský vek)
          2. Didakticky orientované počítačové hry
          3. Arkády („plošinovky“)
          4. Dobrodružné hry (adventúry)
          5. Simulátory
          6. Preteky
          7. Športové hry
          8. Počítačová verzia klasických doskových hier
          9. Počítačová verzia kartových hier
          10. Príležitostné (casual) hry
          11. Hry na postreh
          12. Akčné hry
          13. Tajná (stealth) akcia
          14. Prežitý (survival) horor
          15. RPG (skratka z Role-Playing Game)
          16. On-line RPG – MMORPG (skratka z Massive Multiplayer On-line RPG“
          17. Strategické hry
          18. Strategické vojnové hry
          19. On-line hry
          20. Multižánrové hry
          21. Vizuálne novely
      12. Výukový a vzdelávací SW
          1. Pre podporu jednotlivých predmetov
          2. Prierezový (viac predmetov)
          3. Pre rozvoj konkrétnych schopností a zručností
      13. Prostredia pre tvorbu digitálneho obsahu, najmä
          1. Tvorba WWW stránok
          2. Tvorba videí
          3. Tvorba podcastov
          4. Úprava fotografií
          5. Herné prostredia (napr. Minecraft, Roblox)
      14. Prostredia pre vývoj a programovanie [[21]](#footnote-21) (IDE), napr.
          1. Pre Javu (IntelliJ IDEA, Eclipse, NetBeans)
          2. Pre Python (PyCharm, VS Code, Jupyter Notebook)
          3. Pre C/C++: (Visual Studio, CLion, Eclipse)
          4. Pre JavaScript: (VS Code, WebStorm, Sublime Text)
          5. Pre C#: (Visual Studio, VS Code)
6. **Údaje**, najmä
   1. Systémové údaje
      1. BIOS
      2. Rozširujúce karty
         1. Napr. ovládače pre grafickú kartu
      3. Pre OS
   2. Údaje pre aplikácie
      1. Systémové nastavenia (napr. Windows Registry)
      2. IaM nastavenia
      3. Vlastné adresáre
      4. Konfiguračné súbory
         1. Lokálne
         2. Na cloude
      5. Cookies
   3. Vlastné súbory vytvorené v aplikáciách (napr. samostatné práce, prezentácie)
      1. Na lokálnom disku
      2. Na serveri / cloude
   4. Klasifikované údaje, najmä
      1. Vlastné osobné údaje
         1. Osobitná kategória osobných údajov
      2. Osobné údaje iných osôb
      3. Predmet bankového tajomstva (napr. výpisy z účtov)
      4. Predmet telekomunikačného tajomstva (napr. prehľad hovorov)
      5. Iné klasifikované údaje (práca rodičov)
   5. Stiahnuté súbory, najmä
      1. S vysporiadanými autorskými právami
         1. Obrázky
         2. Videá
         3. Texty
         4. Iné
      2. Bez vysporiadaných autorských práv
         1. Obrázky
         2. Videá
         3. Texty
         4. Iné
      3. S obsahom porušujúcim legislatívu
         1. Detská pornografia
         2. Propagácia fašizmu
         3. Obsah podnecujúci k nenávisti
         4. Iné
   6. Údaje súvisiace s komunikáciou, najmä
      1. Maily
         1. Prílohy mailov
      2. SMS správy
      3. Chaty
      4. Nahraté hovory
      5. Nahraté videhovory
      6. Streamovaná komunikácia

*Súvisiace aktíva*

1. **Dostupná infraštruktúra, najmä** 
   1. Elektrická energia
   2. Dostupný mobilný signál
   3. Metalické pripojenie
   4. Optické pripojenie
2. **Zmluvy s dodávateľmi**, najmä
   1. Dodávatelia infraštruktúry
   2. Dodávatelia HW a SW (ak je záruka)
3. **Technická podpora**
   1. K  HW produktom
   2. K SW produktom
4. **Znalosti a schopnosti**
   1. Rodičia
      1. Všeobecné IKT znalosti
      2. Znalosti v oblasti rizík digitálneho priestoru
      3. Schopnosti implementovať bezpečnostné opatrenia
   2. Deti
      1. Všeobecné IKT znalosti
      2. Primerané znalosti v oblasti rizík digitálneho priestoru
      3. Schopnosti dodržiavať bezpečnostné opatrenia

### Aktíva mobilného IKT

Sú to aktíva, ktoré žiak so sebou prenáša (prenosné ako je tablet a notebook) alebo ich má stále pri sebe (mobil) alebo na sebe (wearables – napr. inteligentné hodinky).

Tieto aktíva sú používané aj v domácnosti a škole, ale naviac aj mimo týchto prostredí. Ich špecifikom je, že sa môžu pripájať k externým sieťam.

1. **Činnosti a agendy podporované mobilným IKT** 
   1. Telefonická hlasová komunikácia (telefonické hovory)
   2. Telefonická video komunikácia (video hovory)
   3. SMS komunikácia
   4. Dištančná výučba (typicky počas COVIDu, individuálny študijný plán)
   5. Čiastočná príprava do školy
   6. Všeobecné vzdelávanie / práca s informačnými zdrojmi
   7. Komunikácia so školou (typicky cez EduPage, uzavreté skupiny ako je Facebook, maily)
   8. Realizácia platobných operácií (ak má kompetenciu)
   9. Sociálne aktivity
      1. Chatovanie
      2. Mailová komunikácia
      3. Sociálne siete
   10. Voľnočasové digitálne aktivity (napr. počítačové hry)
2. **Mobil**
   1. Mobilné pripojenie
      1. Rýchlosť pripojenia
      2. Limity prenosu dát
      3. Rooming v zahraničí
      4. Nespotrebované prenosy dát (resp. limity)
   2. Hardvér
      1. Mobilné zariadenia
      2. Nabíjačka
   3. Softvér, najmä
      1. OS
      2. Systémový SW
      3. Internetový prehliadač (najčastejšie Google Chrome)
      4. Komunikačný SW
         1. WhatsApp
         2. Telegram
         3. MS Teams
         4. Discord
         5. Chat fóra on-line hier a iných aplikácií, ktoré nie sú primárne určené na komunikáciu
      5. Sociálne siete
         1. Facebook
         2. Instagram
         3. Youtube
         4. TikTok
         5. Iné
      6. Aplikačný SW
      7. Bankové a platobné aplikácie
      8. Bezpečnostný SW
      9. Počítačové hry
      10. Iné
   4. Údaje, najmä
      1. Kontakty
      2. Osobné údaje (napr. fotografie a videá)
         1. vlastné
         2. rodinných príslušníkov a známych
         3. iných osôb
      3. Obsah SMS správ
      4. Informácie o hovoroch
      5. Požiadavky na vyhľadávanie
      6. Cookies
      7. Stiahnuté súbory z webových sídiel
      8. Výsledky vlastnej práce
3. **Inteligentné hodinky**
   1. OS
   2. Softvér
      1. SW pre platby
      2. Komunikačný
      3. Zdravotný monitoring
      4. Iné
4. **Telemedicínske zariadenia**
   1. Hardvér
      1. Prístroje pre zdravotný monitoring
      2. Prístroje pre korekcie fyziologických parametrov
   2. Softvér
      1. Monitoring
      2. Vyhodnocovanie údajov
      3. Komunikácia s okolím

### IKT aktíva školy

Sú to aktíva, ktoré sa týkajú informačných a komunikačných systémov školy. Toto prostredie sa môže výrazne líšiť pre niektoré školy. V rámci digitalizácie školstva prebieha zjednocovanie školských prostredí, najmä z hľadiska vybavenia a pripojenia na internet.[[22]](#footnote-22) [[23]](#footnote-23)

1. **Činnosti a agendy podporované** IKT (primárne aktívum v zmysle MIRRI), najmä
   1. Žiak / Študent
      1. Výučba na hodinách
         1. IKT predmetov
         2. Ďalších predmetov s podporou IKT
      2. Dištančná výučba (typicky počas COVIDu, individuálny študijný plán)
      3. Práca na samostatných aktivitách, projektoch mimo vyučovania
      4. Elektronická komunikácia s učiteľmi
   2. Rodičia
      1. Elektronická komunikácia s učiteľmi
   3. Učitelia
      1. Výučba na hodinách
         1. IKT predmetov
         2. Ďalších predmetov s podporou IKT
      2. Príprava na výučbu
      3. Komunikácia
         1. so žiakmi (typicky EduPage)
         2. s rodičmi (typicky EduPage)
         3. s kolegami
         4. s vedením školy
         5. s príslušnými autoritami mimo školy
      4. Školské agendy
      5. Administratívne agendy
      6. Podpora pre žiakov pri práci na samostatných aktivitách, projektoch mimo vyučovania
   4. Vedenie školy
      1. Školské agendy
      2. Administratívne agendy relevantné pre chod školy
      3. Komunikácia
         1. so žiakmi (typicky EduPage)
         2. s rodičmi (typicky EduPage)
         3. s učiteľmi (typicky EduPage)
         4. s nadriadenými orgánmi
   5. Nepedagogickí zamestnanci
      1. Vyhodnocovanie dochádzky (z dochádzkového systému)
      2. Správa stravných lístkov a objednávania obedov
      3. Administratívne agendy
2. **Priestory**
   1. Objekt školy
   2. Miestnosti umiestnenia informačných aktív
      1. Serverovňa
      2. Počítačové učebne
      3. Miestnosti pre učiteľov a vedenie
      4. Spoločné administratívne priestory
   3. Vybavenie IKT pracovísk
      1. Stôl
      2. Stolička
      3. Vonkajšie osvetlenie
      4. Vnútorné osvetlenie
      5. Vhodné prostredie
         1. Vhodná teplota,
         2. Vhodná vlhkosť,
         3. Minimálna prašnosť
3. **Infraštruktúra a zariadenia** 
   1. Externá
      1. Prívod elektrickej energie
      2. Kabeláž (optika, metalická po školu)
   2. Interná
      1. Interné elektrické rozvody
      2. Interná štruktúrovaná kabeláž
   3. Sieťová
      1. Switche
      2. Routery
      3. Bezpečnostný sieťový HW (niekde)
         1. Firewall
         2. IDS / IPS
         3. SIEM
      4. Rádiový priestor (RF) a priestor pre iné typy bezdrôtových pripojení (IR)
      5. Samostatné zariadenia technológie IEEE 802.11
         1. Access point, ktorý nie je súčasťou WiFi routera.
         2. WiFi Repeater
         3. WiFi Mash systémy
      6. Technológie IEEE 802.15.1
4. **Hardvér**, najmä
   * 1. Servery (niektoré školy)
        1. Racky
        2. Diskové polia
        3. UPS
     2. Stolné počítače (v učebniach, kabinetoch, zborovni)
        1. Klávesnica
        2. Monitor
        3. Myš
        4. Prepojovacie káble
     3. Notebooky učiteľov a vedenia
     4. Tablety
     5. Ďalšie periférne zariadenia
        1. Tlačiarne
        2. Multifunkčné zariadenia
        3. Reproduktory
        4. Slúchadlá a mikrofón
        5. Kamery
        6. Iné
     6. Špecializovaný HW (napojený na Internet – niektoré školy)
        1. Inteligentné interaktívne tabule
        2. Zobrazovacie reklamné tabule
        3. Zariadenia dochádzkového a prístupového systému,
        4. Zariadenia stravovacieho systému
        5. Systémy inteligentnej budovy - vykurovanie, klimatizácie, vzduchotechnika.
     7. Dátové úložiská
        1. Externý disk
        2. USB
        3. Pamäťové karty
        4. Sieťové úložisko NAS
        5. Cloudové úložisko
5. **Softvér**, najmä
   1. Vlastníctvo
      1. SW dodávaný s počítačmi
      2. Zakúpené licencie alebo distribuované autoritami
      3. Open licencie
      4. Iné
   2. Inštalovaný
      1. OS (typicky MS Windows)
      2. Systémový SW
         1. SW pre riadenie siete a prostredia

DHCP

DNS

Active Directory,

* + - 1. programy mail servera (MTA,LDA,MDA,IMAP,POP3),
      2. WEB server
    1. SW pre chod školy
       1. Podpora vzdelávacieho procesu (napr. EduPage, ASC agenda)
       2. Personalistika a mzdy
       3. Správa majetku
       4. Dochádzkový systém
       5. Iné
    2. SW pre podporu výučby
       1. Aplikačný SW
       2. Špecializované aplikácie
    3. Internetový prehliadač (najčastejšie Google Chrome)
    4. Kancelársky SW (najmä MS Office)
    5. AI aplikácie (napr. ChatGPT)
    6. Bankové a platobné aplikácie
    7. Komunikačný SW
       1. MS Teams
       2. Emailový klient
       3. Iné
    8. Bezpečnostný SW
       1. Antimalware
       2. Personálny FW
       3. IaM SW
       4. Rodičovský zámok
       5. Iné
    9. Sociálne siete (na niektorých školách)
       1. Facebook
       2. Instagram
       3. Youtube
       4. TikTok
       5. Iné
    10. Počítačové hry (didaktické na ZŠ)
    11. Výukový a vzdelávací SW
        1. Pre podporu jednotlivých predmetov
        2. Prierezový (viac predmetov)
        3. Pre rozvoj konkrétnych schopností a zručností
    12. Prostredia pre tvorbu digitálneho obsahu (pre výučbu)
        1. Tvorba www stránok
        2. Tvorba videí
        3. Tvorba podcastov
        4. Úprava fotografií
        5. Herné prostredia (napr. pre záujmové krúžky na škole)
    13. Prostredia pre vývoj a programovanie (pre špecializovanú výučbu)
        1. Pre Javu
        2. Pre Python
        3. Pre C/C++
        4. Pre C#
        5. Pre JavaScript
        6. Pre PHP
  1. On-line verzie aplikácií spúšťané z prehliadača

1. **Údaje**, najmä
   * 1. Systémové údaje
        1. Dáta pre BIOS
        2. Dáta Rozširujúce karty
        3. Dáta pre OS
   1. Údaje potrebné pre aplikácie
      1. Systémové nastavenia
      2. IaM nastavenia a údaje
      3. Vlastné adresáre
      4. Konfiguračné súbory
         1. Lokálne
         2. Na serveri / cloude
      5. Cookies
   2. Súbory vytvárané používateľmi
      1. Žiakmi v rámci výučby
         1. Na lokálnom disku
         2. Na serveri / cloude
      2. Učiteľmi
         1. V rámci výučby a jej prípravy
         2. Mimo výučby
            1. Napr. v administratíve
      3. Vedením školy
   3. Klasifikované údaje, najmä
      1. Osobné údaje
         1. Osobné údaje žiakov a bývalých žiakov
            1. Osobitná kategória osobných údajov
         2. Osobné údaje rodičov
         3. Osobné údaje učiteľov a ostatných zamestnancov
            1. Osobitná kategória osobných údajov
         4. Osobné údaje iných osôb *(napr. pri prijímacích konaniach)*
      2. Predmet bankového tajomstva *(napr. výpisy z účtov školy)*
      3. Predmet telekomunikačného tajomstva *(napr. prehľad hovorov)*
      4. Iné klasifikované údaje
   4. Stiahnuté súbory *(žiakmi alebo učiteľmi)*
      1. S vysporiadanými autorskými právami
         1. Obrázky
         2. Videá
         3. Texty
         4. Iné
      2. S nevysporiadanými autorskými právami
         1. Obrázky
         2. Videá
         3. Texty
         4. Iné
      3. S obsahom porušujúcim legislatívu, napr. *(ako zlomyseľnosť žiakov, alebo škola má napadnutý zombie počítač)*
         1. detská pornografia
         2. propagácia fašizmu
         3. obsah podnecujúci k nenávisti
         4. iné
      4. Údaje súvisiace s komunikáciou
         1. Maily
            1. Prílohy mailov
         2. SMS správy vedenia a učiteľov
         3. SMS správy žiakov
         4. Chaty (žiaci, učitelia)
         5. Nahraté hovory
         6. Nahraté videhovory
         7. Streamované videá
         8. Video nahrávky na hodinách
2. **Dodávatelia**, najmä
   1. Elektrická energia
   2. Operátori pre internetové pripojenie
   3. Dodávatelia HW a SW
   4. Technická podpora pre HW a SW
3. **Finančné aktíva**, napr.
   1. Na bankových účtoch školy, dostupné cez Internet
   2. Platobné karty vedenia
   3. Financie na prevádzku IKT
4. **Zamestnanci**
   1. Kvalifikovaní učitelia IKT predmetov
   2. Nekvalifikovaní učitelia IKT predmetov
   3. Učitelia aktívne využívajúci IKT vo výučbe
   4. Nepedagogickí zamestnanci aktívne využívajúci IKT
   5. Nepedagogickí zamestnanci aktívne využívajúci IKT
   6. Vedenie školy podporujúce digitálne technológie
5. Znalosti a schopnosti
   1. Učitelia
      1. Všeobecné IKT znalosti
      2. Znalosti a schopnosti správneho využívania IKT v svojom predmete
      3. Znalosti v oblasti rizík digitálneho priestoru
      4. Schopnosti implementovať IKT bezpečnostné opatrenia
      5. Schopnosť zabezpečiť riadny chod hodiny bez narušení
      6. Schopnosť pozitívne vplývať na žiakov, motivovať ich k získaniu vedomostí a zručností
   2. Nepedagogickí zamestnanci
      1. Všeobecné IKT znalosti
      2. Znalosti a schopnosti využívať vecne príslušné aplikácie
      3. Znalosti v oblasti rizík digitálneho priestoru
      4. Schopnosti dodržiavať bezpečnostné opatrenia
   3. Žiaci
      1. Všeobecné IKT znalosti
         1. Získané na ZŠ
         2. Získané v škole
         3. Získané mimo školy
      2. Špecializované IKT znalosti a zručnosti
         1. Podľa zamerania IKT predmetov
   4. Rodičia
      1. Všeobecné IKT znalosti
      2. IKT znalosti v rozsahu predmetu vyučovania
      3. Podpora svojho dieťaťa v rámci výučby IKT
      4. Dobrá spolupráca s vyučujúcimi a vedením školy
      5. Podpora školy pre IKT technológie
      6. Schopnosť rešpektovať autoritu učiteľa
6. Dobré meno / reputácia
   1. Reputácia školy ako celku
   2. Reputácia vedenia
   3. Reputácia jednotlivých učiteľov
   4. Reputácia žiakov
   5. PR školy

## Aktíva dieťaťa ako fyzickej osoby

(vo vzťahu k hrozbám kybernetického priestoru)

Tieto aktíva môžu byť ohrozené aktivitami dieťaťa v kybernetickom priestore (napr. dlhodobé sedenie za počítačom a súvisiacim nedostatkom pohybu) a aktivitami, na ktoré vplýva kybernetický priestor (napr. zjesť čo najviac Panadolu ako výzva v TikToku, iniciácia fyzickej šikany)

Šikmým písmom sú uvedené príklady hrozieb k aktívam.

1. **Fyzické zdravie (ohrozené pri interakcii IKT)**
   1. Predispozície (v čase vstupu do sveta digitálnych technológií)
      1. Genotyp [[24]](#footnote-24)
      2. Epigenetické faktory[[25]](#footnote-25)
      3. Fenotyp [[26]](#footnote-26)
   2. Zmysly
      1. Zrak
         1. *Napr. oči namáhané pri využívaní obrazovky.*
      2. Sluch (
         1. *Napr. nadmerné počúvanie hudby nahlas.*
   3. Orgánové sústavy
      1. Oporná sústava
         1. Krk
            1. *Napr. pri fixácii pohľadu na monitor v nevhodnej výške.*
         2. Chrbtica
            1. *Napr. záťaž a poškodenie pri dlhodobom, nevhodnom sedení.*
      2. Pohybová sústava
         1. Zápästia
            1. *Syndróm karpálneho tunela, poškodenie pri dlhodobej práci s myšou alebo klávesnicou.*
         2. Svalstvo
            1. *Stuhnutie a skrátenie pri dlhodobom sedení za počítačom, mobilom bez pohybovej kompenzácie.*
            2. *Nedostatočný rozvoj svalstva bez adekvátneho pohybu.*
      3. Tráviaca sústava
         1. *Narušenie trávenia pri dlhodobom sedení bez pohybu.*
         2. *Nevhodná sprievodná strava pri aktivitách v digitálnom priestore.*
         3. *Vplyv stresu z digitálneho priestoru na tráviacu sústavu.*
      4. Vylučovacia sústava
         1. *Narušenia pri dlhodobom sedení bez pohybu.*
      5. Rozmnožovacia sústava
         1. *Narušená nezdravým životným štýlom, obezitou.*
      6. Endokrinná sústava
         1. *Narušená nezdravým životným štýlom.*
   4. Primeraná hmotnosť
      1. *Narušená nedostatkom pohybu, nadváha a obezita.*
   5. Fyzická kondícia (narušená nedostatkom pohybu)
      1. Obratnosť
      2. Rýchlosť
      3. Vytrvalosť
   6. Stravovací režim
      1. *Napr. jedenie počas hrania hier, nepravidelná strava.*
   7. Pitný režim
      1. *Zanedbanie alebo preháňanie pitného režimu.*
      2. *Pitie energetických nápojov pri hraní*
   8. Spánkový režim
      1. *Nedostatok spánku.*
      2. *Nekvalitný spánok.*
2. **Duševný stav a mentálne schopnosti ohrozené pri interakcii IKT**
   1. Duševná pohoda
      1. *Napr. narúšaná negatívnymi statusmi na sociálnych sieťach*
      2. *Narúšaná nedostatkom spánku*
   2. Schopnosť sústredenia
      1. *Napr. narúšaná prítomnosťou mobilu pri žiakovi na hodine*
      2. *Narúšaná nedostatkom spánku*
   3. Odolnosť voči záťaži a stresu
      1. *Hovorí sa o generácii "snehových vločiek".[[27]](#footnote-27)*
   4. Intelektuálne schopnosti
      1. *Napr. narúšané dlhodobou pasívnou konzumáciou krátkych videí na Tik-Toku*
   5. Emocionálna inteligencia
      1. *Nedostatočne rozvíjaná v dôsledku obmedzenia fyzických kontaktov.*
   6. Komunikačné schopnosti
      1. *Narúšané nedostatkom interakcií v reálnom svete*
      2. *Narúšané zjednodušenou komunikáciou v digitálnom prostredí*
   7. Vedomosti
      1. *Povrchnosť vo vedomostiach pri zahltení prázdnym informačným obsahom.*
      2. *Nedostatok času na získanie hlbších vedomostí v dôsledku nadmerného času s digitálnymi technológiami bez intelektuálneho prínosu.*
   8. IKT zručnosti
      1. *Napr. práca so súbormi, programovanie, vyhľadávanie, práca s kancelárskymi aplikáciami je obmedzená na úkor sociálnych sietí*
   9. Manuálne zručnosti
      1. *Narúšané nedostatkom primeraných aktivít v reálnom svete*
   10. Iné
3. **Sociálne aktíva**
   1. Dobré meno
   2. Reputácia
   3. Formálne postavenie v  reálnych aj virtuálnych kolektívoch
   4. Neformálne postavenie

*Líder resp. Alfa / Sigma alebo Beta / Looser (L), cieľ šikany*

* + 1. V škole
    2. Vo fyzických kolektívoch
    3. Vo virtuálnych komunitách

1. **Časový fond**

*Z ktorého si môžu nadmerne čerpať aktivity s digitálnymi technológiami*

* 1. Spánok

*Najčastejšie znižovaný časový rozsah*

* 1. Starostlivosť o telo
     1. Stravovanie

*Napr. narúšané sledovaním mobilu počas jedenia, nevhodná strava*

* + - 1. Raňajky
      2. Desiata
      3. Obed
      4. Olovrant
      5. Večera
    1. Pitný režim

*Nedostatok tekutín*

*Nadmerný príjem tekutín*

*Sladené nápoje*

* + 1. Osobná hygiena
    2. Pohybové aktivity
       1. Turistika
       2. Šport
       3. Fyzická práca
  1. Škola
     1. Čas dopravy do školy a späť
     2. Pobyt v škole
     3. Domáca príprava na hodiny
     4. Samostatné domáce aktivity (napr. projekty, odborné práce)
     5. Odborná prax
  2. Voľnočasové aktivity
     1. Kultúra (kino, divadlo, koncerty)
     2. Fyzický kontakt a aktivity s rovesníkmi
     3. Záujmové krúžky
     4. Digitálne aktivity
        1. Samostatné
        2. V kolektíve

## Aktíva rodičov vo vzťahu k dieťaťu a kybernetickému priestoru

1. IKT schopnosti a znalosti rodičov
   1. IKT zručnosti (napr. práca so súbormi, programovanie, vyhľadávanie, práca s kancelárskymi aplikáciami, sociálne siete)
   2. Vedomosti, povedomie o rizikách v KP
2. Čas venovaný dieťaťu (vo vzťahu IKT a KB)
   * 1. Na školské záležitosti,
     2. Na jeho celkový rozvoj, vrátane
        1. Na rozvoj IKT schopností dieťaťa
        2. Na oboznámenie dieťaťa s rizikami v KP
        3. Na monitoring aktivít dieťaťa v KP
3. Psychosociálne danosti a schopnosti
   1. Dôslednosť
      1. Pri rozhodnutí o akceptácii odporúčaného veku dieťaťa pre aktivity v KP (napr. kedy dostane mobil, účet na sociálnej sieti)
      2. Pri nastavení a dodržiavaní časových limitov používania IKT (v súlade s odporúčaniami odborníkov)
      3. Pri prípadných zákazoch niektorých aktivít
   2. Empatia
      1. Schopnosť rozpoznať problémy dieťaťa (napr. kyberšikanu)
   3. Osobný príklad
      1. V správnom spôsobe a miere využívania IKT
      2. V postoji k rizikám celkovo a osobitne v KB

## Finančné aktíva

**Rodina**

1. Na bankových účtoch, dostupné cez Internet
   * 1. Žiak
     2. Rodičia
     3. Súrodenci
2. V aplikáciách s platbami (ako kredity)
3. Platobné karty s kreditom
4. Kredity v hrách a aplikáciách.
5. Financie na prevádzku IKT (internetu, mobilov, dátových prenosov s limitmi)
6. Príjmy rodiny
7. Celkové disponibilné finančné aktíva rodiny

**Školstvo (ZŠ, SŠ)**

(vo vzťahu k kybernetickým hrozbám, ktoré súvisia so vzdelávacím procesom)

1. Celkové náklady na IKT školy
2. Celkové náklady na IKT všetkých škôl
3. Celkové náklady na chod školy (v zmysle normatívu)
4. Celkové náklady na chod všetkých škôl
5. Rozpočtová kapitola rezortu [[28]](#footnote-28) (**5.359 mil. €)**
   1. Národný program výchovy, vzdelávania a mládeže **(3850 mil. €)**
   2. Dotácia na prenesený výkon pôsobnosti štátnej správy na obce - regionálne školstvo (**2.240 mil. €)**

## Aktíva populácie mládeže ako celku

(vo vzťahu k hrozbám súvisiacim s kybernetickým priestorom a jeho digitálnym obsahom)

1. **Populačné ročníky detí** 
   1. Úroveň zdravotného stavu daného populačného ročníka (cca. 45 - 50.000 osôb)
      1. Fyzický
      2. Duševný
   2. Vedomostná úroveň daného populačného ročníka (napr. podľa PISA testov)
   3. Sociálne schopnosti a zručnosti vo fyzickom svete
   4. Sociálne schopnosti a zručnosti v KP
   5. Záujem o samovzdelávanie (kurzy, krúžky)
   6. Záujem o VŠ štúdium
   7. Ochota ostať na Slovensku po ukončení štúdia
2. **Aktíva po prechode do dospelosti podmienené detstvom** (pracujúci vstupujúci na pracovný trh)
   1. Úroveň zdravotného stavu
   2. Vedomostná úroveň
   3. Pracovné schopnosti, návyky a zručnosti (očakávané praxou)
   4. Sociálne schopnosti a zručnosti vo fyzickom svete
   5. Sociálne schopnosti a zručnosti v KP
   6. Ochota ostať pracovať na Slovensku

## Aktíva štátu ako celku

(v priamom alebo nepriamom vzťahu k hrozbám súvisiacim s mládežou a kybernetickým priestorom, interakciami v ňom a jeho digitálnym obsahom)

1. Počet pracujúcich vstupujúcich na pracovný trh v SR
2. Úroveň kvalifikácie pracovnej sily vstupujúcej na pracovný trh
3. Portfólio pracovnej sily vstupujúcej na pracovný trh
4. Konkurencieschopnosť štátu ako celku
5. Sociálna súdržnosť spoločnosti / spoločné hodnoty spoločnosti
6. Úroveň pripravenosti na obranu štátu a vôľa brániť štát
7. Demografia
   1. Preferencie pre založenie rodiny / preferencie mať deti
   2. Schopnosť počatia a donosenia plodu
   3. Počet detí na ženu v plodnom veku

# Hrozby a zraniteľnosti, dopady a riziká

## Domáce IKT prostredie

Výber hrozieb a zraniteľností je z Katalógov hrozieb NBÚ a MIRRI. Špecifikácia aktív domáceho IKT prostredia je uvedená v kap. 3.1. ID je podľa Katalógu hrozieb MIRRI.

### Hrozby

|  |  |  |
| --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Príklady spôsobu realizácie a primárny dopad** |
| **H1** | **Fyzické hrozby** | |
| 1.1 | Požiar | Požiar v dome, bloku alebo byte - po skrate elektrospotrebiča, zásahu blesku, pri opravách objektu, chybnej manipulácii s horľavinami, úmyselnom založení - vedie k poškodeniu priestoru a IKT |
| 1.2 | Prach, korózia, mrazy | Prašné okolie, nadmerná vlhkosť v domácnosti, priestoroch IKT, výpadok kúrenia v zime - môže viesť k poškodeniu hardvéru a pamäťových médií. |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie | Veľká nehoda v okolí ako je požiar vedľajšej budovy, chemické znečistenie okolia, výbuch v blízkosti, závažná dopravná nehoda, letecká nehoda – môže viesť k dočasnej nedostupnosti obydlia a poškodeniu IKT aktív. |
| 1.4 | Voda | Prienik vody do obydlia - záplavou, vytopením, vodoinštalačnou haváriou – môže viesť k nedostupnosti obydlia, jeho poškodenia ako aj jeho vnútorného vybavenia vrátane IKT. |
| 1.5 | Výbuch | Výbuch v objekte v dôsledku výbuchu plynu alebo – môže to viesť k nedostupnosti obydlia, jeho poškodeniu vrátane IKT. |
| 1.6 | Znečistenie, škodlivé žiarenie | Znečistenie IKT (napr. olejom, sadzami, chemikáliami, farbou) v blízkosti IKT vedie k ich poškodeniu alebo výpadku |
| 1.7 | Zničenie zariadenia, alebo médií | Zničenie zariadení alebo médií napr. nesprávnym zaobchádzaním, pádom (pri prenose, upratovaní, hraní sa) či technickou chybou. |
| **H2** | **Hospodárske a ekonomické hrozby** | |
| 2.1 | Chýbajúce zdroje v domácom rozpočte | Chýbajúce zdroje na opravu alebo obnovu IKT alebo prevádzku (napr. antimalware SW na ďalší rok) – môže znamenať obmedzenie využívania IKT alebo jeho časti, alebo zvýšenie miery rizika. |
| 2.2 | Nevýhodná zmluva s dodávateľom | Výhradnosť dodávateľa (tzv. vendor-lock), vyššie ceny ako sú bežné, vysoké sankcie v prípade odstúpenia. Dodávateľ je najčastejšie pre internetové pripojenie, mobilný operátor, pre priebežne aktualizovaný SW (napr. Office 365). |
| **H3** | **Informačné operácie** | |
| 3.1 | Šírenie propagandy | Úmyselné šírenie propagandy za účelom ovplyvňovania svojho virtuálneho okolia – mailom, v elektronických médiách a sociálnych sieťach z domáceho prostredia. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť. |
| 3.2 | Vytvorenie dezinformácií | Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky svojho virtuálneho okolia mailom, v elektronických médiách a sociálnych sieťach z domáceho prostredia. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť. |
| 3.3 | Zdieľanie dezinformácií | Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky svojho virtuálneho okolia mailom, v elektronických médiách a sociálnych sieťach z domáceho prostredia. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť. |
| **H4** | **Kompromitácia funkcií alebo služieb** | |
| 4.1 | Chyba pri používaní | Nechcená modifikácia údajov v cudzích súboroch či databázach (napr. dieťa rodičom), zmazanie systémových súborov, zmazanie pracovných súborov potrebných pre chod softvéru. |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | Nesprávna konfigurácia sieťového zariadenia (napr. pri amatérskych pokusoch o konfiguráciu). |
| 4.3 | Falšovanie práv alebo povolení | Neoprávnené pozmeňovanie identít a prístupových práv do systémov u iných členov rodiny. |
| 4.4 | Odmietnutie konania | Odmietnutie vykonania napr. pri žiadosti o plnenie servisnej podpory. |
| 4.5 | Odmietnutie služby | Narušenie za účelom znefunkčnenia služby - typicky DoS, DDoS útok na infraštruktúru poskytovateľa pripojenia, alebo aj priamo na domáce IKT. Môže sa jednať aj o napadnutie malvérom. |
| 4.6 | Zhoršovanie stavu pamäťových médií | Starnutie archivovaných dokumentov na médiách (zvyčajne USB) zničenie médií napr. pri požiari, vytopení a pod. |
| 4.7 | Zneužitie práv alebo povolení | Neoprávnené získanie identít a prístupových práv do systémov a ich zneužitie na konanie v mene iného používateľa z rodiny (napr. za účelom platby). |
| **H5** | **Ľudské konanie** | |
| 5.1 | Popretie | Stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje zlomyseľnú manipuláciu alebo sfalšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfalšovanie identifikácie nepovolených aktivít. V domácnosti to môže byť oblasť sťahovania detskej pornografie. |
| 5.2 | Detekcia polohy | Zistenie údajov o geografickej polohe člena rodiny. |
| 5.3 | Infiltrácia webovej komunikácie | Poškodenie, alebo neoprávnená zmena obsahu, typicky webovej stránky (rodinnnej alebo cudzej), alebo aplikácie, ktoré môže zmeniť informačný obsah, alebo aj vizuálny vzhľad webovej stránky, alebo aplikácie (tzv. defacement). Hrozba prieniku do domáceho systému prostredníctvom webových aplikácií. |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | Krádež identity a jej zneužitie na podvodné konanie alebo neoprávnený prístup (dieťaťa, rodiča, identity rodiča dieťaťom). |
| 5.5 | Krádež médií alebo dokumentov | Krádež dokumentov, PC so súbormi, pamäťových médií pri vykradnutí obydlia. |
| 5.6 | Krádež zariadenia | Krádež počítača, notebooku, mobilu, pamäťového zariadenia pri vykradnutí obydlia, auta alebo lúpeži. |
| 5.7 | Manipulácia s hardvérom | Amatérska manipulácia s hardvérom, pridanie nekompatibilnej časti zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, odstránenie komponentov zariadenia, pripojenie zariadení (napr. USB diskov) pre štart OS alebo získanie dát, použitie USB kľúčov z neznámych zdrojov. |
| 5.8 | Manipulácia so softvérom | Amatérska manipulácia so softvérom, neschválené aktualizácie, zmeny konfigurácie, odmazanie systémových súborov atď. |
| 5.9 | Neoprávnené používanie zariadení | Neoprávnený alebo neautorizovaný prístup do systému alebo k zariadeniu, znižovanie zabezpečenia zariadení a služieb (napr. k počítaču rodičov, keď nie sú doma). |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Neoprávnené poskytnutie, sprístupnenie alebo zverejnenie osobných údajov o iných osobách. |
| 5.11 | Neoprávnený vstup do priestorov | Neoprávnený fyzický vstup do priestorov, napr. kamaráti dieťaťa na domáce pracovisko rodičov. |
| 5.12 | Nesprávne používanie zariadení | Porušenie politík alebo návodov na bezpečné používanie zariadenia (nechce sa čítať návod k použitiu). |
| 5.13 | Nezákonné spracovanie údajov | Neoprávnená manipulácia s informáciami (napr. na zdieľanom počítači s pracovnými údajmi rodičov). |
| 5.14 | Odosielanie alebo distribúcia malvéru | Infiltrácia škodlivým kódom, PC sa stane zombie PC, cez ktoré sa ďalej rozosiela malvér, alebo malvér sa zasiela ďalej mailami a interakciami v sociálnych sieťach. |
| 5.15 | Odpočúvanie | Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky (napr. kamaráti na PC rodičov). |
| 5.16 | Podvodné kopírovanie softvéru | Neoprávnená manipulácia so softvérom vedúca k nepovolenému/neschválenému kopírovaniu a prípadne aj ďalšiemu šíreniu (napr. dieťa samostatne inštalujúce SW bez licencie) |
| 5.17 | Poškodenie reputácie | Poškodenie reputácie inej osoby úmyselným konaním cez IKT (klebety, ohováranie, dezinformácie, dehonestácia, poškodzovanie dobrého mena atď.) najmä využitím sociálnych sietí, chatu, mailu, SMS |
| 5.18 | Poškodenie údajov | Zmena, alebo zničenie údajov, zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia autora, manipulácia alebo zmena s informáciou, ktorá znamená narušenie jej integrity (napr. dieťa na rodičovskom PC). |
| 5.19 | Poškodenie zariadení alebo médií | Úmyselné poškodenie zariadení, alebo médií, narušenie integrity zariadenia alebo média (napr. zlomyseľní kamaráti). |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Použitie nelegálneho, falošného alebo nelicencovaného softvéru dieťaťom alebo jeho rodičom. |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | Napr. ak sa dá dieťa na hackerskú dráhu. Skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď. |
| 5.22 | Prístup neoprávneného používateľa k sieti | Zneužitie prístupových práv alebo úspešný externý hack do siete. |
| 5.23 | Sociálne inžinierstvo | Dieťa ako obeť - ovplyvňovanie (phishing, sociálne inžinierstvo, podplácanie, a pod.), nátlak (výhražné emaily, psychologické obťažovanie) atď. |
| 5.24 | Teroristický útok, sabotáž | Úmyselná manipulácia alebo poškodenie fyzických objektov, zariadení a/alebo procesov alebo obmedzenie funkcií z dôvodu sabotáže za účelom spôsobenia škody - napr. útok vedený voči rodičom s dôležitým postavením. |
| 5.25 | Útok man-in-the-middle | Typ hrozby počas ktorej útočník prenikne do komunikácie medzi dieťaťom a ďalšími účastníkmi a bez ich vedomia začne komunikáciu neoprávnene modifikovať. |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | Pri samostatnej práci dieťaťa. |
| 5.27 | Vzdialené špehovanie | Hackerské špehovanie sieťovej prevádzky domácej siete, získavanie dát posielaných cez rádiofrekvenčné siete, maskovanie identity, sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu, atď – napr. kvôli dôležitej práci rodičov. |
| 5.28 | Zachytenie žiarenia zariadenia | Sledovanie GPS signálu zariadenia, vzdialená detekcia elektromagnetického vyžarovania zariadenia, vrátane analýzy dátovej prevádzky atď. – pri špeciálnych útokoch voči citlivej práci rodičov. |
| 5.29 | Zber recyklovaných alebo vyradených médií | Odovzdanie médií s osobnými údajmi na skartáciu, recykláciu. |
| 5.30 | Zverejňovanie informácií | Neoprávnené zverejnenie informácií osobám, ktoré k nim nemajú mať prístup – napr. o rodičoch a ich práci, o sebe sexuálnemu predátorovi. |
| **H8** | **Organizačné hrozby** | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | Zanedbanie bezpečnostných požiadaviek pri plánovaní, nákupe a implementácii HW a SW v domácnosti (napr. opomenie sa anti-malware SW). |
| 8.2 | Nedostatok personálu | Nedostatok personálnych kapacít rodičov na vytvorenie bezpečného IKT prostredia pre dieťa. |
| 8.3 | Nedostatok zdrojov | Nedostatok finančných zdrojov pre bezpečné IKT prostredie dieťaťa. |
| 8.4 | Porušenie interných domácich pravidiel | Porušenie domácich pravidiel vedúce k bezpečnostnej udalosti alebo zvýšeniu rizika. |
| 8.5 | Porušenie zákonov alebo nariadení | Porušenie zákona pri činnosti v KP vyúsťujúce do trestno-právnej, správno-právnej alebo inej právnej konzekvencie |
| 8.6 | Zlyhanie poskytovateľov služieb | Prerušenie outsourcovaných služieb, napr. dodávky elektrickej energie, telekomunikačných služieb, narúšajúce prácu s IKT*.* |
| **H9** | **Poruchy infraštruktúry** | |
| 9.1 | Elektromagnetické žiarenie | Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením alebo magnetom, |
| 9.2 | Elektromagnetické impulzy | Poškodenie údajov (typicky na nosičoch) alebo HW elektromagnetickými impulzmi, resp. kolísaním napájania v domácej sieti |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | Porucha ventilácie PC, ktorá môže spôsobiť jeho výpadok. |
| 9.4 | Porucha napájacieho systému | Narušenie alebo poškodenie energetickej infraštruktúry v rámci domácnosti. |
| 9.5 | Porucha telekomunikačného zariadenia alebo služby | Zlyhanie telekomunikačných komponentov, prerušenie kabeláže, slabý telekomunikačný signál, nedostatočný signál Wi-Fi, atď. |
| 9.6 | Porucha telekomunikačnej siete | Poškodenie telekomunikačného spojenia, zničenie kabeláže, výpadok komponentov optického spojenia, nedostupné WiFi pripojenie, atď. |
| 9.7 | Strata napájania | Obmedzená alebo zastavená dodávka energie. |
| 9.8 | Tepelné žiarenie | Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou v miestnosti. |
| **H10** | **Prírodné hrozby** | |
| 10.1 | Klimatický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) alebo obmedzenie funkcií z dôvodu klimatického javu – víchrica, ktorá narušila domácnosť, záplava, lesný požiar v okolí. |
| 10.2 | Meteorologický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) mrazom, vysokou teplotou, vetrom, vlhkosťou, bleskom (napr. v domácnosti počas dovolenky). |
| 10.3 | Pandémia/epidemický jav | Rozsiahla epidémia, nemoc, ktorá sa rozširuje na geograficky rozsiahlom území, ktorá má dopad aj na IKT prevádzku. |
| 10.4 | Poškodenie zvieraťom | *Poškodenie (typicky nosičov údajov, alebo IKT zariadení) zvieratami – domáce (pes, mačka) alebo divými (myš, potkan, hmyz).* |
| 10.5 | Povodeň | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) povodňou, ktorá zasiahla obydlie |
| 10.6 | Seizmický jav | Poškodenie (typicky priestorov, nosičov údajov, alebo IT zariadení) zemetrasením, alebo inými seizmickými udalosťami. |
| **H.12** | **Súkromie** | |
| 12.6 | Neznalosť obsahu | Neznalosť obsahu je hrozba, ktorá indikuje, že používateľ (dieťa) si neuvedomuje obsah informácie spracovanej v systéme a následne napr. zverejňuje nadbytočné informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo používateľ poskytuje informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie (napr. nechcené prezradenie informácií) |
| 12.7 | Neoprávnené sprístupnenie | Neoprávnené sprístupnenie osobných údajov v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup. (Neoprávnené prečítanie, kopírovanie, fotografovanie, použite odpočúvacích zariadení na stretnutiach, atď.) |
| **H13** | **Technické poruchy** | |
| 13.1 | Porucha softvéru | Chyby počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď. |
| 13.2 | Porucha zariadenia alebo systému | Náhle a neplánované zlyhanie alebo porucha IKT zariadenia, alebo akéhokoľvek HW komponentu. |
| 13.3 | Strata napájania alebo kolísanie výkonu | Strata zdroja napájania alebo kolísanie výkonu napájania zariadení. |
| 13.4 | Zahltenie informačného systému | Plná úložná jednotka, preťaženie systému, reakcia na prehriatie spomalením procesora, nedostatok operačnej pamäte, slabý procesor, slabá grafická karta. |
| 13.5 | Zníženie úrovne údržby, chyba údržby informačného systému | Chyba údržby informačného systému, alebo IT zariadení (amatérske zásahy). |
| **H15** | **Verejný poriadok** | |
| 15.1 | Destabilizácia | Destabilizácia a narušenie chodu orgánov verejnej moci napr. v dôsledku masívneho hackerského útoku (zombie počítačom v útoku môže byť aj domáci počítač). |
| 15.2 | Poškodenie zdravia obyvateľstva | Poškodenie zdravia významnej časti obyvateľov v dôsledku vplyvu a dlhodobého pôsobenia digitálnych technológií (závislosti, civilizačné choroby) |
| 15.3 | Verejné nepokoje | Verejné nepokoje a protesty, vedúce k narušeniu verejného poriadku na území okresu, kraja, štátu v dôsledku pôsobenia KP na členov rodiny – hoaxy, šírenie poplašnej správy, panika, podnecovanie k nenávisti a pod. |

**Najčastejšie hrozby v domácom IKT prostredí**

Číslovanie neodráža poradie miery súvisiaceho rizika, slúži na referenčné účely.

1. Porušovanie autorských práv (SW, digitálny obsah)
2. Vstup údajov z nedôveryhodných zdrojov
3. Strata údajov (bez existencie adekvátnej zálohy)
4. Napadnutie počítača malvérom
5. Strata USB so súbormi
6. Porucha zariadenia alebo systému
7. Pôsobenie dezinformácií
8. Chyby pri používaní aplikácií
9. Poškodenie reputácie inej osoby úmyselným konaním v KP
10. Dieťa ako obeť sociálneho inžinierstva s následnými dopadmi (napr. sexting)

### Zraniteľnosti

V Katalógu zraniteľností s ohľadom na domáce IKT prostredie vychádzame z Katalógu MIRRI v členení oblastí, ale ID je vlastné. Uvádzame generické, najčastejšie zraniteľnosti. V rámci komunít a rodiny môžu byť aj ďalšie zraniteľnosti.

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Zraniteľnosť** |
| **1. Hardvér** | 1.1 | Amatérske zásahy do HW (deti, rodičia) |
| 1.2 | Nedostatočná údržba HW v domácich podmienkach. |
| 1.3 | Prach v okolí (narúša činnosť ventilátora). |
| 1.4 | Nevhodné podmienky umiestenia (napr. možnosť zakopnutia o káble). |
| 1.5 | Napäťová nestabilita. |
| 1.6 | Pamäťové média nie sú uložené vo vhodnom priestore. |
| **2. Softvér** | 2.1 | SW stiahnutý a inštalovaný z neautorizovaných zdrojov. |
| 2.2 | Nejasné plnenie licenčných podmienok používaného SW. |
| 2.3 | Neaktualizovaný SW. |
| 2.4 | SW aktualizovaný z neautorizovaných zdrojov. |
| 2.5 | Ukončená technická podpora pre danú verziu SW. |
| 2.6 | Zraniteľnosti identifikované v SW. |
| 2.7 | Nevhodné prístupové heslá. |
| 2.8 | Nesprávna konfigurácia SW (napr. možnosť vzdialeného prístupu) |
| 2.9 | Nevhodné riadenie prístupových práv k SW (napr. možnosť dieťaťa dostať sa k súborom rodičov). |
| 2.10 | Komplikované užívateľské rozhranie. |
| 2.11 | SW v angličtine používaný dieťaťom so slabou znalosťou EN. |
| 2.12 | Chýbajúce vekovo prístupné návody k používaniu SW |
| **3. Sieť** | 3.1 | Nechránené verejné sieťové pripojenie |
|  | 3.2 | Slabé heslo na internú wifi sieť |
|  | 3.3 | Nepostačujúce zabezpečenie internej siete |
|  | 3.4 | Sprístupnenie siete iným osobám (napr. známym na návšteve). |
|  | 3.5 | Prevádzka zastaralých komponentov siete (router, AP, Bluetooth), ktoré obsahujú prelomené ochranné prvky |
| **4. Používatelia** | 4.1 | Nezaškolení používatelia (deti, rodičia) |
|  | 4.2 | Nesprávne postupy pri práci s HW a SW |
|  | 4.3 | Podceňovanie KB |
| **5. Lokalita** | 5.1 | Nedostatočná fyzická ochrana obydlia |
|  | 5.2 | Záplavová oblasť |
|  | 5.3 | Horľaviny v obydlí |
| **8. Org. prostredie** | 6.1 | Nebola vykonaná vysoko-úrovňová analýza rizík (na úrovni, ktorú zvládne aj rodič) |
|  | 6.2 | Chýba plán kontinuity činností (ak príde používateľ o údaje). |
|  | 6.3 | Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládnu aj rodičia). |
|  | 6.4 | Chýbajú interné postupy pre prácu s IKT (na úrovni, ktorej vypracovanie zvládnu aj rodičia. |

**Najčastejšie zraniteľnosti v domácom IKT prostredí**

Číslovanie neodráža poradie miery vplyvu zraniteľnosti, slúži na referenčné účely.

1. Nevhodné prístupové heslá.
2. Neaktualizovaný SW (napr. OS).
3. SW stiahnutý a inštalovaný z neautorizovaných zdrojov.
4. Nesprávna konfigurácia SW (napr. možnosť vzdialeného prístupu)
5. Nezaškolení používatelia (deti, rodičia)
6. Nesprávne postupy pri práci s HW a SW.
7. Podceňovanie KB.
8. Chýba plán kontinuity činností (ak príde dieťa alebo rodič o údaje).
9. Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládnu aj rodičia).
10. Chýbajú interné postupy pre prácu s IKT (na úrovni, ktorej vypracovanie zvládnu aj rodičia).

### Možné dopady / následky

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Následky** |
| **1. Priestory / objekt** |  | **Primárne následky pre priestory** |
| 1.1 | Strata objektu / obydlia vrátane vnútorného vybavenia a IKT aktív ((napr. po silnom požiari, výbuchu) |
| 1.2 | Poškodenie objektu vrátane vnútorného vybavenia a IKT aktív ((napr. po menšom požiari alebo výbuchu). |
| 1.3 | Poškodenie objektu, ale nie IKT aktív (napr. po vytopení) |
|  | ***Sekundárne následky súvisiace s priestormi*** |
|  | Dlhodobá nedostupnosť objektu (napr. po narušení jeho statiky). |
| 1.4 | Dočasná nedostupnosť objektu v dôsledku jeho obnovy. |
| 1.5 | Dočasná neprístupnosť objektu (objekt uzavretý políciou) |
| **2. Hardvér** |  | ***Primárne následky pre HW*** |
| 2.1 | Poškodenie HW (napr. pri spadnutí na zem, pri sérii výpadkov prúdu). |
| 2.2 | Dočasná strata HW (napr. ukradnutý notebook, ktorý sa nájde, dočasné zabavenie políciou). |
| 2.3 | Trvalá strata HW (napr. ukradnutý notebook či mobil, ktorý sa nenájde, HW po požiari alebo zásahu blesku, vytopení). |
| 2.4 | Dočasná neprístupnosť HW (napr. notebook zabudnutý v práci) |
| 2.5 | Dočasná nedostupnosť HW (napr. polícia v rámci šetrenia ho zhabala). |
| 2.6 | Dočasná výpadok prevádzkyschopnosti HW (vypadlo napájanie). |
|  | ***Sekundárne následky súvisiace s HW*** |
| 2.7 | Dočasná nedostupnosť HW kvôli obnove (napr. je v oprave alebo čaká na opravu). |
| 2.8 | Čas spotrebovaný na obnovu HW časti IKT. |
| 2.9 | Finančné náklady na opravu HW. |
| 2.10 | Finančné náklady na kúpu nového HW (ak je poškodený HW nepoužiteľný alebo je ukradnutý a nie je poistený). |
| **3. Softvér** |  | ***Primárne následky pre SW*** |
| 3.1 | Nedostupnosť použitia SW (kvôli narušenej dostupnosti alebo funkcionalite HW). |
| 3.2 | Narušenie funkcionality OS. |
| 3.3 | Nedostupnosť SW kvôli nefunkčnosti OS. |
| 3.4 | Strata nainštalovaného SW (napr. omylom vymazanie súborov, alebo výsledok činnosti malvéru) |
| 3.5 | Nefunkčnosť SW po jeho narušení (napr. pri amatérskom vymazaní niektorých jeho systémových súborov alebo zásahu do nich) |
| 3.6 | Nesprávna činnosť SW po jeho narušení (napr. malvérom, bugom). |
| 3.7 | Poškodenie SW (súborov). |
| 3.8 | Strata licencie pre porušenie podmienok. |
|  | ***Sekundárne následky súvisiace so SW*** |
| 3.9 | Dočasná nedostupnosť SW kvôli obnove (napr. celé PC je v oprave alebo čaká na opravu, reinštaláciu). |
| 3.10 | Čas spotrebovaný na obnovu SW časti IKT. |
| 3.11 | Finančné náklady na obnovu SW (napr. ak to robí servis). |
| 3.12 | Porušovanie autorského práva po ukončení licenčnej zmluvy. |
| **4. Údaje** | 4.1 | Trvalá strata údajov (od poslednej zálohy, alebo aj všetkých – ak nie je záloha). |
| 4.2 | Čas potrebný na obnovu údajov mimo záloh alebo opätovné vykonanie stratenej práce. |
| 4.3 | Poškodenie údajov, narušenie ich integrity |
| 4.4 | Dočasná nedostupnosť údajov. |
| 4.5 | Údaje sú aktuálne nepoužiteľné kvôli nefunkčnému HW / SW. |
| 4.6 | Dopady vyplývajúce z narušenia dôvernosti údajov (najmä osobitnej kategórie). |
| **5. Služby domáceho IKT** | 5.1 | Obmedzenie komunikácie so školou zo strany rodičov. |
| 5.2 | Nemožnosť realizovať internetové platobné operácie. |
| 5.3 | Obmedzenie získavanie informácií o dianí. |
| 5.4 | Obmedzenie virtuálnych sociálnych aktivít. |
| 5.5 | Obmedzenie virtuálnych voľnočasových aktivít. |
| **6. Školské aktivity** | 6.1 | Nesplnenie termínovanej úlohy (napr. seminárnej práce). |
| 6.2 | Meškanie v preberanom učive (ak je závislé na IKT alebo žiak má individuálny plán). |
| 6.3 | Nedostupnosť informačných zdrojov pre samostatnú prácu. |
| 6.4 | Nemožnosť realizovať vzdialený prístup v dištančnom vzdelávaní. |
| 6.5 | Nemožnosť komunikovať školské záležitosti s inými žiakmi. |
| 6.6 | Strata motivácie k školským aktivitám, rezignácia |
| **7. Psychosociálne dopady** | 7.1 | Dlhodobá frustrácia spôsobená vplyvom sociálnych sietí. |
| 7.2 | Narušený psychosociálny vývoj. |
| 7.3 | Negatívne vplyvy nadmerného využívania digitálnych technológií. |
| 7.4 | Negatívne vplyvy nelátkových závislostí. |
| 7.5 | Iné, viď kap. 2.4 |
| **8. Finančné dopady** | 8.1 | Náklady na nový mobilný telefón. |
| 8.2 | Náklady na herný HW a SW. |
| 8.3 | Náklady na nové zariadenie (pokazený / málo výkonný) na úrovni očakávanej komunitou (napr. nový iPhone). |
| 8.4 | Náklady na predmety do hier. |
| 8.5 | Náklady na stávkovanie / gambling. |
| 8.6 | Strata financií v dôsledku podvodu / fraudu. |
| 8.7 | Náklady na prekročené dátové limity (napr. pri sťahovaní videí v zahraničí) |
| 8.8 | Iné náklady |

**Najčastejšie dopady v domácom IKT prostredí**

Číslovanie neodráža poradie miery dopadu, slúži na referenčné účely.

1. Náklady na nový mobil.
2. Náklady na herný HW a SW:
3. Čas potrebný na obnovu údajov mimo záloh alebo opätovnú prípravu stratenej práce.
4. Nedostupnosť IKT prostredia kvôli jeho narušeniu.
5. Dlhodobá frustrácia spôsobená vplyvom sociálnych sietí.
6. Narušený psychosociálny vývoj.
7. Negatívne vplyvy nelátkových závislostí.
8. Nedostatok pohybu.
9. Nesprávne držanie tela, narušenie správneho vývoja chrbtice.
10. Nedostatok spánku.

### Analýza rizík

**Miera rizika v nasledujúcej tabuľke je posúdená pre typickú domácnosť bez primeraných bezpečnostných opatrení.** Vhodnými opatreniami dochádza k zníženiu miery rizika.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| **H1** | **Fyzické hrozby** | | | |
| 1.1 | Požiar | K | N | **S** |
| 1.2 | Prach, korózia, mrazy | M | VN | N |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie | Z | VN | N |
| 1.4 | Voda | Z | VN | N |
| 1.5 | Výbuch | Z | VN | N |
| 1.6 | Znečistenie, škodlivé žiarenie | S | VN | N |
| 1.7 | Zničenie zariadenia, alebo médií | S | N | **S** |
| **H2** | **Hospodárske a ekonomické hrozby** | | | |
| 2.1 | Chýbajúce zdroje v domácom rozpočte | Z | N | **S** |
| 2.2 | Nevýhodná zmluva s dodávateľom | S | VN | N |
| **H3** | **Informačné operácie** | |  |  |
| 3.1 | Šírenie propagandy | Z | VN | N |
| 3.2 | Vytvorenie dezinformácií | Z | VN | N |
| 3.3 | Zdieľanie dezinformácií | Z | N | **S** |
| **H4** | **Kompromitácia funkcií alebo služieb** | | | |
| 4.1 | Chyba pri používaní | S | S | **S** |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | S | VN | N |
| 4.3 | Falšovanie práv alebo povolení | S | VN | N |
| 4.4 | Odmietnutie konania | M | N | N |
| 4.5 | Odmietnutie služby | M | N | N |
| 4.6 | Zhoršovanie stavu pamäťových médií | S | N | **S** |
| 4.7 | Zneužitie práv alebo povolení | Z | N | **S** |
| **H5** | **Ľudské konanie** | | | |
| 5.1 | Popretie | N | VN | N |
| 5.2 | Detekcia polohy | M | N | N |
| 5.3 | Infiltrácia webovej komunikácie | S | VN | N |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | K | S | **V** |
| 5.5 | Krádež médií (najmä USB) alebo dokumentov | S | VN | N |
| 5.6 | Krádež zariadenia (najmä mobilu) | K | S | **V** |
| 5.7 | Manipulácia s hardvérom | S | N | S |
| 5.8 | Manipulácia so softvérom | S | N | S |
| 5.9 | Neoprávnené používanie zariadení | N | N | N |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Z | S | **V** |
| 5.11 | Neoprávnený vstup do priestorov | S | VN | N |
| 5.12 | Nesprávne používanie zariadení | S | S | S |
| 5.13 | Nezákonné spracovanie údajov | Z | N | S |
| 5.14 | Odosielanie alebo distribúcia malvéru | Z | S | **V** |
| 5.15 | Odpočúvanie | S | VN | N |
| 5.16 | Podvodné kopírovanie softvéru | S | N | S |
| 5.17 | Poškodenie reputácie | Z | S | **V** |
| 5.18 | Poškodenie údajov | Z | N | S |
| 5.19 | Poškodenie zariadení alebo médií | Z | VN | N |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Z | S | **V** |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | Z | VN | N |
| 5.22 | Prístup neoprávneného používateľa k sieti | Z | N | S |
| 5.23 | Sociálne inžinierstvo | Z | N | S |
| 5.24 | Teroristický útok, sabotáž | Z | VN | N |
| 5.25 | Útok man-in-the-middle | Z | VN | N |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | Z | N | S |
| 5.27 | Vzdialené špehovanie | S | VN | N |
| 5.28 | Zachytenie žiarenia zariadenia | S | VN | N |
| 5.29 | Zber recyklovaných alebo vyradených médií | S | VN | N |
| 5.30 | Zverejňovanie informácií | Z | S | **V** |
| **H8** | **Organizačné hrozby** | | | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | S | S | S |
| 8.2 | Nedostatok personálu | Z | S | **V** |
| 8.3 | Nedostatok zdrojov | Z | S | **V** |
| 8.4 | Porušenie interných domácich pravidiel | S | S | S |
| 8.5 | Porušenie zákonov alebo nariadení | Z | N | S |
| 8.6 | Zlyhanie poskytovateľov služieb | Z | VN | N |
| **H9** | **Poruchy infraštruktúry** | | | |
| 9.1 | Elektromagnetické žiarenie | Z | VN | N |
| 9.2 | Elektromagnetické impulzy | Z | VN | N |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | S | VN | N |
| 9.4 | Porucha napájacieho systému | S | VN | N |
| 9.5 | Porucha telekomunikačného zariadenia alebo služby | S | VN | N |
| 9.6 | Porucha telekomunikačnej siete | S | VN | N |
| 9.7 | Strata napájania | S | VN | N |
| 9.8 | Tepelné žiarenie | S | VN | N |
| **H10** | **Prírodné hrozby** | | | |
| 10.1 | Klimatický jav | Z | N | S |
| 10.2 | Meteorologický jav | Z | VN | N |
| 10.3 | Pandémia/epidemický jav | Z | N | S |
| 10.4 | Poškodenie zvieraťom | S | VN | N |
| 10.5 | Povodeň | Z | N | S |
| 10.6 | Seizmický jav | Z | VN | N |
| **H.12** | **Súkromie** | | | |
| 12.6 | Neznalosť obsahu | Z | N | S |
| 12.7 | Neoprávnené sprístupnenie | Z | S | **V** |
| **H13** | **Technické poruchy** | | | |
| 13.1 | Porucha softvéru | Z | S | **V** |
| 13.2 | Porucha zariadenia alebo systému | Z | N | S |
| 13.3 | Strata napájania alebo kolísanie výkonu | S | VN | N |
| 13.4 | Zahltenie informačného systému | S | VN | N |
| 13.5 | Zníženie úrovne údržby, chyba údržby informačného systému | S | N | S |
| **H15** | **Verejný poriadok** | | | |
| 15.1 | Destabilizácia | Z | VN | N |
| 15.2 | Poškodenie zdravia obyvateľstva | K | V | **VV** |
| 15.3 | Verejné nepokoje | Z | VN | N |

## Školské IKT prostredie

Výber hrozieb a zraniteľností je na základe Katalógov hrozieb NBÚ a MIRRI.

Školské IKT prostredie (stredné školy) je typicky tvorené sieťovou infraštruktúrou, počítačovými učebňami a pracovnými stanicami, notebookmi učiteľov spolu s periférnymi zariadeniami (napr. tlačiareň, skener).

Realizácia hrozieb môže narušiť toto prostredie s následkami ako je zničenie, poškodenie alebo nedostupnosť IKT, nedostupnosť internetového pripojenia, nefunkčnosť softvéru, strata alebo poškodenie údajov čo vedie k narušeniu vyučovacieho procesu.

Pod pojmom objekt máme na mysli objekt alebo objekty vzdelávacieho zariadenia.

Pod pojmom IKT máme na mysli sieťovú infraštruktúru, hardvér, softvér, pamäťové nosiče a údaje.

### Hrozby

|  |  |  |
| --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Príklady spôsobu realizácie a primárny dopad** |
| **H1** | **Fyzické hrozby** | |
| 1.1 | Požiar | Požiar v objekte alebo učebni - po skrate elektrospotrebiča, zásahu blesku, pri opravách objektu, chybnej manipulácii s horľavinami, úmyselnom založení - vedie k poškodeniu priestorov a IKT |
| 1.2 | Prach, korózia, mrazy | Prašné okolie, nadmerná vlhkosť v priestoroch IKT, výpadok kúrenia v zime - môže viesť k poškodeniu infraštruktúry, hardvéru, pamäťových médií |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie | Veľká nehoda v okolí ako je požiar vedľajšej budovy, chemické znečistenie okolia, výbuch v blízkosti, závažná dopravná nehoda, letecká nehoda – môže viesť k nedostupnosti objektu, poškodeniu IKT aktív. |
| 1.4 | Voda | Prienik vody do objektu záplavou, vytopením, vodoinštalačnou haváriou – môže viesť k nedostupnosti objektu, poškodeniu objektu a jeho vnútorného vybavenia vrátane IKT. |
| 1.5 | Výbuch | Výbuch v objekte v dôsledku výbuchu plynu alebo priemyselnej havárie, málo pravdepodobne bombového útoku, teroristického útoku vojna, zásahu zbraňou – môže to viesť k nedostupnosti objektu, poškodeniu objektu a jeho vnútorného vybavenia vrátane IKT. |
| 1.6 | Znečistenie, škodlivé žiarenie | Znečistenie IKT (napr. olejom, sadzami, chemikáliami, farbou) alebo škodlivé elektromagnetické žiarenie v blízkosti IKT vedie k ich poškodeniu alebo výpadku |
| 1.7 | Zničenie zariadenia, alebo médií | Zničenie zariadení alebo médií napr. nesprávnym zaobchádzaním, vandalizmom či technickou chybou. |
| **H2** | **Hospodárske a ekonomické hrozby** | |
| 2.1 | Chýbajúce zdroje v rozpočte | Chýbajúce zdroje na opravu IKT, jej obnovu alebo prevádzku (napr. podpora SW) – môže znamenať obmedzenie využívania IKT alebo jeho časti |
| 2.2 | Nevýhodná zmluva s dodávateľom | Výhradnosť dodávateľa (tzv. vendor-lock), vyššie ceny ako sú bežné, vysoké sankcie v prípade odstúpenia |
| **H3** | **Informačné operácie** | |
| 3.1 | Šírenie propagandy | Úmyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech vzdelávacieho zariadenia - buď priamo v ňom, alebo v elektronických médiách a sociálnych sieťach |
| 3.2 | Vytvorenie dezinformácií | Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu vzdelávacieho zariadenia - buď priamo v ňom, alebo v elektronických médiách a sociálnych sieťach |
| 3.3 | Zdieľanie dezinformácií | Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu vzdelávacieho zariadenia na jeho IKT - žiakmi alebo učiteľmi. |
| **H4** | **Kompromitácia funkcií alebo služieb** | |
| 4.1 | Chyba pri používaní | Nechcená modifikácia údajov v cudzích súboroch či databázach, zmazanie systémových súborov, zmazanie pracovných súborov, potrebných pre chod softvéru – na úrovni žiaka, učiteľa, technika / administrátora. |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | Nesprávna konfigurácia sieťového zariadenia, zmeny v doručovaní pošty, úprava alebo presmerovanie správ pri reinštalácii alebo rekonfigurácii siete. |
| 4.3 | Falšovanie práv alebo povolení | Neoprávnené pozmeňovanie identít a prístupových práv do systémov pre žiakov a učiteľov, ich zneužitie v mene iného používateľa. |
| 4.4 | Odmietnutie konania | Odmietnutie vykonania pracovnej aktivity administrátorom, učiteľom, žiakom, odopretie pracovnej zodpovednosti v procese, napr. nie je to pracovnou náplňou. |
| 4.5 | Odmietnutie služby | Narušenie procesov, infraštruktúry alebo iných prvkov za účelom znefunkčnenia služby - typicky DoS, DDoS útok na infraštruktúru poskytovateľa pripojenia, zriedkavejšie priamo na vzdelávacie zariadenie. |
| 4.6 | Zhoršovanie stavu pamäťových médií | Starnutie archivovaných dokumentov na médiách, zničenie médií napr. pri požiari, vytopení a pod. |
| 4.7 | Zneužitie práv alebo povolení | Neoprávnené získanie identít a prístupových práv do školských systémov (napr. EduPage) a ich zneužitie na konanie v mene iného používateľa. |
| **H5** | ***Ľudské konanie*** | |
| 5.1 | Popretie | Stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje sfalšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfalšovanie identifikácie nepovolených aktivít, vymazanie zápis nesprávnych údajov do logov. |
| 5.2 | Detekcia polohy | Zistenie údajov o geografickej polohe používateľov, žiakov. |
| 5.3 | Infiltrácia webovej komunikácie | Poškodenie, alebo neoprávnená zmena obsahu webovej stránky školy, alebo aplikácie, ktorá môže meniť informačný obsah, alebo aj vizuálny vzhľad webovej stránky, alebo aplikácie (tzv. defacement). Hrozba prieniku do cieľového systému prostredníctvom webových aplikácií. |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | Krádež identity a jej zneužitie na podvodné konanie alebo neoprávnený prístup zo strany cudzej osoby, žiaka, učiteľa, technika. |
| 5.5 | Krádež médií alebo dokumentov | Krádež dokumentov, krádež súborov, strata súborov počas sťahovania, krádež emailu z mailboxu zo strany návštevníka školy, žiaka, učiteľa, technika. |
| 5.6 | Krádež zariadenia | Krádež notebooku, monitora, PC, myši, pevného disku a pod. |
| 5.7 | Manipulácia s hardvérom | Neoprávnená manipulácia s hardvérom, pridanie nekompatibilnej časti zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, odstránenie komponentov zariadenia, použitie neautorizovaných USB kľúčov alebo diskov. |
| 5.8 | Manipulácia so softvérom | Neoprávnená manipulácia so softvérom, nepovolené, neschválené aktualizácie, konfigurácie, výmena komponentov, nelegálne spájanie údajov, nepovolené získanie vyšších oprávnení, mazanie stôp po použití, zneužite softvérových funkcií zo strany žiaka, učiteľa, technika alebo externého útočníka. |
| 5.9 | Neoprávnené používanie zariadení | Neoprávnené používanie školského IKT na iné ako školské aktivity zo strany žiakov, učiteľov, technika. |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Nesprávne vybraný právny základ, chýbajúci právny základ spracúvania osobných údajov. |
| 5.11 | Neoprávnený vstup do priestorov | Neoprávnený vstup do IKT priestorov zo strany žiakov (napr. bez pedagogického dozoru). |
| 5.12 | Nesprávne používanie zariadení | Porušenie interných politík školy alebo návodov na bezpečné používanie zariadenia. |
| 5.13 | Nezákonné spracovanie údajov | Spracovanie osobných údajov bez právneho základu alebo nad jeho rámec |
| 5.14 | Odosielanie alebo distribúcia malvéru | Infiltrácia školského PC škodlivým kódom, PC sa stane zombie PC, cez ktoré sa ďalej rozosiela malvér, alebo malvér sa zasiela ďalej mailami a interakciami s okolím. |
| 5.15 | Odpočúvanie | Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky (napr. s osobnými údajmi). |
| 5.16 | Podvodné kopírovanie softvéru | Neoprávnená manipulácia so softvérom vedúca k nepovolenému/neschválenému kopírovaniu a prípadne aj ďalšiemu šíreniu (zo strany učiteľa, žiaka, administrátora). |
| 5.17 | Poškodenie reputácie | Poškodenie reputácie školy v dôsledku kybernetického bezpečnostného incidentu, nevhodným konaním žiakov pri využívaní cez IKT (klebety, ohováranie, dezinformácie, dehonestácia, poškodzovanie dobrého mena atď.) najmä využitím sociálnych sietí, chatu, mailu. |
| 5.18 | Poškodenie údajov | Zmena, alebo zničenie údajov, zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia správcu, manipulácia alebo zmena s informáciou, ktorá znamená narušenie jej integrity (napr. žiaci s hackerskými schopnosťami, chyby žiakov a učiteľov). |
| 5.19 | Poškodenie zariadení alebo médií | Úmyselné poškodenie zariadení, alebo médií, narušenie integrity zariadenia alebo média (napr. žiakmi bez pedagogického dozoru). |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Použitie nelegálneho, falošného alebo nelicencovaného softvéru žiakom alebo aj učiteľom. |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | Napr. po prieniku do školského IKT. Skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď. |
| 5.22 | Prístup neoprávneného používateľa k sieti | Zneužitie prístupových práv (žiaka, učiteľa) alebo úspešný externý hack do siete. |
| 5.23 | Sociálne inžinierstvo | Žiak alebo učiteľ ako obeť - ovplyvňovanie (phishing, sociálne inžinierstvo, a pod.), nátlak (výhražné emaily, psychologické obťažovanie) atď. |
| 5.24 | Teroristický útok, sabotáž | Vyhrážka teroristickým útok, úmyselná manipulácia alebo poškodenie fyzických objektov, zariadení a/alebo procesov alebo obmedzenie funkcií školského IKT z dôvodu sabotáže za účelom spôsobenia škody. |
| 5.25 | Útok man-in-the-middle | Typ hrozby počas ktorej útočník prenikne do komunikácie medzi školou a žiakom / rodičom a bez ich vedomia začne komunikáciu neoprávnene modifikovať. |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | V rámci vyučovacieho procesu, pri realizácii aktivít žiaka na školskom IKT. |
| 5.27 | Vzdialené špehovanie | Hackerské špehovanie sieťovej prevádzky školskej siete, maskovanie identity, sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu, atď. |
| 5.30 | Zverejňovanie informácií | Neoprávnené zverejnenie informácií osobám, ktoré k nim nemajú mať prístup – napr. informácie o žiakoch na webovom sídle, v plošnom maili. |
| **H8** | **Organizačné hrozby** | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | Zanedbanie bezpečnostných požiadaviek pri plánovaní, nákupe a implementácii HW a SW v školskom IKT (napr. opomenie sa anti-malware SW) na úrovni školy alebo zriaďovateľa. |
| 8.2 | Nedostatok personálu | Nedostatok personálnych kapacít pre správu školského IKT, pre riešenie jeho bezpečnosti a súladu s legislatívou. |
| 8.3 | Nedostatok zdrojov | Nedostatok finančných zdrojov pre bezpečné IKT prostredie školy. |
| 8.4 | Porušenie interných riadiacich aktov | Porušenie pravidiel školy vedúce k bezpečnostnej udalosti alebo zvýšeniu rizika. |
| 8.5 | Porušenie zákonov alebo nariadení | Porušenie zákona pri činnosti v KP vyúsťujúce do trestno-právnej, správno-právnej alebo inej právnej konzekvencie |
| 8.6 | Zlyhanie poskytovateľov služieb | Prerušenie outsourcovaných služieb, napr. dodávky elektrickej energie, telekomunikačných služieb, internetového pripojenia, údržby IKT narúšajúce prácu so školským IKT. |
| **H9** | **Poruchy infraštruktúry** |  |
| 9.1 | Elektromagnetická radiácia | Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením alebo magnetom. |
| 9.2 | Elektromagnetické impulzy | Poškodenie údajov (typicky na nosičoch) alebo HW elektromagnetickými impulzmi, resp. kolísaním napájania v sieti. |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | Porucha ventilácie PC alebo servera, ktorá môže spôsobiť jeho výpadok. |
| 9.4 | Porucha napájacieho systému | Narušenie alebo poškodenie energetickej infraštruktúry v rámci školy. |
| 9.5 | Porucha telekomunikačného zariadenia | Zlyhanie telekomunikačných komponentov školského IKT, prerušenie internej kabeláže, slabý telekomunikačný signál, nedostatočný signál Wi-Fi, atď. |
| 9.6 | Porucha telekomunikačnej siete | Poškodenie alebo výpadok externého telekomunikačného spojenia, zničenie kabeláže, výpadok komponentov optického spojenia. |
| 9.7 | Strata napájania | Obmedzená alebo zastavená dodávka energie. |
| 9.8 | Tepelné žiarenie | Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou v miestnosti. |
| **H10** | **Prírodné hrozby** |  |
| 10.1 | Klimatický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) alebo obmedzenie funkcií z dôvodu klimatického javu – víchrica, ktorá narušila strechu školy a následný dážď, záplava. |
| 10.2 | Meteorologický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) mrazom, vysokou teplotou, vetrom, vlhkosťou, bleskom. |
| 10.3 | Pandémia/epidemický jav | Výpadok technika, výpadok učiteľov IKT. |
| 10.4 | Poškodenie zvieraťom | Myš, potkan, hmyz. |
| 10.5 | Povodeň | Vytopenie priestorov s IKT aktívami. |
| 10.6 | Seizmický jav | Poškodenie objektu školy po zemetrasení. |
| **H.12** | **Súkromie** |  |
| 12.7 | Neoprávnené sprístupnenie | Neoprávnené sprístupnenie osobných údajov v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup. |
| **H13** | **Technické poruchy** |  |
| 13.1 | Porucha softvéru | Chyby počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď. |
| 13.2 | Porucha zariadenia alebo systému | Náhle a neplánované zlyhanie alebo porucha IKT zariadenia, alebo akéhokoľvek HW komponentu. |
| 13.3 | Strata napájania alebo kolísanie výkonu | Strata zdroja napájania alebo kolísanie výkonu napájania zariadení. |
| 13.4 | Zahltenie informačného systému | Plná úložná jednotka, preťaženie systému, nedostatok operačnej pamäte, slabý procesor, slabá grafická karta. |
| 13.5 | Zníženie úrovne údržby, chyba údržby informačného systému | Chyba údržby informačného systému, alebo IT zariadení (amatérske zásahy učiteľov alebo aj žiakov). |

**Najčastejšie hrozby v školskom IKT prostredí**

Číslovanie neodráža poradie miery rizika, slúži na referenčné účely.

1. Výpadky HW.
2. Strata údajov (s obmedzenými zálohami).
3. Napadnutie počítača malvérom.
4. Porucha zariadenia alebo systému.
5. Chyby pri používaní aplikácií.
6. Úmyselné narúšanie funkcionality IKT žiakmi.

### Zraniteľnosti

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Zraniteľnosť** |
| **1. Hardvér** | 1.1 | Amatérske zásahy do HW (učitelia, žiaci). |
| 1.2 | Nedostatočná údržba HW. |
| 1.3 | Prach v okolí (narúša činnosť ventilátora). |
| 1.4 | Nevhodné podmienky umiestenia (napr. možnosť zakopnutia o káble). |
| 1.5 | Napäťová nestabilita. |
| 1.6 | Pamäťové média nie sú uložené vo vhodnom priestore. |
|  | 1.7 | Starý HW bez technickej podpory. |
| **2. Softvér** | 2.1 | SW stiahnutý a inštalovaný z neautorizovaných zdrojov. |
| 2.2 | Nejasné plnenie licenčných podmienok používaného SW na škole. |
| 2.3 | Neaktualizovaný SW. |
| 2.4 | SW aktualizovaný z neautorizovaných zdrojov. |
| 2.5 | Ukončená technická podpora pre danú verziu SW. |
| 2.6 | Zraniteľnosti identifikované v SW. |
| 2.7 | Nevhodné prístupové heslá. |
| 2.8 | Nesprávna konfigurácia SW (napr. možnosť vzdialeného prístupu) |
| 2.9 | Nevhodné riadenie prístupových práv k SW (napr. možnosť žiaka dostať sa k súborom učiteľov). |
| 2.10 | Komplikované užívateľské rozhranie. |
| 2.11 | SW v angličtine používaný žiakom so slabou znalosťou EN. |
| 2.12 | Nedostatočne zaškolený používateľ na prácu so SW (žiak, učiteľ). |
|  | 2.13 | Starý SW bez technickej podpory. |
| **3. Sieť** | 3.1 | Nechránené verejné sieťové pripojenie. |
|  | 3.2 | Slabé heslo na internú wifi sieť. |
|  | 3.3 | Nepostačujúce zabezpečenie internej siete. |
|  | 3.4 | Sprístupnenie siete iným osobám (napr. bývalým žiakom). |
|  | 3.5 | Sieťová bezpečnosť len na minimálnej úrovni - bez FW / IDS / SIEM. |
|  | 3.6 | Chýbajúca správa siete. |
| **4. Používatelia** | 4.1 | Nezaškolení používatelia (žiaci, učitelia). |
|  | 4.2 | Nesprávne postupy pri práci s HW a SW. |
|  | 4.3 | Podceňovanie KB. |
| **5. Lokalita** | 5.1 | Nedostatočná fyzická ochrana učební, školy. |
|  | 5.2 | Záplavová oblasť umiestnenia školy. |
|  | 5.3 | Horľaviny v školských priestoroch. |
| **8. Org. prostredie** | 6.1 | Nebola vykonaná analýza rizík (na úrovni, ktorú zvládne aj škola, správca) |
|  | 6.2 | Chýba plán kontinuity činností (ak prídu učitelia alebo žiaci o údaje, o prístup k aplikáciám, IS je nedostupný – napr. EduPage). |
|  | 6.3 | Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládnu aj v škole). |
|  | 6.4 | Chýbajú interné postupy pre prácu s IKT (na úrovni, ktorej vypracovanie zvládnu aj v škole). |

**Najčastejšie zraniteľnosti v školskom IKT prostredí**

Číslovanie neodráža poradie miery vplyvu zraniteľnosti, slúži na referenčné účely.

1. Nevhodné prístupové heslá.
2. Neaktualizovaný SW (napr. OS).
3. Nesprávna konfigurácia SW (napr. možnosť vzdialeného prístupu).
4. Nezaškolení používatelia (žiaci, učitelia).
5. Nesprávne postupy pri práci s HW a SW.
6. Podceňovanie KB.
7. Chýba plán kontinuity činností (ak príde škola o údaje).
8. Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládne aj škola).
9. Chýbajú interné postupy pre prácu s IKT (na úrovni, ktorej vypracovanie zvládnu aj učitelia).

*Poznámka: kyberšikana, sexting a pod. zvyčajne prebiehajú mimo školského IKT, aj keď sa to môže diať v rámci vyučovania (cez súkromné mobily).*

### Možné dopady / následky

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Následky** |
|  |  | **Primárne následky pre priestory** |
| **1. Priestory / objekt** | 1.1 | Strata objektu školy vrátane vnútorného vybavenia a IKT aktív  (napr. po silnom požiari, výbuchu) |
| 1.2 | Poškodenie objektu školy vrátane vnútorného vybavenia a IKT aktív (napr. po menšom požiari alebo výbuchu). |
| 1.3 | Poškodenie objektu školy, ale nie IKT aktív (napr. po vytopení) |
|  | ***Sekundárne následky súvisiace s priestormi*** |
| 1.4 | Dlhodobá nedostupnosť objektu školy (napr. po narušení jeho statiky). |
| 1.5 | Dočasná nedostupnosť objektu školy v dôsledku jeho obnovy. |
| 1.6 | Dočasná neprístupnosť objektu školy (objekt uzavretý políciou) |
| **2. Hardvér** |  | ***Primárne následky pre HW*** |
| 2.1 | Poškodenie HW (napr. pri spadnutí na zem, pri sérii výpadkov prúdu). |
| 2.2 | Dočasná strata HW (poškodený HW je v oprave). |
| 2.3 | Trvalá strata HW (napr. ukradnutý HW, HW po požiari alebo zásahu blesku, vytopení). |
| 2.4 | Dočasná neprístupnosť HW (napr. notebook učiteľa zabudnutý v doma) |
| 2.5 | Dočasná nedostupnosť HW (napr. polícia v rámci šetrenia ho zhabala). |
| 2.6 | Dočasná výpadok prevádzkyschopnosti HW (vypadlo napájanie). |
|  | ***Sekundárne následky súvisiace s HW*** |
| 2.7 | Dočasná nedostupnosť HW kvôli obnove (napr. je v oprave alebo čaká na opravu) a z toho vyplývajúce narušenie služieb poskytovaných IKT školy. |
| 2.8 | Čas spotrebovaný na obnovu HW časti IKT. |
| 2.9 | Finančné náklady na opravu HW, reinštaláciu SW. |
| 2.10 | Finančné náklady na kúpu nového HW (ak je poškodený HW nepoužiteľný alebo je ukradnutý a nie je poistený). |
| **3. Softvér** |  | ***Primárne následky pre SW*** |
| 3.1 | Nedostupnosť použitia SW (kvôli narušenej dostupnosti alebo funkcionalite HW). |
| 3.2 | Narušenie funkcionality OS. |
| 3.3 | Nedostupnosť SW kvôli nefunkčnosti OS. |
| 3.4 | Strata nainštalovaného SW (napr. omylom vymazanie súborov, alebo výsledok činnosti malvéru) |
| 3.5 | Nefunkčnosť SW po jeho narušení (napr. pri amatérskom vymazaní niektorých jeho systémových súborov alebo zásahu do nich, pôsobenie malvéru) |
| 3.6 | Nesprávna činnosť SW po jeho narušení (napr. malvérom, bugom). |
| 3.7 | Poškodenie SW (súborov). |
| 3.8 | Strata licencie pre porušenie podmienok. |
| 3.9 | Ukončenie platnosti licencie. |
|  | ***Sekundárne následky súvisiace so SW*** |
| 3.10 | Dočasná nedostupnosť SW kvôli obnove (napr. celé PC je v oprave alebo čaká na opravu, reinštaláciu). |
| 3.11 | Čas spotrebovaný na obnovu SW časti IKT. |
| 3.12 | Finančné náklady na obnovu SW (napr. ak to robí servis). |
| 3.13 | Porušovanie autorského práva po ukončení licenčnej zmluvy. |
| **4. Údaje** | 4.1 | Trvalá strata údajov (od poslednej zálohy, alebo aj všetkých – ak nie je záloha) |
| 4.2 | Čas potrebný na obnovu údajov mimo záloh alebo opätovnú prípravu stratenej práce. |
| 4.3 | Poškodenie údajov, narušenie ich integrity. |
| 4.4 | Nedostupnosť údajov. |
| 4.5 | Údaje sú aktuálne nepoužiteľné kvôli nefunkčnému HW / SW. |
| 4.6 | Údaje sú nedostupné kvôli narušeniu prevádzky IS. |
| **5. Služby školského IKT** | 5.1 | Narušenie vyučovacieho procesu (nedostupné IKT). |
| 5.2 | Nemožnosť realizovať internetové platobné operácie školy. |
| 5.3 | Obmedzenie komunikačných aktivít školy s okolím. |
| 5.4 | Obmedzenie komunikácie školy s rodičmi. |
| **6. Školské aktivity** | 6.1 | Nesplnenie termínovaných úloh žiakov (napr. seminárnej práce na školskom IKT). |
| 6.2 | Meškanie v preberanom učive (ak je závislé na IKT). |
| 6.3 | Nedostupnosť informačných zdrojov pre samostatnú prácu učiteľov a žiakov na hodinách. |
| 6.4 | Nemožnosť realizovať vzdialený prístup v dištančnom vzdelávaní pre žiakov s individuálnym plánom. |
| 6.5 | Nemožnosť plniť úlohy zo strany učiteľov (napr. výkazy, prípravy prijímačiek a maturít). |
|  | 6.6 | Zneužívanie AI pri samostatnej domácej práci (napr. projekt, seminárka) s dopadom na obmedzenie rozvoja mentálnych schopností a rozvoji návyku podvádzania. |
| **7. Psychosociálne dopady** | 7.1 | Dlhodobá frustrácia žiakov aj učiteľov pri nefunkčnom alebo zastaralom IT. |
| 7.2 | Narušený vývoj schopností a zručností pri nesprávnom využívaní IKT na hodinách. |
| 7.3 | Šikana v škole s podporou domácich aktivít na IKT (sociálne siete). |
| 7.4 | Mikrošikana v škole s využitím IKT. |
|  | Sociálne vylúčenie v triede súvisiaca s IKT (napr. žiak nemá smartfón, nie je na sociálnych sieťach) |
| 7.5 | Nesústredenosť na hodinách pri dostupnosti mobilu. |
| **8. Zdravotné dopady** | 8.1 | Bolesti krku, nesprávne držanie tela (napr. pri nesprávnej výške monitorov, nevhodných stoličkách). |

Tu možno doplniť špecifické dopady mimo zoznamu

**Najčastejšie dopady v školskom KT prostredí**

Číslovanie neodráža poradie miery vplyvu dopadu, slúži na referenčné účely.

1. Narušenie vyučovacieho procesu (nedostupné IKT).
2. Čas potrebný na obnovu IKT prostredia po jeho narušení (HW, SW, konfigurácie, údaje).
3. Trvalá strata údajov (od poslednej zálohy, alebo aj všetkých – ak nie je záloha).
4. Čas potrebný na obnovu údajov mimo záloh alebo opätovnú prípravu stratenej práce.
5. Nedostupnosť IKT prostredia kvôli jeho narušeniu.
6. Dopady porušenia legislatívy ochrany osobných údajov.
7. Zneužívanie AI.

### Analýza rizík

Miera rizika v nasledujúcej tabuľke je posúdená pre typickú školu v aktuálne nízkej úrovni bezpečnostných opatrení.

Po realizácii projektu bezpečného pripojenia škôl do internetu bude potrebné túto analýzu aktualizovať.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| **H1** | **Fyzické hrozby** | | | |
| 1.1 | Požiar | K | VN | **S** |
| 1.2 | Prach, korózia, mrazy | S | VN | N |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie) | Z | VN | N |
| 1.4 | Voda | Z | VN | N |
| 1.5 | Výbuch | Z | VN | N |
| 1.6 | Znečistenie, škodlivé žiarenie | S | VN | N |
| 1.7 | Zničenie zariadenia, alebo médií | S | N | **S** |
| **H2** | **Hospodárske a ekonomické hrozby** | | | |
| 2.1 | Chýbajúce zdroje v  rozpočte | Z | N | **S** |
| 2.2 | Nevýhodná zmluva s dodávateľom | S | N | S |
| **H3** | **Informačné operácie** | |  |  |
| 3.1 | Šírenie propagandy | Z | VN | N |
| 3.2 | Vytvorenie dezinformácií | Z | VN | N |
| 3.3 | Zdieľanie dezinformácií | Z | N | **S** |
| **H4** | **Kompromitácia funkcií alebo služieb** | | | |
| 4.1 | Chyba pri používaní | S | S | **S** |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | S | VN | N |
| 4.3 | Falšovanie práv alebo povolení | S | VN | N |
| 4.4 | Odmietnutie konania | S | VN | N |
| 4.5 | Odmietnutie služby | S | VN | N |
| 4.6 | Zhoršovanie stavu pamäťových médií | S | N | **S** |
| 4.7 | Zneužitie práv alebo povolení | K | VN | **S** |
| **H5** | **Ľudské konanie** | | | |
| 5.1 | Popretie | S | VN | N |
| 5.2 | Detekcia polohy | M | VN | VN |
| 5.3 | Infiltrácia webovej komunikácie | S | VN | N |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | Z | VN | N |
| 5.5 | Krádež médií (najmä USB) alebo dokumentov | S | VN | N |
| 5.6 | Krádež zariadenia | S | N | S |
| 5.7 | Manipulácia s hardvérom | S | N | S |
| 5.8 | Manipulácia so softvérom | S | VN | N |
| 5.9 | Neoprávnené používanie zariadení | S | N | S |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Z | S | **V** |
| 5.11 | Neoprávnený vstup do priestorov | S | VN | N |
| 5.12 | Nesprávne používanie zariadení | S | S | S |
| 5.13 | Nezákonné spracovanie údajov | Z | N | **V** |
| 5.14 | Odosielanie alebo distribúcia malvéru | Z | N | S |
| 5.15 | Odpočúvanie | S | VN | N |
| 5.16 | Podvodné kopírovanie softvéru | S | VN | N |
| 5.17 | Poškodenie reputácie | Z | N | S |
| 5.18 | Poškodenie údajov | Z | N | S |
| 5.19 | Poškodenie zariadení alebo médií | Z | VN | N |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Z | VN | N |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | S | VN | N |
| 5.22 | Prístup neoprávneného používateľa k sieti | Z | N | S |
| 5.23 | Sociálne inžinierstvo | Z | N | S |
| 5.24 | Teroristický útok, sabotáž | Z | N | S |
| 5.25 | Útok man-in-the-middle | Z | VN | N |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | S | N | S |
| 5.27 | Vzdialené špehovanie | S | VN | N |
| 5.28 | Zachytenie žiarenia zariadenia | S | VN | N |
| 5.29 | Zber recyklovaných alebo vyradených médií | S | VN | N |
| 5.30 | Zverejňovanie informácií | Z | S | **V** |
| **H8** | **Organizačné hrozby** | | | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | S | S | S |
| 8.2 | Nedostatok personálu | Z | S | **V** |
| 8.3 | Nedostatok zdrojov | Z | S | **V** |
| 8.4 | Porušenie interných riadiacich aktov | S | S | S |
| 8.5 | Porušenie zákonov alebo nariadení | Z | N | S |
| 8.6 | Zlyhanie poskytovateľov služieb | Z | VN | N |
| **H9** | **Poruchy infraštruktúry** | | | |
| 9.1 | Elektromagnetické žiarenie | Z | VN | N |
| 9.2 | Elektromagnetické impulzy | Z | VN | N |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | S | VN | N |
| 9.4 | Porucha napájacieho systému | S | VN | N |
| 9.5 | Porucha telekomunikačného zariadenia alebo služby | S | VN | N |
| 9.6 | Porucha telekomunikačnej siete | S | VN | N |
| 9.7 | Strata napájania | S | N | S |
| 9.8 | Tepelné žiarenie | S | VN | N |
| **H10** | **Prírodné hrozby** | | | |
| 10.1 | Klimatický jav | Z | VN | N |
| 10.2 | Meteorologický jav | Z | VN | N |
| 10.3 | Pandémia/epidemický jav | Z | N | S |
| 10.4 | Poškodenie zvieraťom | S | VN | N |
| 10.5 | Povodeň | Z | N | S |
| 10.6 | Seizmický jav | Z | VN | N |
| **H.12** | **Súkromie** | | | |
| 12.6 | Neznalosť obsahu | Z | N | S |
| 12.7 | Neoprávnené sprístupnenie | Z | S | **V** |
| **H13** | **Technické poruchy** | | | |
| 13.1 | Porucha softvéru | Z | N | S |
| 13.2 | Porucha zariadenia alebo systému | Z | N | S |
| 13.3 | Strata napájania alebo kolísanie výkonu | S | VN | N |
| 13.4 | Zahltenie informačného systému | S | VN | N |
| 13.5 | Zníženie úrovne údržby, chyba údržby IS | S | N | S |
| **H15** | **Verejný poriadok** | | | |
| 15.1 | Destabilizácia | Z | VN | N |
| 15.2 | Poškodenie zdravia obyvateľstva | S | S | S |
| 15.3 | Verejné nepokoje | Z | VN | N |

## Mobilné / externé IKT prostredie

Je to prostredie, v ktorom sa pohybujeme a pracujeme s prenosnými, mobilnými zariadeniami. Jeho špecifikom je možné pripájanie sa do externých sietí s neznámou úrovňou bezpečnosti.

Klasifikácia prostredí:

* Trasa, po ktorej sa osoba pohybuje, má so sebou a prípadne aj využíva mobil.
* Externý objekt s vlastnou infraštruktúrou, kde si osoba prináša svoje zariadenie (BYOD), napr.
  + Kaviareň alebo iný priestor, kde osoba sa pripojí na externú wi-fi sieť.
  + Izba na dovolenke, kde osoba sa pripojí na externú wi-fi sieť.
  + Obydlie u priateľov, , kde osoba sa pripojí na externú wi-fi sieť.
* Externé prostredie s IKT, napr.
  + Počítačové herňa s vlastným HW a sieťou.
  + Externý profesionálny priestor so sieťovou infraštruktúrou pre prácu s vlastným HW.
  + Kaviareň alebo iný priestor, kde osoba môže využívať určený počítač, na ktorý sa prihlási.

Výber hrozieb a zraniteľností je z Katalógov hrozieb NBÚ a MIRRI. Špecifikácia aktív mobilného IKT prostredia je uvedená v kap. 3.1.

HW osoby je z hľadiska hrozieb dvoch druhov:

* Prenosný (tablet, notebook) - ktorý po príchode na miesto aktivity spustíme a pracujeme s ním.
* Mobilný (smartfón, inteligentné hodinky, inteligentné okuliare), ktorý je stále s nami a je v aktívnom stave.

ID je podľa Katalógu hrozieb MIRRI, hrozieb je menej ako v prípade domáceho alebo školského IKT prostredia.

### Hrozby

|  |  |  |
| --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Príklady spôsobu realizácie a primárny dopad** |
| **H1** | **Fyzické hrozby** | |
| 1.1 | Požiar | Požiar v externom objekte – môže viesť k poškodeniu IKT, ktoré sa tam akurát nachádzali. |
| 1.2 | Prach, korózia, mrazy | Prašné okolie, nadmerná vlhkosť v externom objekte - môže viesť k poškodeniu hardvéru a pamäťových médií. |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie) | Zničenie alebo nedostupnosť HW, ktorý bol aktuálne v objekte. |
| 1.4 | Voda | Prienik vody v externej lokalite - záplavou, vytopením, vodoinštalačnou haváriou – môže viesť k poškodeniu IKT (napr. osoba je na pláži a voda je v hoteli). |
| 1.5 | Výbuch | Výbuch v externom objekte v napr. dôsledku výbuchu plynu – môže to viesť k poškodeniu HW. |
| 1.6 | Znečistenie, škodlivé žiarenie | Znečistenie IKT (napr. olejom, sadzami, chemikáliami, farbou) v blízkosti IKT vedie k ich poškodeniu alebo výpadku |
| 1.7 | Zničenie zariadenia, alebo médií | Zničenie zariadení alebo médií napr. nesprávnym zaobchádzaním, pádom (pri prenose, počas chôdze a telefonovania ) či technickou chybou. |
| **H2** | **Hospodárske a ekonomické hrozby** | |
| 2.1 | Chýbajúce zdroje v domácom rozpočte | Chýbajúce zdroje na opravu alebo obnovu mobilného IKT alebo jeho prevádzku (napr. antimalware SW na ďalší rok) – môže znamenať obmedzenie využívania IKT alebo jeho časti, alebo zvýšenie miery rizika. |
| 2.2 | Nevýhodná zmluva s dodávateľom | Istá výhradnosť dodávateľa mobilného pripojenia a HW (tzv. vendor-lock), vyššie ceny ako sú bežné, vyššie sankcie v prípade odstúpenia. |
| **H3** | **Informačné operácie** | |
| 3.1 | Šírenie propagandy | Úmyselné šírenie propagandy za účelom ovplyvňovania svojho virtuálneho okolia využitím aplikácií na mobile – mailom, v elektronických médiách a sociálnych sieťach v externom prostredí. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť (dieťa je mimo domu). |
| 3.2 | Vytvorenie dezinformácií | Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií na mobile za účelom ovplyvňovania mienky svojho virtuálneho okolia mailom, v elektronických médiách a sociálnych sieťach  v externom prostredí. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť (dieťa je mimo domu). |
| 3.3 | Zdieľanie dezinformácií | Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky svojho virtuálneho okolia využitím aplikácií na mobile - mailom, v elektronických médiách a sociálnych sieťach v externom prostredí. Ak je to dieťa, rodičia o tejto aktivite nemusia vedieť. |
| **H4** | **Kompromitácia funkcií alebo služieb** | |
| 4.1 | Chyba pri používaní | Nechcená modifikácia údajov v  súboroch či databázach, zmazanie systémových súborov, zmazanie pracovných súborov potrebných pre chod softvéru. |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | Nesprávna konfigurácia externej siete, kde sa dieťa pripája. |
| 4.3 | Falšovanie práv alebo povolení | Neoprávnené pozmeňovanie identít a prístupových práv do systémov u osôb dostupných na externej sieti využitím hackerských nástrojov. |
| 4.4 | Odmietnutie konania | Odmietnutie vykonania napr. pri žiadosti o plnenie servisnej podpory. |
| 4.5 | Odmietnutie služby | Narušenie za účelom znefunkčnenia služby - typicky DoS, DDoS útok na infraštruktúru poskytovateľa pripojenia, alebo aj priamo na mobil. Môže sa jednať aj o napadnutie malvérom. |
| 4.6 | Zhoršovanie stavu pamäťových médií | Starnutie médií (zvyčajne USB, pamäťová karta v mobile) zničenie médií napr. pri požiari, vytopení a pod. |
| 4.7 | Zneužitie práv alebo povolení | Neoprávnené získanie identít a prístupových práv do systémov a ich zneužitie na konanie v mene iného používateľa na externej sieti (napr. za účelom platby). |
| **H5** | **Ľudské konanie** | |
| 5.1 | Popretie | Stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa na mobile, čo umožňuje zlomyseľnú manipuláciu alebo sfalšovanie identifikácie aktivít. Manipulácia alebo sfalšovanie identifikácie nepovolených aktivít. Na mobile to môže byť oblasť sťahovania detskej pornografie. |
| 5.2 | Detekcia polohy | Zistenie údajov o geografickej polohe používateľa mobilu s cieľom využitia týchto údajov na nekalú činnosť. |
| 5.3 | Infiltrácia webovej komunikácie | Hrozba prieniku do mobilu prostredníctvom webových aplikácií. |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | Krádež identity a jej zneužitie na podvodné konanie alebo neoprávnený prístup (dieťaťa, rodiča, identity rodiča dieťaťom) napr. hacknutím mobilu na externej sieti. |
| 5.5 | Krádež médií alebo dokumentov | Krádež pamäťových médií (napr. USB, ktoré má dieťa pri sebe). |
| 5.6 | Krádež zariadenia | Krádež notebooku, mobilu pri vykradnutí externého objektu, auta alebo lúpeži. |
| 5.7 | Manipulácia s hardvérom | Amatérska manipulácia s mobilom, notebookom pridanie nekompatibilného periférneho zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, odstránenie komponentov zariadenia. |
| 5.8 | Manipulácia so softvérom | Amatérska manipulácia so softvérom, nevhodné aktualizácie, zmeny konfigurácie, odmazanie systémových súborov atď. |
| 5.9 | Neoprávnené používanie zariadení | Neoprávnený alebo neautorizovaný prístup do systému alebo k zariadeniu, ktoré má dieťa pripojené na externej sieti. |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Neoprávnené poskytnutie, sprístupnenie alebo zverejnenie osobných údajov o iných osobách využitím mobilu (dieťa vytvorí fotografiu alebo video iných osôb a pošle to). |
| 5.11 | Neoprávnený vstup do priestorov | Neoprávnený fyzický vstup do externého objektu, kde je dočasne HW dieťaťa. |
| 5.12 | Nesprávne používanie zariadení | Porušenie politík alebo návodov na bezpečné používanie zariadenia (nechce sa čítať návod k použitiu). |
| 5.13 | Nezákonné spracovanie údajov | Neoprávnená manipulácia s informáciami, ku ktorým sa dieťa dostalo na externej sieti. |
| 5.14 | Odosielanie alebo distribúcia malvéru | Infiltrácia škodlivým kódom, mobil sa stane zombie mobil, cez ktoré sa ďalej rozosiela malvér - mailami a interakciami v sociálnych sieťach. |
| 5.15 | Odpočúvanie | Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky mobilu. |
| 5.16 | Podvodné kopírovanie softvéru | Neoprávnená manipulácia so softvérom vedúca k nepovolenému/neschválenému kopírovaniu a prípadne aj ďalšiemu šíreniu (napr. dieťa samostatne inštalujúce SW bez licencie na mobile). |
| 5.17 | Poškodenie reputácie | Poškodenie reputácie inej osoby úmyselným konaním cez mobil mimo domova (klebety, ohováranie, dezinformácie, dehonestácia, poškodzovanie dobrého mena atď.) najmä využitím sociálnych sietí, chatu, mailu, SMS. |
| 5.18 | Poškodenie údajov | Zmena, alebo zničenie údajov, zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia majiteľa, manipulácia alebo zmena s informáciou, ktorá znamená narušenie jej integrity (napr. hacknutý alebo aj požičaný mobil). |
| 5.19 | Poškodenie zariadení alebo médií | Úmyselné poškodenie zariadení, alebo médií, narušenie integrity zariadenia alebo média (napr. zlomyseľní kamaráti, fyzický útok, pokus o lúpež). |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Použitie nelegálneho, falošného alebo nelicencovaného softvéru dieťaťom alebo jeho rodičom na mobile. |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | Napr. ak sa dá dieťa na hackerskú dráhu. Pripojí sa k externej sietí a koná - skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď. |
| 5.22 | Prístup neoprávneného používateľa k sieti | Zneužitie prístupových práv alebo úspešný externý hack do externej siete, kde je dieťa pripojené. |
| 5.23 | Sociálne inžinierstvo | Dieťa ako obeť - ovplyvňovanie (phishing, sociálne inžinierstvo, podplácanie, a pod.), nátlak (výhražné emaily, psychologické obťažovanie) prostredníctvom mobilu. |
| 5.24 | Teroristický útok, sabotáž | Strata a poškodenie HW pri teroristickom útoku v blízkosti dieťaťa. |
| 5.25 | Útok man-in-the-middle | Typ hrozby počas ktorej útočník prenikne do komunikácie medzi dieťaťom a ďalšími účastníkmi v externej sieti a bez ich vedomia začne komunikáciu neoprávnene modifikovať. |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | Pri bežnom samostatnom používaní mobilu dieťaťom. |
| 5.27 | Vzdialené špehovanie | Hackerské špehovanie sieťovej prevádzky externej siete, maskovanie identity, sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu v externej sieti. |
| 5.28 | Zachytenie žiarenia zariadenia | Sledovanie GPS signálu mobilu dieťaťa. |
| 5.29 | Zber recyklovaných alebo vyradených médií | Odovzdanie médií s osobnými údajmi na skartáciu, recykláciu (napr. pokazený mobil s nevymazanými dátami – videá, fotografie). |
| 5.30 | Zverejňovanie informácií | Neoprávnené zverejnenie informácií osobám, ktoré k nim nemajú mať prístup cez mobil alebo na externej sieti – napr. o rodičoch a ich práci, o sebe sexuálnemu predátorovi. |
| **H8** | ***Organizačné hrozby*** | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | Zanedbanie bezpečnostných požiadaviek pri mobile a notebooku, implementácii SW. |
| 8.2 | Nedostatok personálu | Nedostatok personálnych kapacít rodičov na vytvorenie bezpečného mobilného IKT prostredia pre dieťa. |
| 8.3 | Nedostatok zdrojov | Nedostatok finančných zdrojov pre bezpečné mobilné IKT prostredie dieťaťa. |
| 8.4 | Porušenie interných pravidiel | Porušenie interných pravidiel externého IKT prostredia vedúce k bezpečnostnej udalosti alebo zvýšeniu rizika. |
| 8.5 | Porušenie zákonov alebo nariadení | Porušenie zákona pri aktivitách s mobilom vyúsťujúce do trestno-právnej, správno-právnej alebo inej právnej konzekvencie. |
| 8.6 | Zlyhanie poskytovateľov služieb | Prerušenie outsourcovaných služieb, napr. konektivity. |
| **H9** | **Poruchy infraštruktúry** | |
| 9.1 | Elektromagnetické žiarenie | Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením alebo magnetom, ak je mobil alebo notebook v ich blízkosti. |
| 9.2 | Elektromagnetické impulzy | Poškodenie údajov (typicky na nosičoch) alebo HW elektromagnetickými impulzmi, resp. kolísaním napájania v externej sieti. |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | Porucha chladenia notebooku, ktorá môže spôsobiť jeho výpadok. |
| 9.4 | Porucha napájacieho systému | Narušenie alebo poškodenie energetickej infraštruktúry v rámci externého prostredia. |
| 9.5 | Porucha telekomunikačného zariadenia alebo služby | Zlyhanie telekomunikačných komponentov, prerušenie kabeláže, slabý telekomunikačný signál, nedostatočný signál externej Wi-Fi, atď. |
| 9.6 | Porucha telekomunikačnej siete | Poškodenie telekomunikačného spojenia, zničenie kabeláže, výpadok komponentov optického spojenia, nedostupné externé WiFi pripojenie, atď. |
| 9.7 | Strata napájania | Obmedzená alebo zastavená dodávka energie v externom prostredí. |
| 9.8 | Tepelné žiarenie | Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou v externom prostredí (zabudnuté na slnku v lete). |
| **H10** | **Prírodné hrozby** | |
| 10.1 | Klimatický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) alebo obmedzenie funkcií z dôvodu klimatického javu – víchrica, ktorá narušila externé prostredie, záplava, lesný požiar v okolí. |
| 10.2 | Meteorologický jav | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) mrazom, vysokou teplotou, vetrom, vlhkosťou, bleskom (napr. počas dovolenky). |
| 10.3 | Pandémia/epidemický jav | Rozsiahla epidémia, nemoc, ktorá sa rozširuje na geograficky rozsiahlom území, ktorá má dopad aj na IKT prevádzku (napr. pri pobyte v zahraničí). |
| 10.4 | Poškodenie zvieraťom | Poškodenie *(typicky nosičov údajov, alebo IKT zariadení)* zvieratami – domáce (pes, mačka) alebo divými (myš, potkan, hmyz) v externom prostredí. |
| 10.5 | Povodeň | Poškodenie (typicky nosičov údajov, alebo IKT zariadení) povodňou, ktorá zasiahla externé prostredie. |
| 10.6 | Seizmický jav | Poškodenie (typicky externých priestorov, nosičov údajov, alebo IT zariadení) zemetrasením, alebo inými seizmickými udalosťami (napr. na dovolenke v Japonsku). |
| **H.12** | **Súkromie** | |
| 12.6 | Neznalosť obsahu | Neznalosť obsahu je hrozba, ktorá indikuje, že používateľ (dieťa) si neuvedomuje obsah informácie spracovanej v systéme a následne napr. zverejňuje cez mobil v externom prostredí nadbytočné informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. jeho identitu. Alebo poskytuje informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie (napr. nechcené prezradenie informácií). |
| 12.7 | Neoprávnené sprístupnenie | Neoprávnené sprístupnenie osobných údajov v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup. (Napr. videá z mobilu, kde sú snímané iné osoby). |
| **H13** | **Technické poruchy** |  |
| 13.1 | Porucha softvéru | Chyby v mobile počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď. |
| 13.2 | Porucha zariadenia alebo systému | Náhle a neplánované zlyhanie alebo porucha mobilu alebo akéhokoľvek HW komponentu. |
| 13.3 | Strata napájania alebo kolísanie výkonu | Strata zdroja napájania alebo kolísanie výkonu napájania zariadení (napr. mobilu počas aktulizácie SW). |
| 13.4 | Zahltenie informačného systému | Plná pamäť mobilu, nedostatok operačnej pamäte, slabý procesor. |
| 13.5 | Zníženie úrovne údržby, chyba údržby informačného systému | Chyba údržby mobilu, alebo IT zariadení (amatérske zásahy – napr. do napájania). |
| **H15** | **Verejný poriadok** |  |
| 15.1 | Destabilizácia | Destabilizácia a narušenie chodu orgánov verejnej moci napr. v dôsledku masívneho hackerského útoku (zombie mobil v útoku môže byť aj mobil dieťaťa). |
| 15.2 | Poškodenie zdravia obyvateľstva | Poškodenie zdravia významnej časti mladej generácie v dôsledku vplyvu a dlhodobého pôsobenia digitálnych technológií (závislosti, civilizačné choroby). |
| 15.3 | Verejné nepokoje | Verejné nepokoje a protesty, vedúce k narušeniu verejného poriadku na území okresu, kraja, štátu v dôsledku konania interných skupín, koordinované cez špecializované aplikácie (napr. Telegram), v ktorých môže byť zapojená aj mládež. |

**Najčastejšie hrozby v mobilnom a externom IKT prostredí**

Číslovanie neodráža poradie miery súvisiaceho rizika, slúži na referenčné účely.

1. Poškodzovanie zdravia nadmerným používaním mobilu.
2. Kyberšikana v mobilnom prostredí, často kombinovaná s fyzickou šikanou na škole.
3. Dieťa ako obeť sociálneho inžinierstva s následnými dopadmi pri práci s mobilom (napr. sexting).
4. Porušovanie autorských práv (SW, digitálny obsah).
5. Porušovanie ochrany osobných údajov (zdieľanie cudzích osobných údajov, napr. videí).
6. Krádež digitálnej identity alebo prihlasovacích údajov.
7. Vstup údajov z nedôveryhodných zdrojov.
8. Ukradnutie mobilu.
9. Strata údajov v mobile (bez existencie adekvátnej zálohy).
10. Napadnutie mobilu /notebooku malvérom.
11. Chyby pri používaní aplikácií.

### Zraniteľnosti

V Katalógu zraniteľností s ohľadom na mobilné IKT prostredie vychádzame z Katalógu MIRRI v členení oblastí, ale ID je vlastné.

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Zraniteľnosť** |
| **1. Hardvér** | 1.1 | Amatérske zásahy do mobilného HW (deti, rodičia). |
| 1.2 | Nevhodná nabíjačka mobilu. |
| 1.3 | Mobil dieťaťa v zadnom vrecku. |
| 1.4 | Ponechanie mobilu alebo notebooku v nechránenom priestore (napr. počas záujmovej činnosti). |
| **2. Softvér** | 2.1 | SW stiahnutý a inštalovaný z neautorizovaných zdrojov. |
| 2.2 | Nejasné plnenie licenčných podmienok používaného SW. |
| 2.3 | Neaktualizovaný SW. |
| 2.4 | SW aktualizovaný z neautorizovaných zdrojov. |
| 2.5 | Ukončená technická podpora pre danú verziu SW. |
| 2.6 | Zraniteľnosti identifikované v SW. |
| 2.7 | Nevhodné prístupové heslá – k mobilu, do aplikácií. |
| 2.8 | Nesprávna konfigurácia SW (napr. možnosť vzdialeného prístupu) |
| 2.9 | Nevhodné riadenie prístupových práv k SW (napr. možnosť vzdialeného prístupu). |
| 2.10 | Komplikované užívateľské rozhranie. |
| 2.11 | SW v angličtine používaný dieťaťom so slabou znalosťou EN. |
| 2.12 | Nedostatočne zaškolený používateľ (dieťa) pre prácu s mobilom. |
| **3. Sieť** | 3.1 | Nechránené verejné sieťové pripojenie |
|  | 3.2 | Slabé heslo na externú wifi sieť. |
|  | 3.3 | Nepostačujúce zabezpečenie externej siete. |
|  | 3.4 | Sprístupnenie lokálneho access pointu cez mobil iným osobám. |
|  | 3.5 | Prevádzka zastaralých komponentov externej siete (router, AP, Bluetooth), ktoré obsahujú prelomené ochranné prvky |
| **4. Používatelia** | 4.1 | Nezaškolení používatelia (deti, rodičia) z hľadiska bezpečného používania mobilu / notebooku. |
|  | 4.2 | Nesprávne postupy pri práci s mobilným HW a SW. |
|  | 4.3 | Podceňovanie KB mobilných zariadení. |
| **5. Lokalita / objekt** | 5.1 | Nedostatočná fyzická ochrana externej lokality, kde si osoba ponecháva mobil (napr. pri športe) |
| **8. Org. prostredie** | 8.1 | Chýba plán kontinuity činností (ak príde dieťa o mobil). |
|  | 8.2 | Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládnu aj rodičia) – napr. bolo platené niečo, čo si nikto nekúpil. |
|  | 8.3 | Chýbajú interné postupy pre prácu s mobilným  IKT pre dieťa. |
|  | 8.4 | Chýbajúca kontrola digitálnych aktivít dieťaťa. |

**Najčastejšie zraniteľnosti v domácom IKT prostredí**

Číslovanie neodráža poradie miery vplyvu zraniteľnosti, slúži na referenčné účely.

1. Chýba plán kontinuity činností (ak príde dieťa o mobil).
2. Nezaškolení používatelia (deti, rodičia) z hľadiska bezpečného používania mobilu / notebooku.
3. Nevhodné prístupové heslá.
4. Dieťa používa mobil bez rodičovskej kontroly.
5. Nesprávne postupy pri práci s HW a SW.
6. Podceňovanie KB.
7. Chýbajú postupy manažmentu kybernetických bezpečnostných incidentov (na úrovni, ktorú zvládnu aj rodičia a dieťa).

### Možné dopady / následky

|  |  |  |
| --- | --- | --- |
| **Oblasť** | **ID** | **Následky** |
| **1. Priestory / objekt** |  | **Priamo sa netýka.** |
| **2. Hardvér** |  | ***Primárne následky pre HW*** |
| 2.1 | Poškodenie prenášaného mobilného HW (napr. pri spadnutí na zem) a jeho následná nedostupnosť. |
| 2.2 | Dočasná nedostupnosť HW (napr. notebook odložený v schránke na vrátnici). |
| 2.3 | Trvalá strata HW (napr. ukradnutý notebook či mobil). |
| 2.4 | Dočasná neprístupnosť HW (napr. notebook zabudnutý v škole) |
| 2.6 | Dočasná výpadok prevádzkyschopnosti HW (došlo napájanie v mobile). |
|  | ***Sekundárne následky súvisiace s HW*** |
| 2.7 | Čas spotrebovaný na obnovu HW (napr. notebook, mobil). |
| 2.8 | Finančné náklady na opravu HW. |
| 2.9 | Finančné náklady na kúpu nového HW (ak je poškodený HW nepoužiteľný alebo je ukradnutý a nie je poistený). |
| 2.10 | **Nemožnosť pracovať so zariadením a využívať jeho služby.** |
| **3. Softvér** |  | ***Primárne následky pre SW*** |
| 3.1 | Narušenie funkcionality OS. |
| 3.2 | Nedostupnosť SW kvôli nefunkčnosti OS. |
| 3.3 | Strata nainštalovaného SW (napr. omylom vymazanie súborov, alebo výsledok činnosti malvéru po pripojení na externú wifi-sieť). |
| 3.4 | Nefunkčnosť SW po jeho narušení (napr. po napadnutí malvérom). |
| 3.5 | Nesprávna činnosť SW po jeho narušení (napr. malvérom, bugom). |
| 3.6 | Poškodenie SW (súborov). |
| 3.7 | Strata licencie pre porušenie podmienok. |
|  | ***Sekundárne následky súvisiace so SW*** |
|  | Nedostupnosť použitia SW (kvôli narušenej dostupnosti alebo funkcionalite HW) a funkcionality zariadenia. |
| 3.9 | Dočasná nedostupnosť SW kvôli obnove (napr. celý notebook alebo mobil je v oprave alebo čaká na reinštaláciu). |
| 3.10 | Čas spotrebovaný na obnovu SW časti IKT. |
| 3.11 | Finančné náklady na obnovu SW (napr. ak to robí servis). |
| 3.12 | Porušovanie autorského práva po ukončení licenčnej zmluvy. |
|  | 3.13 | **Nemožnosť pracovať so zariadením a využívať jeho služby.** |
| **4. Údaje** | 4.1 | Trvalá strata údajov (od poslednej zálohy, alebo aj všetkých – ak nie je záloha) – v mobile, na notebooku. |
| 4.2 | Čas potrebný na obnovu údajov mimo záloh alebo opätovné vykonanie stratenej práce. |
| 4.3 | Poškodenie údajov, narušenie ich integrity. |
| 4.4 | Dočasná nedostupnosť údajov. |
| 4.5 | Údaje sú aktuálne nepoužiteľné kvôli nefunkčnému HW / SW. |
| 4.6 | Dopady vyplývajúce z narušenia dôvernosti údajov (najmä osobitnej kategórie – napr. privátny sexuálny obsah obrázkov alebo videí). |
| **5. Služby mobilného IKT** | 5.1 | Nemožnosť telefonovať alebo posielať SMS. |
| 5.2 | Nemožnosť realizovať internetové platobné operácie. |
| 5.3 | Obmedzenie virtuálnych sociálnych aktivít (na mobile). |
| 5.4 | Obmedzenie virtuálnych voľnočasových aktivít (na mobile). |
| **6. Školské aktivity** | 6.1 | Týka sa v malej miere |
| **7. Psychosociálne dopady** | 7.1 | Dlhodobá frustrácia spôsobená vplyvom sociálnych sietí. |
| 7.2 | Narušený psychosociálny vývoj. |
| 7.3 | Negatívne vplyvy nadmerného využívania digitálnych technológií. |
| 7.4 | Negatívne vplyvy nelátkových závislostí. |
| 7.5 | Iné, viď kap. 2.4 |
| **8. Finančné dopady** | 8.1 | Náklady na herný HW a SW. |
| 8.2 | Náklady na nové zariadenie (pokazený / málo výkonný) na úrovni očakávanej komunitou (napr. nový iPhone). |
| 8.3 | Náklady na predmety do hier. |
| 8.4 | Náklady na stávkovanie / gambling. |
| 8.5 | Strata financií v dôsledku podvodu / fraudu. |
| 8.6 | Náklady na prekročené dátové limity (napr. pri sťahovaní videí v zahraničí) |
| 8.7 | Iné náklady |

**Najčastejšie dopady v mobilnom IKT prostredí**

Číslovanie neodráža poradie miery dopadu, slúži na referenčné účely.

1. Nemožnosť pracovať so zariadením a využívať jeho služby v dôsledku straty alebo narušenia HW a SW.
2. Náklady na nový mobil (náhrada za stratený mobil, alebo mobil, ktorý nie je „cool“).
3. Náklady na herný HW a SW (mobilná konzola).
4. Čas potrebný na obnovu údajov mimo záloh alebo opätovnú prípravu stratenej práce.
5. Nedostupnosť IKT prostredia kvôli jeho narušeniu.
6. Dlhodobá frustrácia spôsobená vplyvom sociálnych sietí.
7. Narušený psychosociálny vývoj.
8. Negatívne vplyvy nelátkových závislostí.
9. Nedostatok pohybu a spánku.
10. Nesprávne držanie tela, narušenie správneho vývoja chrbtice.

### Analýza rizík

Miera rizika v nasledujúcej tabuľke je posúdená pre dieťa, ktorého mobilné zariadenia sú na nízkej úrovni zabezpečenia a ktoré si nie je plne vedomé rizík wi-fi sietí, do ktorých sa pripája a nástrah v kybernetickom priestore.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| **H1** | **Fyzické hrozby** | | | |
| 1.1 | Požiar | S | VN | N |
| 1.2 | Prach, korózia, mrazy | M | VN | VN |
| 1.3 | Veľká nehoda v okolí (nedostupnosť objektu, poškodenie) | S | VN | N |
| 1.4 | Voda | Z | VN | N |
| 1.5 | Výbuch | Z | VN | N |
| 1.6 | Znečistenie, škodlivé žiarenie | S | VN | N |
| 1.7 | Zničenie zariadenia, alebo médií | S | N | **S** |
| **H2** | **Hospodárske a ekonomické hrozby** | | | |
| 2.1 | Chýbajúce zdroje v  rozpočte | Z | N | **S** |
| 2.2 | Nevýhodná zmluva s dodávateľom | S | VN | N |
| **H3** | **Informačné operácie** | |  |  |
| 3.1 | Šírenie propagandy | Z | N | S |
| 3.2 | Vytvorenie dezinformácií | Z | VN | N |
| 3.3 | Zdieľanie dezinformácií | Z | N | **S** |
| **H4** | **Kompromitácia funkcií alebo služieb** | | | |
| 4.1 | Chyba pri používaní | S | N | **S** |
| 4.2 | Chyby prenosu (vrátane nesprávneho smerovania správ) | S | VN | N |
| 4.3 | Falšovanie práv alebo povolení | S | N | S |
| 4.4 | Odmietnutie konania | M | VN | VN |
| 4.5 | Odmietnutie služby | M | VN | VN |
| 4.6 | Zhoršovanie stavu pamäťových médií | S | VN | N |
| 4.7 | Zneužitie práv alebo povolení | K | N | **V** |
| **H5** | **Ľudské konanie** | | | |
| 5.1 | Popretie | S | VN | N |
| 5.2 | Detekcia polohy | S | N | S |
| 5.3 | Infiltrácia webovej komunikácie | S | N | S |
| 5.4 | Krádež digitálnej identity alebo prihlasovacích údajov | K | N | **V** |
| 5.5 | Krádež médií (najmä USB) alebo dokumentov | S | VN | N |
| 5.6 | Krádež zariadenia | S | N | S |
| 5.7 | Manipulácia s hardvérom | S | N | S |
| 5.8 | Manipulácia so softvérom | S | N | S |
| 5.9 | Neoprávnené používanie zariadení | S | S | S |
| 5.10 | Neoprávnené spracúvanie osobných údajov | Z | S | **V** |
| 5.11 | Neoprávnený vstup do priestorov | S | VN | N |
| 5.12 | Nesprávne používanie zariadení | S | S | S |
| 5.13 | Nezákonné spracovanie údajov | Z | S | **V** |
| 5.14 | Odosielanie alebo distribúcia malvéru | Z | N | S |
| 5.15 | Odpočúvanie | S | VN | N |
| 5.16 | Podvodné kopírovanie softvéru | S | N | S |
| 5.17 | Poškodenie reputácie | Z | N | S |
| 5.18 | Poškodenie údajov | Z | N | S |
| 5.19 | Poškodenie zariadení alebo médií | Z | VN | N |
| 5.20 | Používanie falošného alebo skopírovaného softvéru | Z | N | S |
| 5.21 | Používanie sieťových zariadení neoprávneným spôsobom | S | VN | N |
| 5.22 | Prístup neoprávneného používateľa k sieti | Z | N | S |
| 5.23 | Sociálne inžinierstvo | Z | S | **V** |
| 5.24 | Teroristický útok, sabotáž | Z | VN | N |
| 5.25 | Útok man-in-the-middle | Z | VN | N |
| 5.26 | Vstup údajov z nedôveryhodných zdrojov | Z | N | S |
| 5.27 | Vzdialené špehovanie | Z | N | S |
| 5.28 | Zachytenie žiarenia zariadenia | S | VN | N |
| 5.29 | Zber recyklovaných alebo vyradených médií | S | VN | N |
| 5.30 | Zverejňovanie informácií | Z | S | **V** |
| **H8** | **Organizačné hrozby** | | | |
| 8.1 | Chybné plánovanie a nedostatky v adaptácii | S | S | S |
| 8.2 | Nedostatok personálu | Z | S | **V** |
| 8.3 | Nedostatok zdrojov | Z | S | **V** |
| 8.4 | Porušenie interných pravidiel | S | S | S |
| 8.5 | Porušenie zákonov alebo nariadení | Z | N | S |
| 8.6 | Zlyhanie poskytovateľov služieb | Z | VN | N |
| **H9** | **Poruchy infraštruktúry** | | | |
| 9.1 | Elektromagnetické žiarenie | Z | VN | N |
| 9.2 | Elektromagnetické impulzy | Z | VN | N |
| 9.3 | Porucha chladiaceho alebo ventilačného systému | S | VN | N |
| 9.4 | Porucha napájacieho systému | S | VN | N |
| 9.5 | Porucha telekomunikačného zariadenia alebo služby | S | VN | N |
| 9.6 | Porucha telekomunikačnej siete | S | N | S |
| 9.7 | Strata napájania | S | N | S |
| 9.8 | Tepelné žiarenie | S | VN | N |
| **H10** | **Prírodné hrozby** | | | |
| 10.1 | Klimatický jav | Z | VN | N |
| 10.2 | Meteorologický jav | Z | VN | N |
| 10.3 | Pandémia/epidemický jav | Z | VN | N |
| 10.4 | Poškodenie zvieraťom | S | VN | N |
| 10.5 | Povodeň | Z | VN | N |
| 10.6 | Seizmický jav | Z | VN | N |
| **H.12** | **Súkromie** | | | |
| 12.6 | Neznalosť obsahu | Z | N | S |
| 12.7 | Neoprávnené sprístupnenie | Z | S | **V** |
| **H13** | **Technické poruchy** | | | |
| 13.1 | Porucha softvéru | Z | N | S |
| 13.2 | Porucha zariadenia alebo systému | Z | N | S |
| 13.3 | Strata napájania alebo kolísanie výkonu | S | VN | N |
| 13.4 | Zahltenie informačného systému | S | VN | N |
| 13.5 | Zníženie úrovne údržby, chyba údržby IS | S | N | S |
| **H15** | **Verejný poriadok** | | | |
| 15.1 | Destabilizácia | Z | VN | N |
| 15.2 | Poškodenie zdravia obyvateľstva | K | V | **VV** |
| 15.3 | Verejné nepokoje | Z | VN | N |

## Analýza dopadov (BIA) pre školské IKT prostredie

### Legislatívny a vecný rámec BIA

V zmysle legislatívy KB je jednou z povinností prevádzkovateľa základnej služby vypracovanie analýzy funkčného dopadu (ďalej aj ako „BIA“), ktorá pozostáva z hodnotenia dopadu na činnosť prevádzkovateľa základnej služby spôsobeného realizáciou krízového scenára, ktorý môže spôsobiť ohrozenie alebo narušenie kontinuity jeho poskytovanej služby.

Aj keď ZŠ alebo SŠ nie je prevádzkovateľom základnej služby, je prevádzkovateľom IS verejnej správy. Prevádzkovateľom základnej služby môže byť niektorý z dodávateľov (napr. v novom projekte bezpečnej internetovej konektivity pre školy ako súčasť DigEdu /DigiNet [[29]](#footnote-29)).

V zmysle vyhlášky pre IT VS č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:

§ 3 Minimálne bezpečnostné opatrenia

(2) Minimálne bezpečnostné opatrenia Kategórie I jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na ...

c) právnickú osobu v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia podľa § 5 ods. 2 písm. a) až d) zákona, ktorá nie je uvedená v odsekoch 3 a 4,

ZŠ alebo SŠ spĺňa podmienku podľa písm. c)

Pre Kategóriu 1 sú pre Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti definované nasledujúce požiadavky:

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

1. Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti.

2. Návrh a prijatie bezpečnostných opatrení.

3. Periodické preskúmavanie rizík.

BIA slúži ako podklad pre:

* analýzu rizík, keďže posudzuje mieru dopadu pri narušení kontinuity služieb poskytovaných školou alebo domácnosťou.
* plánovanie kontinuity činností školy resp. domácnosti.

Zmyslom BIA (pre oblasť IKT) je najmä nájsť odpoveď na otázku: Aké dopady (následky) môže mať výpadok činností škôl v rámci poskytovaných služieb podporovaných IS na

1. samotnú školu
2. žiakov
3. ich rodičov
4. pedagógov
5. štát ako celok

Čo má s BIA štát ako celok? Sú to dopady, ktoré sa týkajú významnej časti škôl.

V školskom roku 2024/2024 vyučovalo približne 447.000 žiakov na 1837 základných školách a 215 000 žiakov na cca. 800 stredných školách.

Ak rátame priemerne 1 rodiča na žiaka (osamelý rodič, viac detí v rodine), možné dopady sa môžu týkať aj cca. 662.000 a viac rodičov.

Príklady:

* Je nahlásená bomba v škole, žiaci sú poslaní domov a celý deň sa neučí. Po žiakov nižších ročníkov ZŠ si musia prísť rodičia, ktorým to naruší pracovný proces.
  + Je nahlásená bomba v stovkách škôl a celý deň sa neučí.
  + Je periodicky nahlasovaná bomba v stovkách škôl a celé dni sa neučí, dochádza k destabilizáciu bezpečnosti štátu.
* V dôsledku hackerského útoku prišla škola o dáta a IS nie je dostupný celý týždeň.
  + V dôsledku masívneho hackerského útoku prišli stovky škôl o dáta a IS nie je dostupný celý týždeň a viac.

Rozsah služieb poskytovaných IS školy resp. domácnosti je uvedený v kap. 3.1.

Kľúčové služby školy sú uvedené v zákone č. 350/1994 Z. z. o sústave základných a stredných škôl (školský zákon):

**ZÁKLADNÁ ŠKOLA** - § 5

(1) **Základná škola poskytuje základné vzdelanie**; **zabezpečuje rozumovú výchovu v zmysle vedeckého poznania** a v súlade so zásadami vlastenectva, humanity a demokracie a poskytuje mravnú, estetickú, pracovnú, zdravotnú, telesnú výchovu a ekologickú výchovu žiakov; umožňuje aj náboženskú výchovu.

(2) **Základná škola pripravuje žiakov na ďalšie štúdium a prax.**

Pre napĺňanie služieb poskytovaných ZŠ sú využívané aj IKT a ich narušenie môže negatívne ovplyvniť poskytované služby.

**STREDNÉ ŠKOLY** - § 7

(1) **Stredné školy poskytujú žiakom stredné odborné vzdelanie, úplné stredné vzdelanie, úplné stredné odborné vzdelanie a vyššie odborné vzdelanie** a **pripravujú ich na výkon povolaní a činností v národnom hospodárstve, správe, kultúre, umení a v ostatných oblastiach života; pripravujú žiakov aj na štúdium na vysokých školách.**

(2) Stredné školy uplatňujú jednotu výchovy a vzdelávania, **spojenie školy so životom** a usilujú sa o všestranný harmonický rozvoj osobnosti mladého človeka; **vychovávajú ho v zmysle vedeckého poznania** a v súlade so zásadami vlastenectva, humanity a demokracie, formujú jeho intelektuálny a mravný rozvoj, **pripravujú ho na tvorivú prácu a odbornú činnosť v povolaní** a poskytujú estetickú, zdravotnú, telesnú výchovu a ekologickú výchovu; umožňujú aj náboženskú výchovu.

### Klasifikačné schémy pre posúdenie dopadov

V tejto kapitole sú uvedené klasifikačné schémy dopadov s vysvetlením.

### Časové limity výpadku

voči ktorým popisujeme možné dopady (následky) pre žiaka, triedu, školu ako celok.

1. 5 minút – 1 vyučovacia hodina
2. 2 vyučovacie hodiny – celý pracovný deň
3. 2 - 7 dní (celý týždeň)
4. 7 – 30 dní (celý mesiac)
5. 1 mesiac - štvrťrok
6. Celý školský rok (viď COVID pandémia)

### Klasifikácia dopadov podľa kvantitatívnej škály

**Klasifikácia podľa odhadovanej možnej finančnej škody** resp. neefektívne vynaložených finančných prostriedkov na vzdelávanie.

1. Do 100 €
2. 100 – 1.000 €
3. 1.000 – 10.000 €
4. 10.000 – 100.000 €
5. 100.000 – 1.000.000 €
6. 1.000.000 – 10.000.000 €
7. 10.000.000 – 100.000.000 €
8. 100.000.000 – 1.000.000.000 €
9. 1.000.000.000 – 10.000.000.000 €
10. Nad 10 mld. €

Okrem dopadu na konkrétne dieťa / rodiča / školu je dôležitý aj prípadný kumulatívny dopad na všetky deti, ich rodičov (krát 662.000) a školy ako celok (krát 2.600).

**Klasifikácia podľa časovej straty**

Modelová škola

Dopady z hľadiska odhadovaných časových strát vyučovacích hodín pre modelovú školu s 12 triedami a 30 žiakmi v triede, 5 hodín vyučovania denne. Pre konkrétnu školu sú tieto čísla ľahko upraviteľné.

**Škola**

1. Do 1 vyučovacej hodiny
2. 2 - 30 hodín (vyučovacia hodina triedy)
3. 31 – 150 hodín (vyučovací deň triedy)
4. 151 – 1800 hodín (vyučovací deň školy)
5. 1801 – 9000 hodín (vyučovací týždeň školy)
6. 9001 – 36.000 hodín (vyučovací mesiac školy)

**Školy**

1. 36.000 - 180.000 (vyučovací deň 100 škôl)
2. 181.000 - 1.800.000 (vyučovací deň 1000 škôl)
3. 1.800.000 – 4.746.800 (vyučovací deň všetkých škôl)
4. 4.746.801 – 23.733.000 (vyučovací týždeň všetkých škôl)
5. 23.733.000 – 94.932.000 (vyučovací mesiac v rozsahu 4 týždňov, sú aj sviatky)
6. 94.932.000 - 949.320.000 (školský rok v rozsahu 10 mesiacov pre všetky ZŠ a SŠ)

Ministerstvo stanovuje normatívy finančných prostriedkov pre školy [[30]](#footnote-30). Napr. pre základnú školu je normatív celkových nákladov 2516 € na žiaka na rok (žiako-rok). Časový rozsah výučby je uvedený v rámcových učebných plánoch pre jednotlivé typy škôl [[31]](#footnote-31).

V jednoduchom modeli nech cca. 1250 hodín je ročná vzdelávacia aktivita žiaka (10 mesiacov), čiže v zmysle normatívu na jednu žiako-hodinu je rátaný náklad 2 €. Týmto je možné prepojiť časovú a finančnú škálu dopadov.

### Klasifikácia dopadov podľa kvalitatívnej škály

V zmysle metodiky NBÚ [[32]](#footnote-32).

**Klasifikácia dopadov podľa kvalitatívnej škály pre školu**

1. **Zanedbateľný dopad** 
   1. žiadny vplyv narušenia na kvalitu poskytovanej vzdelávacej služby
   2. dopad je akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov
2. **Minimálny dopad** 
   1. malý vplyv narušenia na kvalitu poskytovanej vzdelávacej služby
   2. malé reputačné riziko
   3. dopad neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi
3. **Stredný dopad** 
   1. stredný vplyv narušenia na kvalitu poskytovanej vzdelávacej služby
   2. stredné reputačné riziko
   3. dopad neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje mimoriadne personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu)
4. **Závažný dopad** 
   1. Strednodobé prerušenie chodu školy
   2. vážne narušenie chodu školy
   3. prerušenie vyučovania vo viacerých triedach
   4. vážne narušenie reputácie školy
   5. potreba hľadania núdzového riešenia (napr. náhradné vyučovanie)
   6. prerušenie výkonu určitej konkrétnej vzdelávacej služby alebo spôsobenie preukázateľného narušenia bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie dôsledkov, resp. prerušenie stredne významných činností,
5. **Katastrofický dopad** 
   1. dlhodobé prerušenie chodu školy
   2. kritické reputačné riziko
   3. zásadné ohrozenie výkonu a funkčnosti primárnych procesov vzdelávania, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej školy.

**Klasifikácia dopadov podľa kvalitatívnej škály pre žiakov / rodičov**

1. **Zanedbateľný dopad** 
   1. žiadny vplyv narušenia na kvalitu a dostupnosť služieb vzdelávania pre žiaka
   2. žiadny negatívny vplyv na vzdelávanie a psychický stav žiaka
2. **Minimálny dopad** 
   1. malý vplyv narušenia na kvalitu a dostupnosť služieb vzdelávania pre žiaka
   2. malý negatívny vplyv na činnosť a psychický stav žiaka
   3. výpadok vo výučbe, ktorý je ľahko dobehnuteľný
3. **Stredný dopad** 
   1. stredný vplyv narušenia na kvalitu a dostupnosť služieb vzdelávania pre žiaka
   2. Stredný negatívny vplyv na vzdelávanie a psychický stav žiaka
   3. Výpadok časti učiva, ktorý nie je nahradený
   4. Zhoršenie známok podmienené narušením dostupnosti vzdelávacích služieb.
4. **Závažný dopad** 
   1. Závažný vplyv narušenia na kvalitu a dostupnosť služieb vzdelávania pre žiaka
   2. Závažný negatívny vplyv na vzdelávanie a psychický stav žiaka
      1. Strach chodiť do školy
      2. Významný pokles vzdelávacích aktivít na úrovni žiaka
   3. Výpadok významnej časti učiva, ktorý nie je nahradený (mesiac a viac)
   4. Dlhodobé prerušenie dostupnosti vzdelávacích služieb školy pre žiaka
   5. Zhoršenie známok podmienené narušením dostupnosti vzdelávacích služieb.
5. **Katastrofický dopad** 
   1. Katastrofický vplyv narušenia na kvalitu a dostupnosť služieb vzdelávania pre žiaka
   2. Mimoriadne závažný negatívny vplyv na psychický stav žiaka
      1. Hospitalizácia
      2. Pokus o samovraždu
   3. Dlhodobé prerušenie dostupnosti služieb vzdelávania pre žiaka školy
   4. Strata školského roka (opakovanie ročníka, predčasné ukončenie štúdia)

### Dopady na školy

**Možné nepriaznivé scenáre bezpečnostných incidentov** (aj mimo KB) vedúce k výpadkom vo vzdelávacom procese:

**Škola**

Vyučovacia hodina triedy (IKT)

* Výpadok pedagóga (nedôjde do školy, napr. pri OČR)
* Masívne meškanie MHD
* Nepripravený HW / SW na hodinu
* Výpadok HW alebo SW na úrovni triedy ako celku
* Výpadok prúdu
* Napadnutie počítačovej učebne malvérom
* Zlomyseľná činnosť žiakov

Vyučovací deň triedy alebo hodiny viacerých tried

* Výpadok skupiny pedagógov
* Masívne meškanie MHD
* Pandemické voľno triedy (napr. je 16 žiakov chorých)
* Výpadok prúdu
* Napadnutie počítačovej učebne malvérom
* Hacknutie počítačovej učebne
* Fyzický útok na žiaka / učiteľa

Vyučovací deň školy alebo väčšieho počtu tried

* Vyhrážka bombou
* Riaditeľské voľno
* Pandemické voľno školy (počas chrípkovej epidémie)
* IKT narušenie v počítačových učebniach
* Fyzický útok na žiaka / učiteľa s následkom smrti
* Kalamita (napr. snehová)
* Nutnosť opakovať maturity / prijímacie skúšky na škole

Vyučovací týždeň školy alebo väčšieho počtu tried

* Dlhšie IKT narušenie v počítačových učební (malvér)
* Pandemické voľno školy (napr. počas chrípkovej epidémie)
* Séria vyhrážok bombou
* Požiar v škole
* Vytopenie alebo zaplavenie školy
* Rozhodnutie Úradu verejného zdravotníctva (hygiena)

Vyučovací mesiac školy

* Vážne poškodenie objektu školy (napr. po požiari, vytopení)
* Pandémia (ako to bolo počas COVIDu)
* Rozhodnutie Úradu verejného zdravotníctva (hygiena)
* Radiačné zamorenie územia (napr. v blízkosti JE)

Školský rok

* Pandémia (ako to bolo počas COVIDu)
* Radiačné zamorenie územia (napr. v blízkosti JE)
* Vojnový stav

**Školy**

Vyučovací deň väčšieho počtu škôl

* Vyhrážky bombou veľkému počtu škôl
* Ostrý štrajk učiteľov
* Pandemické voľno pre školy (napr. počas chrípkovej epidémie)
* Masívny hackerský útok na IKT infraštruktúru škôl

Vyučovací týždeň väčšieho počtu škôl

* Dlhšie IKT narušenie počítačových učební (malvér)
* Pandemické voľno školy (počas chrípkovej epidémie)
* Séria vyhrážok bombou

Vyučovací mesiac veľkého počtu škôl

* Pandémia (ako to bolo počas COVIDu)
* Radiačné zamorenie územia (napr. v okolí JE)

Školský rok veľkého počtu škôl

* Pandémia (ako to bolo počas COVIDu)
* Radiačné zamorenie územia (napr. v okolí JE)
* Vojnový stav

Ako kvantitatívnu škálu používame ohodnotenie straty vyučovacích hodín

|  |  |  |  |
| --- | --- | --- | --- |
| **Rozsah výpadku** | **Kvalitatívne** | **Kvantitatívne** (strata času) | **Slovný popis dopadu** |
| 5 – 30 min.  *Trieda* | 1 | 2 | V triede sa narušila časť vyučovacej hodiny (napr. pri výučbe s IKT vypadol prúd) |
| 45 – 180 min.  *Trieda* | 2 | 3 | Narušilo sa viacero hodín triedy, alebo hodina viacerých tried (napr. v dôsledku výpadku prúdu) |
| 6 hodín  *Trieda* | 3 | 3 | V daný deň sa nekonala výučba v danej triede (napr. pri riešení aktuálnej vážnej šikany, alebo pri chrípkovej epidémii) |
| 6 hodín  *Škola* | 4 | 4 | V daný deň sa nekonala výučba v škole (napr. po nahlásení bomby). Žiaci mali náhradné dištančné vzdelávanie alebo náhradné voľno. So žiakmi nižších ročníkov ZŠ musia zostať doma rodičia. |
| 6 hodín  *Veľký počet škôl (100+)* | 5 | 8 | Vo veľkom počte škôl sa neučilo (napr. po nahlásení bomby). Žiaci mali náhradné dištančné vzdelávanie alebo náhradné voľno. So žiakmi nižších ročníkov ZŠ musia zostať doma rodičia. |
| Týždeň  *Trieda* | 4 | 6 | Trieda sa týždeň neučila, alebo viacero tried sa deň neučilo, napr. v dôsledku chrípkových prázdnin. |
| Týždeň  *Škola* | 4 | 7 | V škole sa týždeň neučilo. Žiaci mali náhradné dištančné vzdelávanie alebo náhradné voľno alebo chrípkové prázdniny. So žiakmi nižších ročníkov ZŠ musia zostať doma rodičia. |
| Týždeň  *Všetky školy* | 5 | 10 | Vo veľkom počte škôl sa neučilo (napr. chrípkové prázdniny). Žiaci mali náhradné dištančné vzdelávanie alebo len samostatnú prácu doma. So žiakmi nižších ročníkov ZŠ musia zostať doma rodičia. |
| Mesiac  *Škola* | 5 | 9 | Celý mesiac sa v škole neučilo. Boli nutné náhradné postupy – dištančné vzdelávanie. |
| Mesiac  *Všetky školy* | 5 | 11 | Celý mesiac sa v školách neučilo. Boli nutné náhradné postupy – dištančné vzdelávanie (nedostupné pre 100.000+ žiakov, viď správa ministerstva o COVIDe). |
| Školský rok  *Všetky školy* | 5 | 12 | Celý rok sa v školách neučilo. Boli nutné náhradné postupy – dištančné vzdelávanie (nedostupné pre 100.000+ žiakov, viď správa ministerstva o COVIDe). |

### Dopady na žiaka

Ako kvantitatívnu škálu používame ohodnotenie straty vyučovacích hodín

|  |  |  |  |
| --- | --- | --- | --- |
| **Rozsah výpadku** | **Kvalitatívne** | **Kvantitatívne** (strata času) | **Slovný popis dopadu** |
| 5 – 30 min. | 1 | 2 | Časť vyučovacej hodiny bola narušená. |
| 45 – 180 min. | 2 | 3 | Narušilo sa viacero hodín triedy žiaka. |
| Deň | 2 | 3 | V daný deň sa nekonala výučba v danej triede žiaka alebo žiak deň chýbal (napr. zo zdravotných dôvodov). |
| Týždeň | 3 | 4 | Trieda sa týždeň neučila (napr. pre chrípkové prázdniny) alebo žiak týždeň chýbal (ochorenie, prázdniny s rodičmi). |
| Mesiac | 4 | 5 | Mesiac sa v škole neučilo, alebo žiak bol dlhodobo chorý. |
| Školský rok | 5 | 5 | Celý rok sa v škole neučilo. Boli nutné náhradné postupy – dištančné vzdelávanie (nedostupné pre 100.000+ žiakov, viď správa ministerstva o COVIDe). |

## Špecifické oblasti hrozieb, zraniteľností, rizík

V tejto kapitole sú uvedené podrobnejšie prehľady špecifických hrozieb a zraniteľností pre vybraná aktíva alebo oblasti. Pre dané hrozby je ohodnotené riziko. Hodnotenie rizík je generické a slúži ako východiskový podklad pre hodnotenie rizík v konkrétnej situácii / škole / domácnosti.

### Hrozby pre vzdelávací proces

Tieto hrozby sa týkajú priamo možných narušení vzdelávacieho procesu. Okrem IKT sú aj zdroje ďalších možných narušení. Patria tu najmä:

1. Výpadok dostupnosti IKT potrebných pre výučbu a následné narušenie výučby
   1. Výpadok internetového pripojenia
   2. Technická porucha zastaralého počítača
   3. Ukradnutie častí IKT (napr. pevného disku)
   4. Výpadok napájania
   5. Hackerský útok
   6. Napadnutie malvérom
   7. Zásahy žiakov do HW a SW
   8. Výpadok služieb tretích strán
2. Narušenie IKT pri vyučovaní
   1. Neúmyselná chyba študentov
   2. Úmyselná zlomyseľná činnosť študentov
   3. Poškodenie počítača (napr. pri jeho zhodení alebo zakopnutí)
   4. Nevhodne zvolená digitálna technika a jej použitie na danú vyučovaciu hodinu.
   5. Zastaralé technické vybavenie
3. Narúšanie vyučovacieho procesu mobilom / inteligentnými hodinkami žiaka
   1. Nesústredenosť
   2. Prezeranie obsahu namiesto aktívnej účasti na vyučovaní
   3. Vyrušovanie spolužiakov pri zvonení mobilu
4. Zneužívanie AI pri samostatnej práci a zadaniach
   1. Prezentácia AI výstupov ako vlastných
   2. Obmedzenie vlastných kognitívnych aktivít
5. Nesprávne alebo nadmerné využívanie IKT na vyučovacích hodinách zo strany učiteľa
   1. Nepostačujúca úroveň prípravy pedagógov pre správne využívanie IKT vo vyučovacom procese
   2. Nepripravenosť pedagóga pre správne využitie IKT na hodine
   3. Nadmerné púšťanie prezentácií (PowePoint) alebo videí na úkor iných samostatných aktivít
   4. Technická nepripravenosť IKT na hodinu (z nej odoberá cenné minúty)
   5. Nevhodný koncept využívania IKT na hodine, ktorý vedie žiakov k únikovým aktivitám.
6. Narušenie podporných služieb výchovno-vzdelávacieho procesu
   1. Narušenie služieb tretích strán pre vzdelávací proces (výpado EduPage).
   2. Narušenie IKT podpory kritických procesov chodu školy (prijímacie skúšky, maturity).
   3. Narušenie IKT podpory dôležitých procesov chodu školy (triedna kniha, zastupovanie, dochádzka, klasifikácia, komunikácia so žiakmi a rodičmi – typicky cez EduPage).
7. Personálne zdroje narušenia výchovno-vzdelávacieho procesu
   1. Odchod učiteľov počas školského roka.
   2. Chýbajúci kvalifikovaní učitelia.
   3. Dlhodobý výpadok učiteľa (choroba – napr. dostal čierny kašeľ od žiaka)
   4. Výpadok učiteľov počas pandémie (napr. chrípkovej)

**Posúdenie miery rizika**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 1.1 | Výpadok dostupnosti IKT potrebných pre výučbu | K | N | S |
| 1.2 | Narušenie IKT pri vyučovaní | S | S | S |
| 1.3 | Narúšanie vyučovacieho procesu mobilom žiaka | Z | VV | **VV** |
| 1.4 | Zneužívanie AI pri samostatnej práci a zadaniach | Z | S | **V** |
| 1.5 | Nesprávne alebo nadmerné využívanie IKT na vyučovacích hodinách zo strany učiteľa | S | N | S |
| 1.6 | Narušenie podporných služieb výchovno-vzdelávacieho procesu | K | VN | S |
| 1.7 | Personálne zdroje narušenia výchovno-vzdelávacieho procesu | Z | S | **V** |

### Hrozby týkajúce sa porušenia ochrany osobných údajov na škole

Porušovanie zákona o ochrane osobných údajov (nevedomé / vedomé):

1. Chýbajúce povinné informácie o ochrane OÚ na webe školy.
2. Chýbajúca riadiaca dokumentácia k práci s osobnými údajmi (pre pedagógov aj nepedagogických pracovníkov)
3. Právny základ pre spracovanie OÚ je
   1. nesprávne určený
   2. chýbajúci
4. Nedoriešené právne vzťahy s dodávateľmi SW pre školy (ako je EduPage)
   1. Dodávateľ je aj sprostredkovateľom
   2. Zabezpečenie plnenia povinností sprostredkovateľa
5. Chýbajúce súhlasy pre spracovanie OÚ, kde je to legislatívne požadované
6. Nejasný rámec a chýbajúce nástroje na uplatňovanie práv nositeľov osobných údajov, napr.
   1. Právo na prenositeľnosť údajov
   2. Právo na opravu údajov
   3. Právo na obmedzené spracovanie údajov
   4. Právo na vymazanie údajov
   5. Právo na zabudnutie
   6. Právo vzniesť námietku
   7. Právo podať sťažnosť
7. Realizácia spracovateľských operácií, ktoré nie sú v súlade s GDPR, najmä
   1. Sprístupnenie osobných údajov o žiakoch
      1. neoprávneným osobám (učitelia, žiaci, rodičia detí nad 18 rokov)
      2. na EduPage v časti prístupnej neoprávneným osobám
      3. na nástenkách školy
      4. na počítačoch učiteľov a ich obrazovkách
      5. v počítačových učebniach
      6. priamo na Internete
         1. školou
         2. pedagógmi
         3. samými žiakmi (napr. školský časopis)
   2. Monitoring počítačových učební a priestorov
   3. Nesprávna archivácia a skartácia OÚ
   4. Neoprávnený zber a spracovanie osobných údajov
      1. Fotografovanie ale najmä natáčanie učiteľov na hodinách
      2. Fotografovanie alebo najmä natáčanie žiakov učiteľmi
      3. Zverejnenie videí zo školského prostredia na sociálnych sieťach
8. Nesprávne nakladanie s osobitnou kategóriou osobných údajov
9. Nepostačujúca úroveň legislatívne požadovanej ochrany OÚ
10. Ďalšie porušenie zákona

**Posúdenie miery rizika**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 2.1 | Chýbajúce povinné informácie o ochrane OÚ na webe školy. | N | N | N |
| 2.2 | Chýbajúca riadiaca dokumentácia k práci s OÚ | S | S | S |
| 2.3 | Nesprávny alebo chýbajúci právny základ pre spracovanie OÚ | S | N | S |
| 2.4 | Nedoriešené právne vzťahy s dodávateľmi SW pre školy (ako sprostredkovateľmi) | S | S | S |
| 2.5 | Chýbajúce súhlasy pre spracovanie OÚ, kde je to legislatívne požadované | S | S | S |
| 2.6 | Nejasný rámec a chýbajúce nástroje na uplatňovanie práv nositeľov osobných údajov | S | N | S |
| 2.7 | Realizácia spracovateľských operácií, ktoré nie sú v súlade s GDPR | S | S | S |
| 2.8 | Nesprávne nakladanie s osobitnou kategóriou osobných údajov | Z | N | S |
| 2.9 | Nepostačujúca úroveň legislatívne požadovanej ochrany OÚ | Z | N | S |

### Hrozby pre finančné aktíva

Tieto hrozby sa týkajú finančných aktív žiaka / rodiny v oblasti hrozieb súvisiacich s kybernetickým priestorom.

1. Zneužitie internetového platobného prostriedku žiaka / rodičov s následným neoprávneným použitím finančných prostriedkov útočníkom
2. Nekontrolované internetové nakupovanie zo strany žiaka, prípadne jeho rodičov, napr.
   1. Všeobecné nakupovanie
   2. Virtuálne predmety do počítačových hier
   3. Špecifické platené služby napr. OnlyFans
3. Internetové platby za tovar s neadekvátnym plnením
   1. Nedodaný tovar
   2. Dodaný tovar v inej, nízkej kvalite alebo vecnom plnení
4. Prekročenie dátových limitov s následným vysokým poplatkom (najmä na mobile)
   1. Dátové prenosy
   2. Prevolané minúty
   3. Rooming v zahraničí
5. Volanie na čísla s platenými službami
   1. Spoplatnené spätné volania
   2. Využívanie platených služieb (erotické, veštenie a pod.)
6. Rizikové investície rodiny na základe psychologickej manipulácie alebo stavu núdze, napr.
   1. Do kryptomien
   2. Do iných aktív
   3. Využívanie financií nebankových spoločností, napr.
      1. Založenie bytu ako ručenie
7. Finančné podvody na členoch rodiny, napr.
   1. Psychologická manipulácia pre zaslanie financií na účet podvodníka, napr.
      1. rámci zoznamovacích aktivít (pomoc fiktívnemu partnerovi)
      2. poplatky pri fiktívnom dedení (úmrtie bohatej osoby)
   2. Oznámenie o nehode spôsobenom príbuzným a požiadavka na financie
8. Manipulatívne požiadavky na financie (platba je dobrovoľná), napr.
   1. Uzavretie nevýhodných zmlúv
   2. Tovar na splátky
   3. Platby za neobjednaný tovar
9. Hazard v kybernetickom priestore
   1. Elektronické stávkové kancelárie
   2. Elektronické kasína (poker, ruleta a pod.)
   3. Lootboxy a mysteryboxy v počítačových hrách
   4. Iné
10. Chyby pri realizácii platobnej operácie
    1. Zaslanie financií na chybný účet

**Posúdenie miery rizika**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 3.1 | Zneužitie internetového platobného prostriedku žiaka / rodičov | Z | S | **V** |
| 3.2 | Nekontrolované internetové nakupovanie zo strany žiaka, prípadne jeho rodičov | S | N | S |
| 3.3 | Internetové platby za tovar s neadekvátnym plnením | S | VN | N |
| 3.4 | Prekročenie dátových limitov s následným vysokým poplatkom (najmä na mobile) | S | VN | N |
| 3.5 | Volanie na čísla s platenými službami | S | VN | N |
| 3.6 | Rizikové investície na základe psychologickej manipulácie | K | VN | S |
| 3.7 | Finančné podvody na členoch rodiny | Z | N | S |
| 3.8 | Manipulatívne požiadavky na financie | Z | VN | N |
| 3.9 | Hazard v kybernetickom priestore | K | N | S |
| 3.10 | Chyby pri realizácii platobnej operácie | Z | VN | N |

### Hrozby pre reputáciu a osobnú integritu

(dobré meno / reputáciu / osobnú integritu / postavenie / čistý register trestov)

Reputácia osoby môže byť narušená množstvom spôsobov. Špecifikum kybernetického priestoru sú digitálne stopy vykonávaných aktivít. Napr. na politikov sa vyťahujú nevhodné výroky, ktoré na nejakom fóre povedali pre desiatimi aj viacerými rokmi a ktoré aktuálne by už nepovedali.

Reputácia môže byť narušená vlastnou chybou alebo úmyselnou nepriateľskou činnosťou iných osôb (napr. deepfake video). Najčastejšie spôsoby:

1. Nevhodné výroky, správanie, príspevky, komunikácia
   1. Na sociálnej sieti v rámci svojho účtu
   2. Na svojom webovom sídle
   3. V rámci svojej publikačnej činnosti
   4. SMS komunikácia
   5. Hlasová telefonická komunikácia
   6. Mailová komunikácia

*Poznámka: citácia týchto výrokov a príspevkov v budúcnosti môže v dospelosti spôsobiť osobe vážne problémy v zamestnaní aj komunite. Digitálna stopa na internete je veľmi silná a trvácna.*

1. Medializované nevhodné výroky, správanie, komunikácia, aktivity osoby
   1. V rámci diskusných fór (médiá, sociálne siete)
   2. Na sociálnej sieti v rámci svojho účtu
   3. Preposielaním obsahu od iných osôb
      1. Napr. pornografie
      2. Detskej pornografie
   4. Na svojom webovom sídle
   5. V rámci svojej publikačnej činnosti
   6. Videa z verejných vystúpení
   7. Privátne videá
   8. SMS komunikácia
   9. Hlasová telefonická komunikácia
   10. Mailová komunikácia

*Poznámka: citácia týchto výrokov a príspevkov v budúcnosti môže v dospelosti spôsobiť osobe vážne problémy v zamestnaní aj komunite.*

1. Získanie citlivých osobných údajov o osobe a ich zverejnenie útočníkom
   1. Zdravotné záznamy
      1. Zdravotné záznamy o osobe (diagnózy, lieky, vyšetrenia)
         1. Zdravotné záznamy o duševných alebo venerických chorobách
   2. Videá a fotografie
      1. fotografie nahých detí
      2. intímne situácie
      3. Sexting
      4. nevhodné správanie (napr. pod vplyvom alkoholu a iných drog)
      5. privátna komunikácia
      6. vytrhnuté z kontextu
      7. účelovo zostrihané videá
   3. Komunikácia, kde sú obsahom aj s osobné údaje
      1. SMS
      2. Chaty
      3. Video hovory
   4. Sociálne siete
      1. Privátne publikovaný obsah o sebe
   5. Informácie o realizovaných platbách za niektoré služby (napr. eskortné)
2. Zverejnenie ďalšieho digitálneho obsahu týkajúceho sa osoby
   1. Videá a fotografie
      1. vytrhnuté z kontextu
      2. účelovo zostrihané videá
   2. Komunikácia
      1. SMS
      2. Chaty
   3. Sociálne siete
      1. Publikovaný obsah
      2. Komentáre k iným príspevkom
   4. Informácie o kontaktoch s inými osobami
      1. Naznačovaná nevera
      2. Rizikoví obchodní partneri
      3. Závadové osoby
3. Fiktívny digitálny obsah súvisiaci s danou osobou (digitálny obsah, ktorý niekto vytvorí a prezentuje, že je to od danej osoby - fakes)
   1. Videá
      1. Deep fake videá (ťažko rozpoznateľná umelosť videa)
   2. Obrázky
      1. Deep fake obrázky
   3. Hlasové nahrávky
      1. Deep fake nahrávky
   4. Publikované texty
   5. SMS správy
   6. Fiktívne webové stránky
   7. **Fiktívne účty na sociálnych sieťach v mene danej osoby**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 4.1 | Nevhodné výroky, správanie, príspevky, komunikácia | S | S | **V** |
| 4.2 | Medializované nevhodné výroky, správanie, komunikácia, aktivity osoby | Z | N | S |
| 4.3 | Získanie citlivých osobných údajov o osobe a ich zverejnenie útočníkom | K | S | V |
| 4.4 | Zverejnenie ďalšieho digitálneho obsahu týkajúceho sa osoby | S | VN | N |
| 4.5 | Fiktívny digitálny obsah súvisiaci s danou osobou | K | S | **V** |

### Hrozby pre zdravie

Podrobnejšie informácie o hrozbách - viď kap. 2.2

1. Psychosociálne hrozby, najmä:
   1. **Nadmerné používanie digitálnych technológií**
   2. Nelátkové závislosti
   3. Narušenie sociálnych väzieb
   4. Problémy v socializácii
   5. Zahltenie negatívnymi emóciami zo sociálnych sietí
   6. Diskriminácia
   7. Útoky voči osobe v KP
   8. Dlhodobé sledovanie krátkych videí (TikTok, ale už aj Youtube)
   9. Dlhodobá pasívna konzumácia digitálneho obsahu
   10. Technoferencia (narúšanie vzťahu rodič - dieťa digitálnych technológiami)
   11. Vznik FOMO (fear of missing out): neustála potreba byť online a obava, že dieťa niečo zmešká, čo prispieva k psychickému vyčerpaniu.
   12. Porovnávanie vzhľadu, výkonu a pod. (body image, úspech...) s negatívnymi výsledkami
   13. Znížená schopnosť zvládať stres a frustráciu v reálnych situáciách
   14. Zhoršené schopnosti emocionálnej regulácie a zvládania konfliktov
   15. Vývoj antisociálnych alebo egocentrických postojov z online prostredí bez spätných väzieb.
   16. Vytváranie návyku neustáleho hľadania stimulácie a odmien (notifikácie, lajky, komentáre)
       1. Rastúca potreba intenzívnejšej stimulácie.
       2. Neschopnosť nudiť sa a závislosť od externých podnetov / vnemov
   17. Prežívanie úzkosti pri obmedzení prístupu k technológii (digitálny „hlad“)
   18. Znížená motivácia na vykonávanie iných (menej stimulujúcich) činností
   19. Znížená schopnosť sústredenia sa na úlohy s odloženou odmenou
   20. Rozptýlenie pri učení, multitasking ako návyk.
   21. Oslabenie kritického myslenia – prijímanie neoverených informácií
   22. Zníženie schopnosti písomného a jazykového prejavu (dôsledok auto-korekcie, diktovania a vizuálneho písania)
2. Stres a frustráciu vyvolávajúci digitálny obsah
   1. Zvýšený výskyt úzkostných porúch a depresie u používateľov sociálnych sietí
   2. Seba-prezentácie iných osôb ako super-úspešných spôsobujúce stres (napr. fotografie na Instagrame, na iných sociálnych sieťach)
   3. Narušenie sebahodnoty a telesného obrazu (body image) spôsobené porovnávaním so „zdokonaľovanými“ online identitami
   4. Agresia od iných osôb v komunikácii
   5. Mikroagresia od iných v komunikácii
   6. Digitálne obťažovanie
   7. Provokácie na vyvolanie negatívnej odozvy
      1. Videom
      2. Diskusným príspevkom
      3. Chatom
      4. Mailom
      5. Telefonickým kontaktom
   8. Počítačové hry
      1. Pay-for-win
      2. Pay-for-social status
3. Nevhodný / škodlivý digitálny obsah
   1. Nadmerné prezentované násilie
   2. Sexuálny obsah
      1. Idealizovaný
      2. Nevhodný
      3. Zvrhlý
   3. Obsah podnecujúci k
      1. Diskriminácii
      2. Radikalizácii
      3. Násiliu
      4. Vylúčeniu
      5. Prezentujúci dominanciu voči ženám ako správny postoj
   4. Zdieľanie intímnych fotografií alebo videí („nudes“) a ich následné zneužitie (revenge porn)
      1. „Catfishing“ a manipulácia cez falošné identity
      2. Online groomovanie a nábor do rizikových komunít (napr. pro-ana fóra, incel skupiny, manosféra, femosféra, extremistické fóra)
      3. Tvorba a zdieľanie nelegálneho obsahu (napr. deepfake pornografie)
   5. Dezinformácie o zdraví a výžive
   6. Neodborné rady influencerov, AI
4. Nezdravý životný štýl v dôsledku nadmerného používanie digitálnych technológií
   1. Narušenie zdravého fyzického vývoja dieťaťa
      1. Nedostatok spánku
      2. Prerušovanie spánku notifikáciami a modrým svetlom
      3. Nedostatok pohybu
      4. Narušenie funkcionality orgánových systémov
      5. Obezita
   2. Civilizačné choroby
5. Digitálny obsah navádzajúci na zdraviu škodlivú aktivitu (najmä TikTok výzvy), napr.
   1. Sebapoškodzovanie
   2. Dusenie sa igelitovým sáčkom
   3. Lízanie záchodových mís
   4. Prehĺtanie magnetov
   5. Konzumácia liekov (napr. Panadolu)
   6. Nevhodné diéty
   7. Extrémne chudnutie
   8. Konzumácia anabolík, steroidov
6. Narušenie mentálnych schopností
   1. Znížená schopnosť učiť sa, udržiavať pozornosť
   2. Impulzivita a problémo vé správanie v dôsledku hyperstimulácie mozgu
   3. Prestimulovanosť podnetmi, informačná preťaženosť a s tým spojená únava, stres
   4. Strata schopnosti čítania s porozumením pre zložitejšie texty
   5. Zníženie schopnosti fyzickej komunikácie

**Ohodnotenie pravdepodobnosti / očakávania / možnosti realizácie hrozby**

V hodnotení rizík verejného zdravia sa používa namiesto pravdepodobnosti prevalencia negatívneho javu / hrozby v populácii.

Populácia žiakov (k 15.9.2024 [[33]](#footnote-33)):

Ročník 1 – 4: 213.898

Ročník 5 – 9: 233.859

ZŠ spolu: 447.757

SŠ: cca. 215.000

Celkovo: **cca. 662.000 žiakov**

Prevalencia 10 % znamená, že u 10 % detí (66.200 a viac) sa prejavil negatívny jav resp. realizovala hrozba; náhodne vybrané dieťa má 10 % pravdepodobnosť, že sa ho hrozba týka.

**Škála pre prevalenciu (pre účely tohto dokumentu)**

**VV:** veľmi vysoká - prevalencia negatívneho javu v detskej populácii je viac ako 15 % (99.000+ žiakov)

**V:** Vysoká - prevalencia negatívneho javu v detskej populácii je viac ako 5 % (33.000+ žiakov)

**S:** stredná - prevalencia negatívneho javu v detskej populácii je viac ako 1 %. (6.600+ žiakov)

**N:** nízka - prevalencia negatívneho javu v detskej populácii je menej ako 1 % (pod 6.600 žiakov)

**VN**: veľmi nízka - prevalencia negatívneho javu v detskej populácii je menej ako 0,1 % (pod 660 žiakov)

**Ohodnotenie zdravotných dopadov**

Pre určenie miery rizika k jednotlivým hrozbám je potrebné ohodnotiť aj dopady, ktoré realizáciou hrozby môžu nastať. Zdravotné dopady sú iného charakteru ako IKT dopady, preto je potrebná pre tieto dopady samostatná škála.

Ohodnotenie je možné kvalitatívne a kvantitatívne. Kvalitatívne ohodnotenie je jednoduchšie, ale s menšou vypovedateľnou hodnotou.

Škála v zmysle metodiky MIRRI (pre IKT)

Obrázok, na ktorom je text, snímka obrazovky, číslo, písmo

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.

**Škála pre hodnotenie dopadov ( následkov) pre zdravie dieťaťa v zmysle škály MIRRI**

1. Zanedbateľný
   1. Žiadna zdravotná ujma
2. Minimálny
   1. Minimálna zdravotná ujma (napr. po nevyspatej noci pri hraní)
   2. Malé narušenie zdravia pri nadmernom používaní digitálnych technológií
3. Stredný
   1. Mierne narušenie zdravia na hranici diagnostikovania.
   2. Nezdravý životný štýl v dôsledku nadmerného využívania digitálnych technológií.
   3. Isté psychologické problémy (riešené na úrovni rodiny).
   4. Rast potenciálu vzniku chronického ochorenia.
4. Závažný
   1. Vznik nelátkovej závislosti
   2. Závažné psychologické problémy (riešené na úrovni psychológa alebo psychiatra)
   3. Obezita
   4. Rozvoj civilizačnej choroby súvisiacej s nezdravým životným štýlom
   5. Čiastková invalidita
5. Katastrofálny
   1. Diagnostikované závažné duševné ochorenia v priamej súvislosti s digitálnymi technológiami
   2. Celoživotné zníženie úrovne kognitívnych schopností
   3. Trvalá invalidita s ťažkým zdravotným postihnutím
   4. Úmrtie

**Posúdenie rizika pre skupiny hrozieb**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov skupiny hrozieb** | **Následok** | **Prevalencia** | **Riziko** |
| 5.1 | Psychosociálne hrozby | Z | VV | **VV** |
| 5.2 | Stres a frustráciu vyvolávajúci digitálny obsah | S | V | **V** |
| 5.3 | Nevhodný / škodlivý digitálny obsah | Z | S | **V** |
| 5.4 | Nezdravý životný štýl v dôsledku nadmerného používania digitálnych technológií | K | V | **VV** |
| 5.5 | Digitálny obsah navádzajúci na zdraviu škodlivú aktivitu | Z | N | S |

Ohodnotenie negatívnych dopadov digitálnych technológií na zdravie detí je publikované v aj májovom reporte ministerstva zdravotníctva USA [[34]](#footnote-34).

Celkové zhrnutie z tohto reportu, „The Crisis of Childhood Behavior in the Digital Ag*e*“, Section Three

*„Over the past four decades, American children have transitioned from an active, play-based childhood to a sedentary, technology-driven lifestyle, contributing to increases in chronic physical and mental health disease.*

Za posledné štyri desaťročia prešli americké deti z aktívneho detstva založeného na hre na sedavý životný štýl ovplyvnený technológiami, čo prispelo k nárastu chronických fyzických a duševných ochorení.

*Jonathan Haidt, a social psychologist and co-author of The Anxious Generation, terms this shift the “Great Rewiring of Childhood,” driven by increased screen time, reduced physical activity, and psychosocial stressors such as loneliness, chronic stress, and sleep deprivation“.*

Jonathan Haidt, sociálny psychológ a spoluautor knihy The Anxious Generation, nazýva tento posun „Veľkou zmenou nastavenia detstva“, ktorá je riadená zvýšeným časom stráveným pred obrazovkami, zníženou fyzickou aktivitou a psychosociálnymi stresormi, ako sú osamelosť, chronický stres a nedostatok spánku.

### Hrozby pre časový fond

Časový fond má 24 hodín denne, z neho si môžu nadmerne čerpať aktivity v KB.

Obmedzenie alokácie času kvôli digitálnym aktivitám na:

1. Spánok
2. Starostlivosť o telo
   1. Stravovanie a pitný režim
   2. Osobná hygiena
3. Škola a vzdelávanie
   1. Domáca príprava na hodiny
   2. Samostatné domáce aktivity (napr. projekty, odborné práce)
   3. Odborná prax
   4. Krúžky na rozvoj schopností
4. Fyzická sociálna interakcia
   1. Fyzická interakcia a aktivity s rovesníkmi
   2. Fyzický interakcia s inými osobami v reálnych životných situáciách
5. Voľnočasové aktivity
   1. Kultúra (kino, divadlo, koncerty)
   2. Vlastné tvorivé aktivity
   3. Fyzická práca
   4. Šport a pohyb

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 6.1 | Obmedzenie alokácie času na spánok | Z | V | **V** |
| 6.2 | Obmedzenie alokácie času na starostlivosť o telo | S | VN | N |
| 6.3 | Obmedzenie alokácie času na školu a vzdelávanie | Z | N | S |
| 6.4 | Obmedzenie alokácie času na fyzickú sociálnu interakciu | Z | V | **V** |
| 6.5 | Obmedzenie alokácie času na iné voľnočasové aktivity, napr. šport | Z | S | **V** |

### Vekovo špecifické hrozby

Tu neuvádzame všetky hrozby, ale len tie, ktoré sú vekovo špecifické.

**Členenie / etapizácia**

1. Pred počatím
   1. Nezdravý životný štýl budúcej matky v dôsledku pôsobenia digitálnych technológií so zdravotnými dopadmi
      1. Nedostatok spánku
      2. Nedostatok pohybu so zdravotnými následkami
      3. Psychosociálna nepohoda (napr. stres, kyberšikana, sexting)
      4. Neodborné rady a dezinformácie ohľadom výživy, životosprávy a pod.
      5. Ďalšie dopady
2. Prenatálne obdobie (plod)
   1. Zdravotné hrozby pre matku v dôsledku negatívneho pôsobenia digitálnych technológií s následným dopadom na plod
      1. Nezdravý životný štýl budúcej matky v dôsledku pôsobenia digitálnych technológií
         1. Nedostatok spánku
         2. Nedostatok pohybu so zdravotnými následkami
         3. Psychosociálna nepohoda (napr. stres, kyberšikana, sexting)
         4. Neodborné rady a dezinformácie ohľadom výživy, životosprávy a pod.
         5. Ďalšie dopady
      2. Nelátková závislosť na digitálnych technológiách
   2. Nepriame hrozby pre plod
      1. Možné narušenie zdravého vývoja plodu
      2. Možné epigenetické dopady.
3. Novorodenec (0 – 28 dní)
   1. Hrozby pre matku v dôsledku pôsobenia digitálnych technológií, ktorých dopady sa môžu týkať aj dieťaťa
      1. Nadmerné používanie digitálnych technológií
         1. Nedostatok spánku
         2. Nedostatok pohybu
         3. Nadmerné používanie digitálnych technológií so zdravotnými dopadmi (viď kap. 2.4).
      2. Nelátková závislosť na digitálnych technológiách
      3. Psychosociálna nepohoda prenášajúca sa na dieťa
         1. Stres zo sociálnych sietí
         2. Porovnávanie sa s inými
         3. Pocity viny
      4. Neodborné rady a dezinformácie ohľadom výživy, životosprávy a pod.
   2. Špecifické hrozby pre novorodenca
      1. Rušivé podnety digitálnych technológií (hlasná hudba, bežiaca TV, počítač)
      2. Emocionálne neprítomná matka
      3. Nedostatok komunikačných podnetov zo strany matky
      4. Negativne ovplyvnenie procesu vzťahovej väzby
      5. Narušenie budovania väzby medzi matkou a dieťaťom v dôsledku častej technoferencie (napr. pri dojčení, kŕmení alebo uspávaní)
      6. Ďalšie obmedzenie alebo narušenie starostlivosti o novorodenca
4. Dieťa (právne)
   1. Dojča (29 dní – 1 rok)
      1. Špecifické hrozby pre matku - detto ako u novorodenca
      2. Špecifické hrozby pre dojča
         1. Narušenie tvorby vzťahovej väzby
         2. Nedostatok komunikačných a emocionálnych reakcií a podnetov zo strany matky
         3. Rušivé podnety digitálnych technológií (hlasná hudba, bežiaca TV, počítač)
         4. Možné narušenie psychomotorického vývoja
         5. Obmedzenie alebo narušenie starostlivosti o dieťa
         6. Počiatky sledovania TV / videa (napr. pri kŕmení)
         7. Nesprávne stravovacie návyky

Hrozby pre rodičov ostávajú, ako boli horeuvedené. Ďalej uvádzame hrozby pre dieťa

* 1. Špecifické hrozby pre batoľa (od 1 roka do 3 rokov)
     1. Nedostatok komunikačných a emocionálnych reakcií a podnetov a emocionálnych reakcií a podnetov zo strany rodičov
     2. Negatívne ovplyvnenie tvorby vzťahovej väzby
     3. Možné narušenie psychomotorického vývoja
     4. Obmedzenie alebo narušenie starostlivosti o dieťa
     5. Nadmerné sledovania TV / videa
     6. Rušivé podnety digitálnych technológií (hlasná hudba, bežiaca TV pri zaspávaní, počítač)
     7. Nesprávne stravovacie návyky
     8. Znížená pozornosť a schopnosť samoregulácie (zvýšené vystavenie obrazovkám znižuje kapacitu dieťaťa rozvíjať pozornosť a sebareguláciu)
     9. Budovanie raných parasociálnych väzieb (vzťahov k postavám na obrazovke) namiesto reálnych väzieb so živou osobou
     10. Oslabenie vývinu exekutívnych funkcií (pamäť, plánovanie, inhibícia) v dôsledku nadmerného času pred obrazovkou.
     11. Obmedzenie rozvoja jazyka a komunikačných zručností v dôsledku zníženého počtu konverzačných obratov medzi rodičom a dieťaťom.
     12. Závislosť na mediálnom obsahu ako forma sebaupokojenia (napr. na zaspávanie alebo pri záchvatoch hnevu)
  2. Predškolský vek (3 - 6 rokov)

*Detto ako u batoľaťa plus*

* + 1. Nevhodné používanie digitálnych technológií
    2. Nadmerné používanie digitálnych technológií s dopadmi na zdravie (viď kap. 2.4)
    3. Predpoklady pre vznik nelátkových závislostí
    4. Možný nedostatok komunikačných a emocionálnych reakcií a podnetov zo strany rodičov.
    5. Možné narušenie psychomotorického vývoja
    6. Možné narušenie sociálneho rozvoja
    7. Obmedzenie alebo narušenie starostlivosti o dieťa zo strany rodičov
    8. Negatívny príklad rodičov s nevhodným využívaním digitálnych technológií
  1. Mladší školský vek (6 – 12 rokov)

*Detto ako u predškolského veku plus*

* + 1. Nevhodné využívanie mobilov a sociálnych sietí
    2. Možný vznik nelátkovej závislosti na digitálnych technológiách
    3. Digitálne vylúčenie, ak dieťa nevyužíva digitálne technológie ako rovesníci
    4. Znížená schopnosť sústredenia na vyučovaní
    5. Pomalý nábeh schopnosti čítať s porozumením
    6. Frustrácia a problémy s reguláciou správania
    7. Narušenie spánku v dôsledku používania technológií pred spaním
  1. Starší školský vek (12 – 15 rokov), začiatok puberty

*Detto ako u mladšieho školského veku*

* + 1. Negatívny vplyv sociálnych sietí
    2. Zanedbávanie vzdelávania a prípravy na pracovnú kariéru
  1. Adolescent (15 – 18 rokov, trestná zodpovednosť)

*Detto ako u staršieho školského veku*

* + 1. Závažné psychosociálne dopady sociálnych sietí
    2. Podceňovanie rizík súvisiacich s aktivitami v KP z hľadiska trestno-právnej zodpovednosti

1. Osoba blízka veku mladistvých (18-21, právne)

*Detto ako u adolescentov*

* 1. Obmedzenia schopností nadväzovať dlhodobejšie vzťahy
  2. Nezáujem o prípravu na náročné povolanie

1. Mladšia dospelosť (18/21 – 30) - obdobie mladého muža a ženy

*Naviac: Detto ako u osôb blízkych veku mladistvých*

* 1. Nezáujem o kariérny postup v zamestnaní
  2. Neschopnosť alebo nezáujem založiť si rodinu a mať deti (s prispením negatívneho pôsobenia digitálnych technológií – preferencia „mama hotelu“)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 7.1 | Pred počatím - nezdravý životný štýl budúcej matky v dôsledku pôsobenia digitálnych technológií | Z | VN | N |
| 7.2 | Prenatálne obdobie – zdravotné hrozby pre matku v dôsledku negatívneho pôsobenia digitálnych technológií s následným dopadom na plod | Z | N | S |
| 7.3 | Prenatálne obdobie – nepriame hrozby pre plod | Z | VN | N |
| 7.4 | Novorodenec - hrozby pre matku v dôsledku pôsobenia digitálnych technológií, ktorých dopady sa môžu týkať aj dieťaťa | Z | VN | N |
| 7.5 | Dojča - špecifické hrozby | Z | S | **V** |
| 7.6 | Batoľa - špecifické hrozby | K | S | **V** |
| 7.7 | Predškolský vek - špecifické hrozby | K | S | **V** |
| 7.8 | Mladší školský vek - špecifické hrozby | Z | S | **V** |
| 7.9 | Starší školský vek - špecifické hrozby | Z | S | **V** |
| 7.10 | Adolescent - špecifické hrozby | Z | V | **V** |
| 7.11 | Osoba blízka veku mladistvých - špecifické hrozby | Z | **V** | **V** |
| 7.12 | Mladšia dospelosť - špecifické hrozby | K | V | **VV** |

### Hrozby vo virtuálnych prostrediach

Sú to prostredia aplikácií, v ktorých je viacero (desiatky – miliardy) používateľov, ktorí môžu medzi sebou interagovať a vidia konanie, správanie iných používateľov.

1. **Negatívne vplyvy prostredia niektorých počítačových hier**
   1. Prostredie, ktoré podporuje:
      1. vznik nadmerného používania až závislosti na hre.
         1. Nadmerné trávenie času v hernom prostredí – zaujímavé prostredie a dej, veľa pozitívnych emócií, úspechov v hre ako lákadlo.
         2. Vznik závislosti na hre.
      2. nadmernú súťaživosť a porovnávanie (s prípadnou následnou podporu pay-to win predaja predmetov na zlepšenie pozície hráča)
         1. Tabuľky postavenia v hre (Leaderboards)
         2. Dosiahnuté úspechy (Achievements)
      3. vznik silnej komunity
         1. spoločné aktivity v skupine – Guild, Alliance, Kingdom, State
            1. sám hráč nič nedokáže, len v kolektíve
         2. spoločný boj proti iným skupinám
         3. podporujúca chatová komunikácia
         4. zdieľanie úspechov členmi
      4. vznik sociálneho statusu prostredníctvom nákupu
         1. virtuálnych predmetov, z ktorých majú úžitok aj iní členovia skupiny, ktorí to oceňujú
         2. vybavenia silných postáv, ktoré umožní zvíťaziť v súbojoch s inými a od toho sú závislí slabší členovia skupiny
   2. Nadmerné násilie v hre
      1. Detailné zobrazenie zabíjania, spôsobenia zranenia, reakcie napadnutých postáv nevhodné najmä pre mladšie deti.
         1. Napr. hry Postal 2, Manhunt, Resident Evil 7
         2. Novšie napr. simulácie prípadov zabíjania na školách v Robloxe.
      2. Sexuálne násilie.
      3. Široké možnosti spôsobovať herne neodôvodnené utrpenie iným (napr. nechať utopiť postavu v hre SIMS, totálne zabíjanie virtuálnych dedinčanov vrátane detí, mučenie).
   3. Tlak na financie
      1. Reklamy a ovplyvňovanie v prospech nákupu virtuálnych predmetov v hre.
         1. Obťažujúca reklama.
         2. Sofistikovaná reklama rôznych zliav a výhodných nákupov.
         3. Informácie o nákupoch u iných hráčov.
      2. Sociálna nerovnosť a jej dopady na psychiku (pay for win hry – kde bohaté dieťa je boss, ktorého všetci obdivujú)
      3. Vizualizácia bohatstva, napr. lepšie vyzerajúce postava, sídlo – stimuluje k nákupu.
      4. Pocit sociálnej vylúčenia alebo pocit menejcennosti (eLko – looser, NPC, socka) u hráča, ktorý má len základné, bezplatné vybavenie.
      5. Hazard v hrách – napr. loot boxy kupované za peniaze, z ktorých s malou pravdepodobnosťou vypadne vzácna herná vec
   4. Denné úlohy (quests), ktoré vytvárajú virtuálne povinnosti pre dieťa, ktoré sa ich snaží plniť aj na úkor iných aktivít.
   5. Dlhodobé používanie veľmi zjednodušeného jazyka v hernej komunikácii.
   6. Chat (komunikácia v hre):
      1. Používanie vulgarizmov.
      2. Urážanie hráča
      3. Mikrošikana.
      4. Diskriminácia.
      5. Sexuálne obťažovanie.
      6. Šírenie toxického obsahu – napr. vložením liniek na nevhodné webové stránky.
   7. Narušenie spánkového režimu spoločnými aktivitami v nevhodnom čase.
      1. V hre sú hráči z rôznych časových pásiem. Výber času pre spoločnú aktivitu môže byť v čase spánku dieťaťa. Neúčasť na spoločných aktivitách môže viesť vylúčeniu hráča z komunity (Guild, Alliance, State, Kingdom)
   8. Sexuálne obťažovanie (v chate hry, priamo v hre).
   9. Sociálne vylúčenie z kolektívu (reálny, virtuálny) / diskriminácia.
      1. ak dieťa nepozná a nehrá „cool“ hru – napr. Fortnite.
      2. ak dieťa nemá vhodné virtuálne predmety (napr. skins)
2. **Negatívne vplyvy prostredia niektorých sociálnych sietí** 
   1. Zneužitie účtu na sociálnej sieti inou osobou
      1. Narušenie integrity obsahu pod daným účtom
      2. Narušenie dôvernosti informácií pod daným účtom (napr. ak ide o privátnu skupinu)
      3. Strata obsahu (napr. úmyselné vymazanie)
      4. Publikovanie nevhodného obsahu akože danou osobou
      5. Nevhodná interakcia s priateľmi danej osoby
   2. Malvér
      1. Napadnutie danej aplikácie sociálnej siete malvérom
      2. Ďalšie šírenie malvéru
         1. Po napadnutí účtu
         2. Využitím sociálneho inžinierstva – osoba v dobrej viere sama šíri ďalej malvér (napr. cez publikované linky)
   3. Mechanizmy manipulácie a ovplyvňovania autonómie dieťaťa
      1. Sofistikované mechanizmy na zabezpečenie čo najdlhšieho času stráveného v prostredí danej sociálnej siete.
      2. Sledovanie správania a vytváranie behaviorálnych profilov
      3. Mikrocielenie obsahu na základe emočného stavu a minulých digitálnych aktivít
      4. Preferencia odporúčania negatívneho obsahu
      5. Tzv. „dark patterns“ - dizajnové stratégie manipulujúce používateľa k súhlasu / aktivite, ktorú by inak dieťa odmietlo
   4. Prostredie, ktoré podporuje vytvorenie nadmerného používania až závislosti na sociálnej sieti.
      1. Nadmerné trávenie času na sociálnej sieti.
      2. Vznik závislosti na sociálnej sieti.
         1. Algoritmické podsúvanie personalizovaného obsahu zvyšujúce mieru zotrvania na platforme (králičie nory),
         2. Princíp odmeňovania - posilňujú správanie cez dopamínové mechanizmy (podobne ako hazardné hry).
         3. Denná frekvencia interakcií so sieťou mimo hlavného času používania siete (napr. pozretie na nový príspevok, komentár – po zvukovom signáli alebo nutkavom pocite, napr. 30 krát za deň).
         4. Narúšanie koncentrácie na iné aktivity (napr. na vyučovanie).
   5. Negatívne komentáre k osobou zverejneným príspevkom (napr. na Facebooku).
      1. Znevažovanie obsahu príspevku
         1. nízka kvalita príspevku
         2. je to hlúposť, nezmysel, zbytočnosť
         3. spochybnenie pravdivosti príspevku
      2. Komentáre k osobe
         1. k jej fyzickým vlastnostiam (napr. postave)
         2. k jej psychickým danostiam (napr. že je psychopat, nepríčetný)
         3. k jej predchádzajúcim aktivitám a vyjadreniam
         4. k jej rase, vierovyznaniu, veku a iným danostiam
         5. fabulácia k jej motívom (napr. je to zradca Slovenska, zapredanec)
      3. Virtuálne útoky na osobu
         1. Nenávistné komentáre
         2. Vyhrážanie
         3. Zosmiešňovanie
         4. Kyberšikana
         5. Mikrošikana
   6. Negatívne komentáre k príspevkom iných osôb
      1. Detto ako v predchádzajúcom bode
   7. Porovnávanie sa s inými podľa ich príspevkov na sociálnej sieti (napr. fotografie na Instagrame, svedčiace o super živote danej osoby).
      1. Frustrácia z pocitu neúspešnosti, zaostávania a pod. (not so cool).
   8. Sociálne vylúčenie z kolektívu, ak dieťa nie je na sieti a ostatní spolužiaci áno.
      1. FOMO (Fear of Missing Out) - strach z premeškania dôležitej udalosti v komunite sociálnej siete.
   9. Toxický obsah prezentovaný na sociálnych sieťach a podsúvaný používateľovi ako preferovaný, odporúčaný obsah.
      1. Používajú sa na to tzv. Králičie nory a filtračné bubliny
      2. i. Dezinformácie a konšpirácie zdieľané virálne cez známe osoby alebo "influencerov"
      3. ii. Obsah zobrazujúci/glorifikujúci rizikové správanie (napr. samovraždy, poruchy príjmu potravy, extrémne výzvy)
3. **Negatívne vplyvy prostredia niektorých digitálnych médií** (osoba vystupuje ako prispievateľ, alebo komentuje príspevky)
   1. Negatívne komentáre k osobou zverejneným príspevkom (napr. v diskusii k článkom).
      1. Znevažovanie obsahu príspevku
         1. nízka kvalita príspevku
         2. je to hlúposť, nezmysel, zbytočnosť
         3. spochybnenie pravdivosti príspevku
      2. Komentáre k osobe
         1. k jej fyzickým vlastnostiam (napr. postave)
         2. k jej psychickým danostiam (napr. že je psychopat, nepríčetný)
         3. k jej predchádzajúcim aktivitám a vyjadreniam
         4. k jej rase, vierovyznaniu, veku a iným danostiam
         5. fabulácia k jej motívom (napr. je to zradca Slovenska, zapredanec)
      3. Virtuálne útoky na osobu
         1. Nenávistné komentáre
         2. Vyhrážanie
         3. Zosmiešňovanie
         4. Mikrošikana
         5. Kyberšikana
   2. Negatívne komentáre k príspevkom iných osôb
      1. Detto ako v predchádzajúcom bode
   3. Znižovanie kvality diskusie a motivácie prispievať
      1. Strach z reakcií, ktorý bráni vyjadriť svoj názor
      2. Prevládanie emocionality, polarizácie a tým úpadok argumentačnej kultúry (argumentačné fauly a pod.)
4. **Negatívne vplyvy virtuálnych svetov** (typu Metaverse, čiatočne aj Minecraft a Roblox), VR prostredia (helma alebo okuliare a SW)
   1. Nahrádzanie reálneho, fyzického sveta virtuálnym svetom.
      1. Skreslené vnímanie reality.
         1. Napr. „new game“ a „load from from last position“ v reálnom svete zvyčajne nefungujú.
   2. Sexuálne obťažovanie (v chate prostredia, priamo v prostredí – napr. virtuálne znásilnenie)
   3. Dlhodobé používanie zjednodušeného jazyka v komunikácii s inými avatarmi.
   4. Obťažujúca reklama.
   5. Mikrošikana.
   6. Diskriminácia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 8.1 | Negatívne vplyvy prostredia niektorých počítačových hier | Z | N | S |
| 8.2 | Negatívne vplyvy prostredia niektorých sociálnych sietí | Z | S | **V** |
| 8.3 | Negatívne vplyvy prostredia niektorých digitálnych médií | Z | S | **V** |
| 8.4 | Negatívne vplyvy virtuálnych svetov | Z | VN | N |

### Hrozby súvisiace s digitálnym vylúčením

Sú to hrozby, ktoré súvisia s tým, že nie všetky deti majú rovnaký potenciál prístupu k digitálnym technológiám, ku kvalitnej výučbe čo môže viesť k digitálnemu vylúčeniu (resp. digitálnej priepasti v zmysle dikcie Európskeho parlamentu [[35]](#footnote-35)).

*„Začiatkom 21. storočia sa tento termín začal používať hlavne na opis rozdelenia medzi ľuďmi s prístupom k internetu a bez neho a postupne, aj na opis rozdelenia medzi ľuďmi s prístupom k širokopásmovému pripojeniu a bez neho. Okrem fyzického prístupu k technológiám a zdrojom zahŕňa tento pojem aj potrebné zručnosti na efektívne využívanie informačno-komunikačných technológií.[[36]](#footnote-36).*

Príklad veľkého digitálneho vylúčenia (počas COVIDu):

„Výsledky prieskumov MŠVVŠ SR ukazujú, že 565 000 žiakov malo prístup k online výučbe. Učitelia považovali online formu výuky za najlepšiu alternatívu k bežnej výuke, napriek **tomu sa nepodarilo zaradiť do online výuky 128 000 žiakov (18,5 %)**. V školách s vysokým podielom žiakov zo sociálne znevýhodneného prostredia bol podiel žiakov, ktorí neboli pripojení na distančné vyučovanie najvyšší – 51,4 %. Najhoršie na tom boli špeciálne základné školy, ktoré majú najvyšší podiel žiakov zo sociálne znevýhodneného prostredia, kde **90 % žiakov neparticipovalo na online výuke**. [[37]](#footnote-37)

**Väčšina detí pochádzajúcich zo sociálne zraniteľných skupín neparticipovala na online vyučovaní, čím stratila takmer rok školskej dochádzky.** Vynechanie roku povinnej školskej dochádzky bude mať negatívny efekt na výšku príjmov v dospelosti. To znamená, že okrem iných prekážok budú v budúcnosti tieto deti ešte viac znevýhodnené než ich rovesníci, ktorí mali lepší prístup k (online) vzdelávaniu“.

1. **Digitálne vylúčenie detí zo sociálne znevýhodneného prostredia**

*Aj oponenti tejto témy by si mali uvedomiť, že dieťa za svoje znevýhodnené prostredie nemôže.*

Vymedzenie osoby zo sociálne znevýhodneného prostredia

* + - ktorej sa poskytuje pomoc v hmotnej núdzi a príjem rodiny je najviac vo výške životného minima,
    - v ktorej aspoň jeden z rodičov alebo osoba, ktorej je dieťa zverené do osobnej starostlivosti patrí do skupiny znevýhodnených uchádzačov o zamestnanie,
    - v ktorej najvyššie ukončené vzdelanie rodičov je základné, alebo aspoň jeden z rodičov nemá ukončené základné vzdelanie,
    - ktorá má neštandardné bytové a hygienické podmienky (napr. žiak nemá vyhradené miesto na učenie, nemá vlastnú posteľ, nie je zavedená elektrická prípojka a pod.)

Spôsob digitálneho vylúčenia

1. Chýbajúci alebo obmedzený prístup k digitálnym technológiám doma vedúci k možnému čiastočnému alebo plnému vylúčeniu v rámci reálnych aj virtuálnych komunít:
   1. v domácnosti nie je elektrina
   2. v domácnosti nie je internet
   3. v domácnosti nie je širokopásmový internet
   4. v domácnosti nie je počítač
   5. vekovo primerané dieťa nemá mobil
2. Chýbajúce základné znalosti a zručnosti
   1. všeobecné použitie
      1. počítača
      2. mobilu
   2. použitie kancelárskych aplikácií
   3. použitie špecializovaných aplikácií
   4. vyhľadávanie
   5. využívanie služieb na internete
   6. využívanie sociálnych sietí
3. **Digitálne vylúčenie detí so zdravotným znevýhodnením / postihnutím**

Kategorizácia niektorých zdravotných znevýhodnení je uvedená v kap. 2.3.

Podrobnejšie informácie sú napr. na webe Ministerstva práce, sociálnych vecí a rodiny [[38]](#footnote-38)

*„Zdravotné postihnutie môžeme definovať ako akúkoľvek duševnú, telesnú, dočasnú, dlhodobú alebo trvalú poruchu alebo handicap, ktorý* ***osobám so zdravotným postihnutím bráni prispôsobovať sa bežným nárokom života****. Zdravotné postihnutie zahŕňa množstvo funkčných obmedzení, ktoré sa vyskytujú v spoločnosti v každej krajine na svete. Môže byť telesné, psychické a kombinované.*

*Za fyzickú osobu s ťažkým zdravotným postihnutím (ďalej len osoba s ŤZP) sa považuje fyzická osoba, ktorej miera funkčnej poruchy je najmenej 50 % .*

*Funkčná porucha je nedostatok telesných schopností, zmyslových schopností alebo duševných schopností fyzickej osoby, ktorý z hľadiska predpokladaného vývoja zdravotného postihnutia bude trvať dlhšie ako 12 mesiacov.“*

V našom prípade ide o situáciu, keď školské aj domáce prostredie neposkytuje služby zohľadňujúce špecifiká znevýhodnenia (napr. pre zrakovo postihnutých). V rámci bežnej vyučovacej hodiny bez súčinnosti asistenta má učiteľ minimálny priestor.

Oblasti digitálneho vylúčenia

1. Chýbajúci alebo obmedzený prístup k digitálnym technológiám doma vedúci k možnému čiastočnému alebo plnému vylúčeniu v rámci reálnych aj virtuálnych komunít:
   1. V domácnosti nie je hardvér / softvér pre asistenčné technológie, podporujúci prácu s počítačom s ohľadom na zdravotné postihnutie dieťaťa (napr. čítačka obrazovky) [[39]](#footnote-39)
   2. Smartfón nemá podporu pre asistenčné technológie. Ten môže sa zmeniť na pomocníka aj pri čítaní, zisťovaní farieb a svetla, ale aj pri orientácii v priestore
   3. Rodičia nemajú postačujúce znalosti a schopnosti, ako sprístupniť takémuto dieťaťu digitálne technológie.
   4. Niektorí rodičia nemajú postačujúcu časovú kapacitu alebo vôľu pre sprístupňovanie digitálnych technológií takémuto dieťaťu.
   5. Obmedzené možnosti používania PC / smartfónu vedú k
      1. obmedzenému využívaniu prospešných aplikácií
      2. vylúčeniu z virtuálnych komunít spolužiakova a rovesníkov.
2. V škole
   1. Nie je hardvér / softvér pre asistenčné technológie, podporujúci prácu s počítačom s ohľadom na zdravotné postihnutie dieťaťa.
   2. Učiteľ nemá časovú kapacitu venovať sa týmto deťom naviac (ak nie je na hodine osobný asistent)
3. Chýbajúce alebo nepostačujúco rozvinuté základné znalosti a zručnosti
   1. všeobecné použitie
      1. počítača
      2. mobilu
   2. použitie kancelárskych aplikácií
   3. použitie špecializovaných aplikácií
   4. vyhľadávanie
   5. využívanie služieb na internete
   6. využívanie sociálnych sietí
4. **Digitálne vylúčenie detí v dôsledku nepostačujúcej školskej prípravy**

Ide o situáciu, keď školské vzdelávacie prostredie neposkytne postačujúcu úroveň prípravy s digitálnymi technológiami pre vzdelávanie, budúcu prax aj súkromný život žiaka (napr. málotriedka na dedine).

Často to prejaví pri prechode zo ZŠ na SŠ, kde časť detí okrem hrania a sociálnych sietí nevie v oblasti IKT skoro nič viac.

Niečo v menšom rozsahu býva aj pri prechode zo SŠ na VŠ. Často sa to prejavuje aj v rozdielnej úrovni vedomostí a zručností žiakov rôznych škôl rovnakého typu v prvom ročníku VŠ.

Významné výzvy v tejto oblasti sú minimálne tri:

* Správne nastavenie časovej dotácie
* Správne nastavenie kurikula v rámci časovej dotácie
* Zabezpečenie kvalifikovanej prípravy pedagógov pre nové technológie

Časté oblasti nepostačujúcej prípravy:

1. Všeobecná práca s počítačom *(ak dieťa ovláda mobil, neovláda automaticky počítač)*
   1. Základné ovládanie počítača
   2. Konfigurácia a nastavenia preferencií v OS
   3. Spúšťanie aplikácií, ak nie sú na lište
   4. Práca so súbormi (napr. kde je na disku stratený súbor?, uložiť súbor pod iným názvom do iného adresára a potom ho nájsť je občas vážny problém).
2. Použitie kancelárskych aplikácií
   1. textový editor (napr. ako používať štýly a vytvoriť obsah)
   2. tabuľkový kalkulátor (napr. spočítať priemer, formátovať bunky)
   3. prezentačný program (napr. včlenenie videí, timing slidov)
3. Vyhľadávanie na internete
4. Zmysluplné a bezpečné využívanie služieb na internete (napr. kúpa lístkov do kina, návod na opravu vodovodu, internetová platba za knihu)
5. Použitie špecializovaných aplikácií potrebných pre vybranú prax (napr. práca s grafikou)
6. Zmysluplné využívanie sociálnych sietí
7. Zmysluplné využívanie AI
8. **Digitálne vylúčenie detí v dôsledku vedomého obmedzenia prístupu k digitálnym technológiám**

Ide o situáciu, keď časť detí už má prístup k digitálnym technológiám a časť nie:

* mobil,
* hry,
* internet,
* sociálne siete

na prvom stupni ZŠ.

Ak sú deti bez súhlasu rodičov k prístupu k digitálnym technológiám vo výraznej menšine vedie to k ich digitálnemu vylúčeniu, prípadne aj klasickému vylúčeniu (nepatrí do okruhu priateľov, nemá spoločné záujmy - napr. nehrá Fortnite, nie je na Istagrame, nepozná trendy na Tik-toku).

Preto odpoveď na otázku – kedy povoliť digitálne technológie je netriviálna. Jednoduchšie je to vtedy, ak sa to rieši legislatívou – napr. v Austrália zakázali vybrané sociálne siete deťom do 16 rokov [[40]](#footnote-40) [[41]](#footnote-41).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 9.1 | Digitálne vylúčenie detí zo sociálne znevýhodneného prostredia | K | V | **VV** |
| 9.2 | Digitálne vylúčenie detí so zdravotným znevýhodnením / postihnutím | Z | S | **V** |
| 9.3 | Digitálne vylúčenie detí v dôsledku nepostačujúcej školskej prípravy | Z | N | S |
| 9.4 | Digitálne vylúčenie detí v dôsledku vedomého obmedzenia prístupu k digitálnym technológiám | Z | N | S |

### Hrozby súvisiace s možnosťami poznania

Teória poznania alebo gnozeológia je filozofická disciplína, ktorá sa zaoberá hľadaním odpovedí na problémy a otázky súvisiace s poznaním, najmä:

* Čo je to poznanie?
* čo sa poznanie opiera a ako je získavané?
* Aké sú možnosti a medze poznania?

Kybernetický priestor a jeho možnosti narúšajú staré istoty týkajúce sa poznania. Dopady sú nielen na deti, ale aj ich rodičov, ktorí prenášajú svoje poznanie na deti.

**Významné oblasti hrozieb:**

1. **Falošné (Fake) fotografie** 
   1. Sú to umelo aranžované reálne fotografie, pre ovplyvňovanie verejnej cieľovej skupiny (mládeže, náboženskej skupiny, politických prívržencov, aj bežných občanov). Často ich využíva propaganda a pokročilý marketing. Dieťa či rodič nie sú často schopní rozpoznať, že sú umelo aranžované.
   2. Sociálne siete a ďalšie digitálne médiá umožňujú ich rýchle šírenie.
   3. Množstvo emocionálnych komentárov pod obrázkom môže významne ovplyvniť osobu v akceptácii príbehu (napr. hoaxu), ktorý je s danou fotografiou spojený.
   4. Kvalitnými fake fotografiami s dôveryhodne vyzerajúcim príbehom je možné rýchlo a významným spôsobom v kybernetickom priestore ovplyvniť cieľové skupiny aj širokú verejnosť.
2. **AI generované falošné (Deepfake) fotografie**

*Tie sa dostali na úroveň, že dieťa, rodič nie sú často schopní rozpoznať, či sú umelo vytvorené.*

* 1. To vytvára množstvo následných hrozieb – napr. pre kompromitáciu osoby sexuálne orientovaným obrázkom, alebo plnenie účelov, aké sú uvedené pri fake fotografiách.
  2. Na druhej strane osoba môže poprieť svoj hovorený prejav s odkazom na deepfake verziu.
  3. Sociálne siete a ďalšie digitálne médiá umožňujú rýchle šírenie týchto fotografií a eskaláciu napätia až nepokojov (napr. fiktívna urážka náboženskej skupiny, ktorá podnieti jej neadekvátne reakcie).

1. **AI generované falošné (Deepfake) hlasové nahrávky**

*Použitím pokročilej AI dieťa, rodič občan nie sú schopní rozpoznať, či hlas patrí skutočne danej osobe.*

* 1. To vytvára množstvo následných hrozieb, napr.
     1. na mobile zavolá hlas ako mamin a prikáže dieťaťu, aby niečo vykonalo.
     2. Alebo hlas dieťaťa žiada o finančnú pomoc starého rodiča (podobné podvody sú dnes bežné, deepfake uľahčí manipuláciu staršej osoby).
     3. Mediálne známa osobnosť je zneužitá v deepfake nahrávke na propagáciu podvodných ponúk (napr. super investičné príležitosti).
  2. Na druhej strane osoba môže poprieť svoj hovorený prejav s odkazom na deepfake verziu.
  3. Sociálne siete umožňujú rýchle šírenie týchto nahrávok a eskaláciu napätia až nepokojov (napr. fiktívna urážka náboženskej skupiny, ktorá podnieti jej neadekvátne reakcie).

1. **Falošné (Fake) videá**
   1. Sú to umelo aranžované reálne videá, pre ovplyvňovanie verejnej cieľovej skupiny (mládeže, náboženskej skupiny, politických prívržencov, aj bežných občanov). Významná skupina influencerov na internete sa zaoberá
   2. Sociálne siete a ďalšie digitálne médiá umožňujú ich rýchle šírenie.
   3. Množstvo emocionálnych komentárov pod videom môže významne ovplyvniť osobu v akceptácii príbehu, ktorý je s danou fotografiou spojený (dieťa, rodič, verejnosť).
2. **AI generované falošné (Deepfake) videá**

*Umelo vytvorené v kombinácii s deepfake hlasovými nahrávkami sú stále účinnejším nástrojom na oklamanie či manipuláciu detí, ich rodičov, verejnosti ale aj časti odbornej verejnosti.*

* 1. To vytvára množstvo následných hrozieb, napr.
     1. Deepfake videá dievčat a žien v pornografii, ktoré sú schopné ich priviesť až k samovražde.
     2. Alebo video dieťaťa žiada o finančnú pomoc starého rodiča (podobné podvody sú dnes bežné, deepfake uľahčí manipuláciu staršej osoby).
     3. Mediálne známa osobnosť je zneužitá v deepfake videu na propagáciu podvodných ponúk (napr. super investičné príležitosti).
     4. Na druhej strane osoba môže poprieť svoj hovorený prejav s odkazom na deepfake verziu.
     5. Sociálne siete umožňujú rýchle šírenie týchto videí a eskaláciu napätia až nepokojov (napr. fiktívna urážka náboženskej alebo istej sociálnej skupiny, ktorá podnieti jej neadekvátne reakcie).
  2. Deepfakes majú znásobené negatívne dopady fake videí.

1. **Falošné / chybné / zavádzajúce odborné publikácie**
   1. Najznámejší prípad: očkovanie spôsobuje autizmus - Andrew Wakefield je britský gastroenterológ, ktorý v roku 1998 prišiel s výskumom, podľa ktorého očkovanie proti osýpkam, príušniciam a ružienke spôsobuje autizmus. Hoci má táto vyvrátená, chybná publikácia o autizme už vyše dvadsať rokov, prostredie sociálnych sietí ju živí aj dnes.
   2. Predátorské vedecké časopisy umožňujú publikovanie nedostatočne overených vedeckých faktov (od chybnej metodológie, výberu vzorky až po úmyselné falšovanie výsledkov výskumu).
      1. V diskusiách sú používané citácie z týchto článkov ako ekvivalent iných odborných faktov zo štandardných odborných médií.
      2. Deti a ich rodičia nemajú odborné znalosti na objektívne posúdenie relevantnosti faktov diskutujúcich strán.
      3. Negatívne dopady môžu byť až fatálne.
         1. Napr. generálne odmietanie očkovania (viď USA a zmena názoru ministra zdravotníctva po úmrtiach neočkovaných detí).
   3. Situácia je skomplikovaná tým, že veľké spoločnosti (v súčasnosti najmä farma firmy) boli schopné negatívne ovplyvniť aj štandardné odborné médiá a autority nepriaznivým spôsobom nimi platenými grantami, napr.
      1. fajčenie neškodí zdraviu (50. roky)
      2. opioidové lieky nevytvárajú závislosť (viď pandémia v USA, v súčasnosti najmä fentanyl [[42]](#footnote-42))
         1. „U.S. Food and Drug Administration’s approval of Purdue Pharma’s blockbuster OxyContin—led the U.S. health care system to greatly increase prescribing of opioid painkillers“
         2. „Opioid Manufacturer Endo Health Solutions Inc. Ordered to Pay $1.536B In Criminal Fines and Forfeiture for Distributing Misbranded Opioid Medication“
      3. Najnovším trendom je generovanie pseudo-odborných článkov v predátorských časopisoch s masívnym využitím AI (bez odbornej recenzie). [[43]](#footnote-43) V odbornej diskusii sú závery týchto článkov stavané voči štandardným vedeckým výsledkom. Ak niekto nie je odborník z danej oblasti, je mu ťažké objektívne posúdiť, kde je pravda.
2. **Falošné informácie, hoaxy, manipulatívne naratívy** 
   1. Táto oblasť bola tu už pred vznikom internetu, alebo rozvoj sociálnych sietí a digitálnych médií im umožnil nebývalý rozvoj.
      1. Ako príklad môžeme uviesť Protokoly sionských mudrcov.
      2. Ale aj zbrane hromadného ničenia v Iraku ako jedna zo zámienok na inváziu.
   2. Digitálne média v súčinnosti fake a deepfake artefaktov a sociálnych sietí rádovo zvyšujú rýchlosť ich šírenia a účinnosť.
   3. Zaujímavý je hoax plochej Zeme, ktorý napriek svoje absurdnosti a triviálnym experimentom s jeho vyvrátením vo virtuálnom  prostredí nabral novú silu.
   4. Otvorenou otázkou je, ako rozpoznať hoax od odlišného odborného názoru. Napr. vznik COVIDu – únik z laboratória vs. prirodzený pôvod. S tým majú problém nielen dospelí aj odborná verejnosť, nieto deti.
   5. Falošné informácie, propaganda a manipulatívne naratívy sa vďaka prepojeniu digitálnych platforiem šíria rýchlo a často sa navzájom podporujú cez reťazce „odkazov“, „komentárov“ a „citácií“, čím vytvárajú dojem dôveryhodnosti.
   6. Rastúce riziko predstavuje aj cieľové šírenie dezinformácií ako súčasť informačných vojen, hybridných hrozieb a psychologických operácií. Tie môžu ovplyvniť verejnú mienku, voľby, postoj k vede aj medicíne, či postoje k vojne.
3. **Stieranie hranice medzi názormi a faktami** 
   1. Novým trendom v mnohých médiách je stieranie hranice medzi reálnymi faktami a názormi žurnalistu – ako pravda často prezentovaný názor redakcie [[44]](#footnote-44).
   2. Niekedy je rozpoznanie hranice ťažké aj pre profesionála s kritickým myslením.
   3. Mládež má teda často problém odlíšiť fakty od názorov média, skupiny na sociálnej sieti alebo nejakej ideológie.
   4. Ak sú fakty systematický zamieňané za názory bez zohľadnenia faktov, ďalším krokom je prezentácia rovnocennosti všetkých názorov, ktorým sa má poskytnúť rovnaký priestor. Extrémnym príkladom je názor, že Zem je plochá [[45]](#footnote-45).
   5. Iným efektom je spochybňovanie faktov a idey pravdy – s tým, že pravda je skrytá a je tajne odhaľovaná v rámci sociálnych bublín.
   6. Tento trend oslabuje verejnú dôveru v vedu, médiá a inštitúcie a vedie k polarizácii spoločnosti, kde sa ľudia prestávajú dohadovať o riešeniach – pretože sa už ani nezhodnú na tom, čo sú fakty.

**Dopady horeuvedených hrozieb**

* 1. Vznik „Matrixu“ – virtuálnej vrstvy, ktorá deťom aj ich rodičom stále viac sprostredkúva informácie o dianí vo svete, na rozdiel od osobných skúseností v reálnych komunitách. Tento „Matrix“ je ovplyvňovaný vlastníkmi sociálnych sietí a digitálnych médií.
  2. Strata schopnosti stále väčšieho počtu osôb rozpoznať reálne informácie a objektívne fakty o dianí.
  3. Komunikácia v bublinách sociálnych sietí vplýva na generálne spochybnenie objektívnej pravdivosti poznania (napr. že všetko, čo produkujú oficiálne médiá je fake, ale len naša skupina pozná skutočnú pravdu).
  4. Spochybnenie objektívnosti všetkých oficiálnych médií.
  5. Ale aj spochybnenie nepohodlných alternatívnych médií v niektorých krajinách.
  6. Ľahšia manipulácia s osobami po spochybnení možnosti objektívneho poznania (ide o názory, nie fakty).

*Poznámka: v tejto kapitole pod pojmom:*

* *Falošný (Fake) obrázok je digitálne upravený alebo zámerne zmanipulovaný vizuálny materiál, ktorý vytvára klamlivý dojem reality s cieľom ovplyvniť vnímanie, emócie alebo názory príjemcu.*
* *deepfake chápeme umelo vytvorený obrázok, hlas či video (s pomocou AI), ktorý sa tvári ako reálny a je veľmi ťažké rozpoznať to, že je umelo vytvorený artefakt.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 10.1 | Fake fotografie | Z | N | **S** |
| 10.2 | Deep fake fotografie | K | N | **S** |
| 10.3 | Deepfake hlasové nahrávky | K | S | **V** |
| 10.4 | Fake videá | Z | N | S |
| 10.5 | Deepfake videá | K | S | **V** |
| 10.6 | Fake odborné publikácie | K | S | **V** |
| 10.7 | Hoaxy a falošné informácie | K | S | **V** |
| 10.8 | Stieranie hranice medzi názormi a faktami | K | N | S |

### Hrozby v špecifických životných situáciách

Sú to hrozby a riziká súvisiace so špecifickými životnými situáciami (pre presnosť: Life events), v ktorých sa deti a mladí ľudia môžu nachádzať. V tejto kapitole uvádzame príklady spracovania. Systematický prehľad hrozieb podľa životných situácií bude predmetom samostatnej aktivity.

1. **On-line zoznamovanie**

Obmedzovanie fyzických kontaktov mladých znamená aj zníženie šancí sa zoznámiť s potenciálnou partnerkou / partnerom. Preto čoraz väčší počet zoznámení sa realizuje v kybernetickom priestore – či už pri klasických chatoch v sociálnych sieťach, hrách, komunikačných aplikáciách, alebo v špecializovaných online zoznamkách. Tie majú tiež svoje špecifické riziká [[46]](#footnote-46)

Hrozby a riziká

1. Zneužitie účtu inou osobou (napr. je použité slabé heslo)
2. Zneužitie osobných údajov (mimo sextingu)
3. Odhalenie svojej reálnej identity potenciálnemu útočníkovi (ak ešte osobu fyzicky nepoznáme)
4. Falošná identita osoby na druhej strane
5. Prikrášľovanie u potenciálnych partnerov a vytváranie priestoru pre idealizáciu partnera
   1. Napr. žiadne fotografie, len text.
   2. Fotografie iných, lepšie vyzerajúcich osôb.
6. Potenciálny partner je v skutočnosti podvodník, vydierač, násilník alebo sexuálny predátor.
   1. Sexting, sextortion (zdieľanie sexuálneho obsahu) s potenciálnym partnerom, ktorý tento obsah zneužije na vydieranie.
   2. Žiadosti o náhlu finančnú pomoc.
   3. Emocionálne vydieranie.
7. Emocionálna nestabilita, depresia, pocit osamelosti oslabuje pozornosť pri rozpoznaní potenciálneho škodcu namiesto partnera.
8. Prvé stretnutie (ak u jedného z partnerov je hlboké sklamanie a druhý je z toho frustrovaný, agresívny).
   1. Okradnutie.
   2. Ublíženie na zdraví
   3. Znásilnenie
9. Emocionálna únava pri veľkom počte neúspešných pokusov o zoznámenie
10. **Hľadanie vlastnej identity (aj v kybernetickom priestore)**

Vo veku puberty aj neskôr (napr. pri frustrácii a osamelosti) zisťujú či hľadajú mnohí mladí ľudia svoju identitu, budúce smerovanie, hodnoty a preferencie. Pri tomto hľadaní využívajú webové sídla, digitálne médiá, sociálne siete, virtuálne komunity. Nie všetko, čo nájdu je ale pre ich hľadanie sa a rozvoj pozitívne.

Hrozby a riziká

1. Sekty, ktoré hľadajú nových členov
2. Radikálne skupiny rozširujúce svoj vplyv a členskú základňu
   1. Náboženské
   2. Idelogické
   3. Iné (napr. mizogýnne skupiny [[47]](#footnote-47), Incels komunity [[48]](#footnote-48))
3. Influenceri podnecujúci k nezdravým škodlivým aktivitám (napr. sebapoškodzovanie, extrémne diéty)
4. **Online nakupovanie**

Nakupovanie v digitálnom priestore sa týka starších žiakov, ktorí dostali svoje platobné prostriedky (napr. platobné karty, platby cez mobil naviazané na účty rodičov). V súvislosti s realizáciou nákupov a platieb pôsobí významných hrozieb a zraniteľností. Platby u mladých sú limitované celkovým objemom financií na účte a denným limitom.

Hrozby a riziká

1. Krádež a zneužitie identity na získanie finančných prostriedkov
   1. Získanie identifikačných a autentizačných údajov karty alebo účtu (PIN, bezpečnostný kód na karte).
      1. Využitie phisingu
      2. Podvodné webové stránky
      3. Priame sociálne inžinierstvo
      4. Podvodné platobné brány
   2. Následné zneužitie identifikačných a autentizačných údajov karty alebo účtu.
      1. Nákupy (tovar, služby)
      2. Uzatvorenie zmluvy
      3. Presun peňazí na iný účet
   3. Je ťažké dokázať, že na vine nie je dieťa a že jeho identitu niekto zneužil.
2. Získanie prístupu do internetového bankovníctva a nastavenie vlastného tokenu pre overovanie platieb.
   1. Ak útočník získa plnú kontrolu nad účtom, vie prevádzať peniaze až do úplného vyčerpania účtu alebo dosiahnutia stanovených limitov.
3. Nedodanie zaplateného tovaru alebo služby
   1. Dieťa si vyberie na webe položku, za ktorú zaplatí.
   2. Tovar alebo služba nie je dodaná.
4. Nekvalitné tovary a služby
   1. Dodaný tovar alebo služba nie v deklarovanej alebo očakávanej kvalite.
5. Nebezpečné tovary
   1. Ide najmä o lieky, anaboliká a výživové doplnky, ktoré sú ponúkané na pochybných webových stránkach.
6. Dodanie nevyžiadaného tovaru alebo služby
   1. Ide o tovar alebo službu, ktoré je dieťaťu vnútená bez toho aby si ju vybralo.
7. Stimulácia k nadmerným nákupom
   1. Web obchodníka manipuluje s dieťaťom, aby ho stimuloval k nadmerným nákupom
      1. Množstevné zľavy
      2. Mimoriadne výhodné ponuky
      3. Výpredaje
   2. Web obchodníka manipuluje s dieťaťom, aby ho stimuloval k nepotrebným nákupom
      1. Efektívna propagácia pre dieťa nepotrebného tovaru

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 11.1 | On-line zoznamovanie | K | S | **V** |
| 11.2 | Hľadanie vlastnej identity | K | N | S |
| 11.3 | Online nakupovanie | S | S | S |

### Hrozby súvisiace so sociálno-spoločenskou kontinuitou

Tieto hrozby nie sú priamo generované kybernetickým priestorom, ale virtuálne prostredie má na nich významný vplyv. Sú to hrozby súvisiace so zmyslom existencie (ontologické otázky) a priorít mládeže (aj ich rodičov) z hľadiska nielen svojho budúceho miesta v spoločnosti, ale aj fungovania kontinuity a trvalej udržateľnosti spoločnosti (schopnosť vôľa mať a vychovávať deti, sociálna solidarita, komunitná súdržnosť, ochota žiť a pracovať v svojej krajine a pod.).

**Významné hrozby:**

1. **Polarizácia spoločnosti**
   1. Sociálne siete a digitálne médiá významne prispievajú k extrémnej polarizácii spoločnosti. Je to viditeľné na Slovensku, v USA a množstve ďalších krajín.
   2. Istá polarizácia spoločnosti bola aj v minulosti, ale nóvum je jej extrémnosť a vyhrotenosť. Problém je v tom, že vo virtuálnom svete je možnosť uzavretia sa do virtuálnych sociálnych bublín a preferencia prezentácie negatívneho obsahu na sociálnych sieťach (negatívne priťahuje viac ako pozitívne).
   3. Skupinová polarizácia je tendencia sociálnych skupín robiť rozhodnutia, ktoré sú extrémnejšie než rozhodnutia jednotlivcov (priemer rozhodnutí jednotlivcov tvoriacich skupinu). Takáto tendencia sa prejavuje za predpokladu, že väčšina členov skupiny zastáva rovnaké stanovisko, čo je prípad bublín sociálnych sietí.
   4. Nárast radikalizácie a extrémistických postojov v spoločnosti – nedostatočná prevencia a absencia podpory pri hľadaní identity a bezpečia môže viesť k zvýšenej náchylnosti mladých ľudí k extrémistickým ideológiám, čo predstavuje hrozbu pre vnútornú bezpečnosť a súdržnosť spoločnosti.
   5. Mladí ľudia a dospievajúci sa často radikalizujú v online priestore, preberajú nenávistné postoje voči rôznym skupinám obyvateľstva, ktoré môžu vyústiť do násilného konania priamo ohrozujúceho život, zdravie, majetok. Môže to byť priame ohrozenie demokracie.
2. **Filozofia poslednej generácie** 
   1. Príkladom je nemecká aktivistická skupina Letzte Generation a jej pôsobenie aj vo virtuálnom priestore. Názov skupiny bol odvodený od presvedčenia jej členov, že patria do poslednej generácie ľudí, ktorá je schopná odvrátiť globálnu klimatickú katastrofu. A ak teda nie, sú poslednou generáciou. Preto napr. nemá zmysel mať deti. V širšom slova zmysle táto filozofia znamená, že „ja“ a môj well-being je hlavným zmyslom mojej existencie a čo bude po mne, nie je pre mňa podstatné.
   2. Inou variantou je totálne odtrhnutie od spoločnosti, pre ktoré majú Japonci špeciálny názov – Hikikomori.[[49]](#footnote-49)
3. **Možná kolízia práv jednotlivca a povinností voči spoločnosti**
   1. História ľudstva je sprevádzaná nárastom základných práv a slobôd pre všetkých občanov.
   2. V poslednom období nastala proliferácia požiadaviek na širšie ako základné práva a slobody [[50]](#footnote-50), často až na úrovni absurdnosti (napr. aby ma všetci rešpektovali ako psa [[51]](#footnote-51)).
   3. Paralelne v histórii možno sledovať pokles rozsahu povinností (otrok mal len povinnosti a minimálne práva, nevoľník menej, súčasný občan podstatne menej).
   4. V istom bode sociálnej evolúcie tieto trendy strácajú svoju sociálnu prínosnosť (napr. v digitálnych médiách široko prezentovaná predstava influencerov pre mladú generáciu, že nemá žiadne povinnosti voči spoločnosti, len práva) [[52]](#footnote-52).
   5. V teórii nelineárnych systémov s rastom stupňov voľnosti môže nastať stav fázového prechodu vedúci k deštrukcii existujúceho stavu a zániku systému alebo prechodu do nového stavu.

Príklad: desivý experiment populačnej dynamiky „raja“ - Universe 25 [[53]](#footnote-53).

1. **Juvenilizácia mladej generácie**
   1. Ide o fakt neskoršieho psychosociálneho dospievania a osamostatňovania sa mladej generácie.
   2. Vzdelávací systém umožňuje bytie bez nadmernej spoločenskej zodpovednosti až do 24 - 30 rokov (VŠ, postgraduálne vzdelávanie, PhD.).
   3. Virtuálny svet tento trend len posilňuje (napr. sociálne siete, počítačové hry, „vrtuľníkoví“ rodičia). Juvenilizáciu podporuje aj digitálny obsah s jednoduchou vetnou štruktúrou, emotikonmi a krátkymi videami.
   4. Dôsledkom juvenilizácie je aj „mama hotel“ aj u detí, ktoré by sa mohli a mali osamostatniť. SR je z hľadiska odchodu detí od rodičov druhé najhoršie v EÚ, s priemerným vekom 31 rokov.
2. **Demografické hrozby** 
   1. Jednou z očakávaných povinností jednotlivca voči spoločnosti je zabezpečiť jej kontinuitu vrátane požiadavky mať deti a vychovať budúcu generáciu.
   2. U influencerov a konzumentov virtuálneho sveta môže byť táto povinnosť viac obťažujúca a vedie k snahe vyhnúť sa jej (je „ cool“ tráviť čas vo virtualite a byť oprostený rodičovských povinností). Ich názor je, že je to vec každého či chce deti, alebo nie. Ak tento názor prestane byť minoritným, podporuje demografickú krízu.
   3. Nová generácia digitálnej pornografie v využitím AI a deep fake technológií, virtuálnych priateliek – chatbotov poskytuje mladým náhradu za rozvoj normálnych vzťahov.
   4. Významná časť mladých uprednostňujú kariéru, cestovanie a osobný rozvoj, pričom zakladanie rodiny odsúva na neskôr. Priemerný rok prvorodičiek je viac než 28 rokov. V okrese Bratislava I je to až 32 rokov. Digitálne média tieto trendy len posilňujú (viď napr. Instagram).
   5. OSN spracovalo prehľad vývoja fertility krajín pod záchovnou hodnotou 2.1 (sú tam aj moslimské krajiny). [[54]](#footnote-54) Prehľad po jednotlivých krajinách spracovala Svetová banka. [[55]](#footnote-55)
   6. Hodnota pre Slovensko je 1,5 dieťaťa na ženu v plodnom veku. V roku 2024 sa narodilo len 46.423 detí [[56]](#footnote-56). V roku 2016 to bolo 57,5 tisíca detí. V 70 rokoch (Husákove deti) to bolo cca. 100.000 detí ročne.
   7. Pohľad veliteľstva NATO, admirál Vandier, šéf veliteľstva pre transformáciu „Pretože vymierame, nebudeme schopní posielať na bojisko milióny ľudí ako za druhej svetovej vojny, takže sa musíme spoľahnúť na roboty a bezpilotné stroje.

Obrázok, na ktorom je text, vývoj, snímka obrazovky, diagram

Obsah vygenerovaný pomocou AI môže byť nesprávny.

1. **Mať vs. byť**
   1. Sociálne siete, napr. Instagram sú vhodným publikačným nástrojom pre prezentáciu úspešného životného štýlu, super dovoleniek, vrátane vlastnenia drahých vecí. Porovnávanie sa s influencermi a celebritami vedie u väčšinu používateľov sociálnych sietí k frustrácii a túžbe vlastniť aspoň časť z prezentovaných vecí a ukázať to svojmu virtuálnemu okoliu. Virtuálne komunity oceňujú „mať“ omnoho viac ako „byť“. Tieto negatívne vplyvy sa znásobujú u mladej generácie vstupujúcej do sveta sociálnych sietí.
   2. Nadmerné sa porovnávanie s celebritami na Instagrame vedie  väčšinu používateľov len k väčšej frustrácii [[57]](#footnote-57), alebo hľadaniu skratiek k zbohatnutiu (napr. drogový díler, sexuálna prezentácia na OnlyFans, zlatokopky ale už aj zlatokopi).
   3. Ideálom významnej časti mladých ľudí je byť influencerom [[58]](#footnote-58). Nakoľko je tak veľa záujemcov, šanca uspieť si vyžaduje stále extrémnejší obsah.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** | **Následok** | **Pravde-podobn.** | **Riziko** |
| 12.1 | Filozofia poslednej generácie | Z | N | S |
| 12.2 | Možná kolízia práv jednotlivca a povinností voči spoločnosti | Z | N | S |
| 12.3 | Juvenilizácia časti mladej generácie | Z | N | S |
| 12.4 | Demografické hrozby | K | V | **VV** |
| 12.5 | Mať vs. byť | K | S | **V** |
| 12.6 | Polarizácia spoločnosti | K | S | **V** |

### Hrozby súvisiace s AI (umelá inteligencia)

Umelá inteligencia prináša okrem príležitostí aj množstvo rizík [[59]](#footnote-59). O ich miere je silná odborná diskusia.

#### Hrozby a riziká z pohľadu EÚ

Nariadenie EÚ o umelej inteligencii [[60]](#footnote-60) vymedzuje regulačný rámec pre riadenie rizík súvisiacich s AI, a je v nej uvedené

„ AI môže zároveň v závislosti od okolností týkajúcich sa jej konkrétnej aplikácie, použitia a úrovne technologického vývoja vytvárať riziká a ujmu pre verejné záujmy a základné práva, ktoré sú chránené právom Únie. Toto poškodzovanie môže byť hmotné aj nehmotné vrátane fyzickej, psychickej, spoločenskej alebo ekonomickej ujmy.“

1. Funkčné riziká [[61]](#footnote-61)
   1. Diskriminácia
   2. Skreslenie / halucinácie
   3. Nedostatočná zodpovednosť
2. Oblasti použitia so zvýšenou mierou rizika
   1. diagnostika chorôb
   2. autonómne vedenie vozidla
   3. **autonómne vzdelávanie**
   4. biometrická identifikácia jednotlivcov zapojených do trestnej činnosti
3. Oblasti s neakceptovateľnou mieru rizika
   1. Kognitívna manipulácia správania
   2. Prediktívne vykonávanie policajných funkcií
   3. Rozpoznávanie emócií na pracovisku a vo vzdelávacích inštitúciách a sociálne hodnotenie.
   4. Systémy diaľkovej biometrickej identifikácie v reálnom čase
4. Zakázané praktiky využívajúce AI (všetky viď Čl. 5 Nariadenia EÚ [[62]](#footnote-62)), napr.
   1. používanie systému AI, ktorý využíva podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčiní, že prijmú rozhodnutie, ktoré by inak neprijali, a to spôsobom, ktorý tejto osobe, inej osobe alebo skupine osôb spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;
   2. používanie systému AI, ktorý využíva ktorúkoľvek zo zraniteľností fyzickej osoby alebo osobitnej skupiny osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie s cieľom alebo účinkom podstatne narušiť správanie tejto osoby alebo osoby patriacej do tejto skupiny spôsobom, ktorý tejto alebo inej osobe spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

#### Ďalšie riziká súvisiace s používaním AI

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

1. **Vplyvy na kognitívne schopnosti a duševné zdravie**
2. Znižovanie úrovne mentálnych schopností nadmerným nevhodným využívaním AI.
3. Nadmerná miera dôvery voči AI výstupom (možné halucinácie AI)
   1. Nepriaznivý vplyv halucinácií AI, nepostačujúca miera istoty, či sú poskytnuté informácie v poriadku.
4. Psychosociálna závislosť na AI chatbotoch.
5. Zneužívanie AI v pornografii, napr. pri tvorbe deepfake videí dievčat, ktoré sú schopné dohnať ich až k samovražde.
6. Modifikácia hodnotového systému vplyvom interakcie s AI.
7. Neschopnosť rozlíšiť reálnych komunikačných partnerov (ľudí) od pokročilých chatbotov (existuje chatbot, ktorý prešiel Turingovým testom).
8. Erózia etických a morálnych noriem – bez správneho vedenia môže mládež preberať postoje, že „ak to AI dovolí alebo vytvorí, je to v poriadku“, čo vedie k oslabeniu morálneho úsudku.
9. Nárast psychických ťažkostí – porovnávanie sa s „dokonalými“ AI-generovanými avatarmi alebo obsahom môže prispieť k nízkemu sebavedomiu, frustrácii a úzkostiam.
10. Zneistenie v oblasti pravdy a reality – rastúci výskyt deepfake videí, textov a obrázkov generovaných AI môže spôsobiť zmätok v rozlišovaní medzi skutočnosťou a manipuláciou.
11. Skrytá diskriminácia v AI interakciách a podpore rozhodovania (pri nesprávnych trénovacích dátach).
12. **IKT riziká**
13. Nová úroveň sociálneho inžinierstva využívaná hackermi (reálne znejúce maily, falošné weby, komunikácia, pokročilý malvér)
14. Strata súkromia – AI systémy zhromažďujú obrovské množstvo osobných údajov; mládež aj jej rodičia nemusia rozumieť, ako sú tieto údaje používané alebo zneužívané.
15. Narastajúce zneužívanie AI (najmä deepfake) pri kyberšikane vo vzťahu žiak-žiak, žiak-pedagóg.
16. **Vplyvy na vzdelávací proces**
17. Zníženie miery samostatného, kritického myslenia žiaka nadmerným resp. nesprávnym využívaním AI.
18. Zneužívanie AI ako náhrady pre vykázanie samostatnej aktivity žiaka.
19. Istá miera digitálnej vylúčenosti žiakov, ktorí nevedia AI využívať.
20. Zníženie hodnoty ľudskej tvorby – vnímanie, že „AI to spraví lepšie alebo rýchlejšie“, môže viesť k znevažovaniu vlastnej práce a znižovaniu motivácie.
21. **Plánované zavádzanie AI do výučby (výzvy a riziká)**

Táto aktivita je veľmi dôležitá, ale prináša riziká, ktoré je potrebné efektívne riadiť – aby táto zmena vo výuke bola významným prínosom.

1. Nesprávne nastavenie kurikula.
2. Nepostačujúco pripravení školitelia.
3. Nepripravení alebo nepostačujúco pripravení pedagógovia.
4. Chýbajúce menšie overenie nasadenia AI vo výučbe (Proof of Concept).
5. Nesprávne nastavené spôsoby získania benefitov z AI.
6. Nemotivovaní žiaci využívajú AI ako náhradu za svoju aktivitu.
   1. Aplikácia AI vo výučbe nevedie k zvýšeniu kritického, samostatného a tvorivého myslenia.
   2. Nenaplnenie očakávaných benefitov AI vo výučbe.
7. **Riziká pre pracovný trh a konkurencieschopnosť**

*Tieto riziká sú úzko previazané s mierou (ne)úspešnosti implementácie AI do vzdelávacieho procesu.*

1. Znevýhodnenie pri vstupe na pracovný trh pri neznalosti potenciálu AI a schopností ju tvorivo využiť.
   1. Zmena povahy práce – Tlak na rýchle preškolenie pracovnej sily, potreba nových digitálnych zručností.
2. Významné ohrozenie pracovných miest budúcej generácie pracujúcich.
   1. Automatizácia pracovných miest – AI ohrozuje mnohé profesie (napr. v administratíve, doprave, spracovaní dát), čo môže zvýšiť nezamestnanosť a sociálne napätie.
3. Zníženie konkurencieschopnosti krajiny,
   1. ktorá nemá pripravených zamestnancov na využívanie AI v pracovnom procese,
   2. ktorej firmy nevyužívajú potenciál AI,
   3. ktorá nemá vlastné jazykové modely.
4. **Riziká na úrovni štátov**
5. Digitálna kolonizácia – štáty bez vlastných AI kapacít sú závislé na technologických veľmociach (vrátane svojich vzdelávacích systémov).
6. Závod v zbrojení s AI – súťaž medzi veľmocami o dominanciu v AI môže viesť k ignorovaniu bezpečnostných a etických noriem (s dopadom aj na deti / mládež).
7. Monopolizácia výskumu – Malé množstvo firiem (napr. Big Tech) koncentruje pokročilé AI schopnosti a výskum.
8. Ovplyvňovanie verejnej mienky v iných štátoch prostredníctvom AI (odpovede sú politicky podfarbené).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov oblasti hrozieb** (negatívne vplyvy v danej oblasti) | **Následok** | **Pravde-podobn.** | **Riziko** |
| 13.1 | Funkčné riziká | Z | S | **V** |
| 13.2 | Oblasti použitia so zvýšenou mierou rizika | Z | N | S |
| 13.3 | Oblasti s neakceptovateľnou mieru rizika | K | S | **V** |
| 13.4 | Zakázané praktiky využívajúce AI | K | S | **V** |
| 13.5 | Vplyvy na kognitívne schopnosti a duševné zdravie | K | V | **VV** |
| 13.6 | IKT riziká | Z | N | S |
| 13.7 | Vplyvy na vzdelávací proces | Z | S | **V** |
| 13.8 | Riziká plánovaného zavádzania AI do výučby | Z | N | S |
| 13.9 | Riziká pre pracovný trh a konkurencieschopnosť | Z | S | **V** |
| 13.10 | Riziká na úrovni štátov | Z | N | S |

### Nové oblasti zdrojov hrozieb a zraniteľností

V tejto kapitole uvádzame novo sa objavujúce technologické oblasti zdrojov hrozieb a zraniteľností pri interakcii s digitálnym alebo digitálne riadeným svetom. Je to nad rámec kybernetického priestoru v oblasti, kde dochádza k pôsobeniu robotických / dronových zariadení s fyzickým vplyvom na predmety aj osoby.

**I.**

AI – viď predchádzajúca kapitola.

#### Inteligentná technika

Sú to zariadenia a technika napojená na Internet, diaľkovo ovládateľná a prípadne cloudovú vedomostnú bázu.

Inteligentná technika v domácnosti (smart home – napr. hlasoví asistenti, kamery, smart chladničky, žiarovky, zámky, robotické vysávače) prináša pohodlie, ale zároveň so sebou nesie vážne riziká v oblasti bezpečnosti, súkromia a závislosti na technológii.

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

Hrozby a riziká

* 1. Zraniteľnosť voči hackerským útokom
     1. Slabo zabezpečené zariadenia napojené na wi-fi môžu byť napadnuté a útočník môže:
        1. získať prístup ku kamere alebo mikrofónu, sledovať a odpočúvať domácnosť alebo aj do nej priamo alebo nepriamo zasahovať,
        2. ovládať zámky dverí,
        3. zapínať/vypínať spotrebiče (aj spôsobom vedúcim k ich deštrukcii),
     2. Botnet útoky
        1. Nezabezpečené zariadenia môžu byť zneužité ako súčasť siete útočných zariadení (napr. pre DDoS útoky – ako bol známy prípad útoku Mirai).
     3. Obsolescencia (ukončenie technickej podpory)
        1. Zariadenia môžu prestať fungovať po pár rokoch, ak výrobca ukončí podporu – čo spôsobuje zbytočný odpad aj dodatočné náklady.
  2. Strata súkromia a ochrana osobných údajov
     1. Neustále sledovanie členov domácnosti
        1. Hlasoví asistenti (napr. Amazon Alexa, Google Assistant) môžu „počúvať“ aj mimo aktivácie. Niektoré zariadenia neustále zbierajú zvukové alebo obrazové dáta.
     2. Zber a predaj dát tretím stranám
        1. Mnohé zariadenia zbierajú údaje o správaní používateľa (kedy zapína svetlo, aké príkazy dáva, ako sa pohybuje po dome) a tieto dáta môžu byť predávané na marketingové účely.
        2. Nízka transparentnosť toho, čo zariadenie robí
           1. Používatelia často nevedia, aké dáta sú zhromažďované a kam putujú – ani aké bezpečnostné opatrenia sú použité.
  3. Psychologické a sociálne riziká
     1. Závislosť od technológie
        1. Prílišná automatizácia môže viesť k strate samostatnosti a základných zručností – napr. zabúdanie na jednoduché úlohy, nižšia schopnosť riešiť technické problémy.
     2. Strata súkromia aj v rodine
        1. Sledovanie členov domácnosti (napr. cez kamery alebo senzory) môže narušiť dôveru a súkromie, najmä u detí a tínedžerov.
  4. Riziká pre deti
     1. Nekontrolovaný prístup k technológii
        1. Deti môžu bez dozoru komunikovať s hlasovými asistentmi alebo mať prístup k obsahu, ktorý nie je vhodný pre ich vek.
     2. Sledovanie detí bez ich vedomia
        1. Smart kamery, trackery a senzory môžu byť zneužité na neetické sledovanie správania detí.
     3. Hacknuté inteligentné hračky (napr. používajú vulgarizmy, navádzajú dieťa na zlé veci)
  5. Prevádzkové riziká
     1. Technická závislosť na internete a cloude
        1. Ak vypadne internet alebo dôjde k výpadku serverov poskytovateľa, mnohé zariadenia môžu byť nepoužiteľné (napr. zámok na dverách, kúrenie, alarm).
     2. Neplánované aktualizácie a zmeny funkčnosti
        1. Výrobca môže softvérovo zmeniť alebo zrušiť funkcie zariadenia bez súhlasu používateľa (napr. vypnutie podpory starších modelov).
  6. Finančné riziká
     1. Vysoké náklady na údržbu a kompatibilitu
        1. Rôzni výrobcovia majú vlastné ekosystémy – zariadenia medzi sebou nemusia spolupracovať, čo núti spotrebiteľa kupovať drahšie produkty v jednom systéme (tzv. vendor lock-in).

#### Robotika

Roboty sa dostávajú aj do domácností. Medzi prvými boli inteligentné vysávače. Pre staršie osoby s obmedzenou mobilitou sú pripravované podporné asistenčné roboty. Roboty sú dnes bežnou súčasťou v ponuke hračiek. Ich inteligencia rastie.

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

Hrozby a riziká

1. IKT riziká
   1. Zraniteľnosť voči hackerom
      1. Mnohé roboty sú pripojené k internetu (Wi-Fi, cloud), no nie vždy dostatočne chránené.
      2. Slabo zabezpečené robotické zariadenia môžu byť napadnuté. Útočník môže:
         1. ovládnuť robota na diaľku,
         2. získať prístup k senzorom, kamerám a mikrofónom,
         3. zhromaždiť mapu bytu (napr. cez robotický vysávač),
         4. monitorovať činnosť domácnosti.
      3. Hacknuté domáce hračky s kamerou (umožňujú nahrávanie videí z domácnosti).
   2. Botnet útoky
      1. Nezabezpečené robotické zariadenia môžu byť zneužité ako súčasť siete útočných zariadení (napr. pre DDoS útoky – ako bol známy prípad útoku Mirai).
   3. Zraniteľnosť voči hackerom
   4. Hoci zriedkavé, teoreticky by mohol byť robot zmanipulovaný tak, aby spôsobil škodu (napr. náraz, zablokovanie výstupu, zničenie objektov).
2. Ochrana súkromia a osobných údajov
   1. Mapovanie priestoru a nahrávanie dát
      1. Niektoré roboty vytvárajú presné mapy miestností, sledujú pohyb osôb a analyzujú zvukové aj obrazové dáta.
   2. Zber citlivých informácií
      1. Údaje môžu byť odosielané výrobcom, uložené v cloude, alebo dokonca predávané tretím stranám.
   3. Trvalé monitorovanie
      1. Opatrovateľské alebo sociálne roboty môžu narúšať pocit súkromia (najmä u seniorov, detí a osôb so zdravotným postihnutím).
3. Psychologické a sociálne riziká
   1. Závislosť na robotoch
      1. Prílišná dôvera v robota môže viesť k oslabeniu samostatnosti – napr. u detí alebo starších ľudí.
   2. Falošný pocit spoločnosti
      1. Sociálni roboti môžu vytvárať dojem vzťahu či empatie, hoci ide len o program. To môže viesť k osamelosti alebo skreslenému vnímaniu reality zo strany dieťaťa.
   3. Zmena v správaní detí
      1. Dlhodobé používanie robotov môže ovplyvniť rozvoj empatie, sociálnych zručností či vzťah k autorite.
4. Zdravotné riziká
   1. Domáce roboty s vyššou mierou autonómie
      1. Možnosť ublíženia na zdraví (napr. chybný SW vedúci k podrazeniu nôh majiteľa)
   2. Domáce, v istej miere autonómne kinetické hračky
      1. Možnosť ublíženia na zdraví (napr. útoky voči dieťaťu v dôsledku technickej chyby, chyby v SW, po hacknutí)
   3. Roboty vo verejnom priestore (napr. policajné)
      1. Môžu ublížiť deťom neznalým bezpečnostných rizík.
5. Technické a prevádzkové riziká
   1. Poruchy a zlyhania systému
      1. Robot chybou SW môže nečakane zlyhať, naraziť do objektov alebo poškodiť domácnosť (napr. rozliať tekutiny, zachytiť káble).
   2. Technická závislosť na internete a cloude
      1. Ak vypadne internet alebo dôjde k výpadku serverov poskytovateľa, mnohé robotické zariadenia môžu byť nepoužiteľné.
   3. Neplánované aktualizácie a zmeny funkčnosti
      1. Výrobca môže softvérovo zmeniť alebo zrušiť funkcie robota bez súhlasu používateľa (napr. vypnutie podpory starších modelov).
   4. Nevhodné aktualizácie softvéru
      1. Aktualizácia môže zmeniť správanie robota alebo znefunkčniť niektoré funkcie.
      2. Zastarávanie a obmedzená životnosť
      3. Výrobcovia často prestanú podporovať roboty po pár rokoch – výsledkom je elektronický odpad a opätovná investícia.
      4. Zastarávanie a obmedzená životnosť
         1. V rýchlom inovačnom cykle výrobcovia často prestanú podporovať roboty po pár rokoch – výsledkom je elektronický odpad a potrebná opätovná investícia.
6. Etické a právne riziká
   1. Nejasná zodpovednosť
      1. Ak robot poškodí majetok alebo zdravie – kto je zodpovedný? Používateľ, výrobca, softvérový vývojár?
   2. Neprimerané sledovanie členov domácnosti
      1. Ak je robot vybavený kamerou či mikrofónom, môže byť zneužitý na sledovanie detí, partnera alebo návštev.
   3. Zníženie ľudskej interakcie
      1. V rodinách, kde robot nahrádza starostlivosť alebo komunikáciu, môže dôjsť k oslabeniu medziľudských väzieb.

#### Porno produkty na novej technologickej úrovni

Pornografický priemysel rýchlo implementuje moderné technológie. Vysoký grafický výkon nových domácich počítačov zvyšuje potenciál aj príťažlivosť porno produktov (aj pre mládež). V súčasnosti je to najmä využitie AI.

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

Hrozby a riziká

1. Psychologické a vývinové riziká
   1. Skreslený obraz o sexualite a vzťahoch
      1. Deti môžu začať vnímať sex ako agresívny, neosobný alebo podriadený výkonu, nie ako prejav intimity a lásky.
   2. Zvýšená úzkosť a zmätenosť
      1. U detí môže pornografia vyvolať strach, odpor alebo zvedavosť, ktorú nedokážu spracovať. Môžu mať nočné mory alebo výčitky.
   3. Zníženie sebaúcty
      1. Porovnávanie s nerealistickými telami alebo „výkonom“ v porne môže ovplyvniť vlastný obraz tela a sebadôveru.
   4. Závislosť a kompulzívne správanie
      1. U niektorých detí sa môže rozvinúť závislosť na pornografii, ktorá ovplyvní ich koncentráciu, emócie a denné návyky.
   5. OnlyFans je príťažlivou alternatívou pre mladé dievčatá. Konkurencia je vysoká a preto prerazenie v tejto branži vyžaduje stále emocionálnejší, extrémnejší obsah.
   6. Interaktívne vizuálne novely vytláčajúce iné formy komunikácie príbehov (knižné, TV, film).
   7. Realistická grafika s podporou podporujúca vtiahnutie dieťaťa k digitálnemu obsahu.
   8. Využitie AI chatbotov na pripútanie dieťaťa k danej aplikácii alebo webovej stránke.
   9. Inteligentné silikónové erotické bábiky / roboty [[63]](#footnote-63)
      1. Tie predstavujú oveľa vyššiu úroveň sexuálneho pripútania a závislosti
2. Predčasná a riziková sexualizácia
   1. Nábeh na skoré sexuálne správanie
      1. Deti môžu napodobňovať to, čo videli, bez pochopenia dôsledkov – čo vedie k rizikovému správaniu alebo zneužívaniu iných.
   2. Poruchy sexuálnej identity alebo vývinu
      1. Môže sa narušiť zdravý vývin sexuálnej orientácie a preferencií.
   3. Riziko, že sa dieťa stane obeťou alebo páchateľom
      1. Kontakt s pornografiou môže dieťa buď zlákať k nevhodnému obsahu, alebo naopak spôsobiť, že zneužije iné deti (napr. ako „hra“).
   4. Nerealistické sexuálne správanie a praktiky ako inšpirácia.
3. Online riziká
   1. Kontakt s predátormi
      1. Niektoré weby alebo aplikácie môžu viesť deti k rozhovorom s dospelými, ktorí ich zneužívajú alebo manipulujú (grooming).
   2. Prístup k ilegálnemu obsahu
      1. Deti môžu nevedomky naraziť na detskú pornografiu alebo extrémne násilie, ktoré zanechá traumatické následky.
   3. Digitálne stopy a kyberšikana
      1. Ak dieťa zdieľa intímne fotky alebo videá, môže byť vydierané (sextortion) alebo zosmiešňované.
4. Právne riziká
   1. Nevedomé alebo vedomé porušenie zákona
      1. Držba, zdieľanie alebo vyhľadávanie pornografie (aj medzi rovesníkmi) môže mať právne následky, hoci išlo o „zvedavosť“.
   2. Trestné činy z nedbanlivosti
      1. Niektoré deti môžu zdieľať nahé fotky seba alebo iných, čím nevedome vytvoria detskú pornografiu.

#### Sociálne siete - pokročilý digitálny obsah

Pokročilý digitálny obsah zahŕňa aj pokročilých AI botov (časom autonómných „bytostí“), ktorých je často ťažko rozpoznať od reálnych ľudí. Je možné ich pomerne rýchlo vytvoriť vo veľkom množstve.

Hrozby a riziká

1. Negatívne pôsobenie AI digitálnych influencerov [[64]](#footnote-64)
2. Negatívne pôsobenie AI digitálnych trolov v diskusiách
3. Fiktívni AI partneri, poradcovia, psychológovia
4. Deepfake videá na sociálnych sieťach

#### Civilné drony

Civilné drony s videokamerou (mobilom) sú bežne dostupné. Je nimi možné monitorovať aj aktivity iných osôb a narúšať ich súkromie.

Hrozby a riziká

1. Nová úroveň narušenia súkromia
   1. Osoba zneužívajúca dron na špicľovanie, stalking a sexting (dieťaťa)
      1. Osobou zneužívajúcou dron môže byť staršie dieťa
   2. Súkromie dieťaťa / rodičov zneužívané dronmi
2. Budúce zneužívanie kriminálnym podsvetím na fyzické útoky

#### Letálne autonómne zbrane

(LAW - Lethal autonomous weapons [[65]](#footnote-65))

Sú to novo vyvíjané zbraňové systémy schopné autonómneho konania s využitím AI (likvidácie určených osôb).

Hrozby a riziká

1. LAW predstavujú vážne riziko v prípade ich rozšírenia do kriminálneho podsvetia a ich využitie v útokoch voči občanom, vrátane detí.
2. S pokrokom AI bude možné LAW funkcionalitu implementovať aj do súčasných zariadení (napr. autonómny vysávač, ktorý vás zhodí zo schodov, chodiaca bábika, ktorá vedome ublíži dieťaťu – ako to bolo doteraz prezentované v hororoch).

#### Sektor neurónových technológií

Ide o najmä o plánovanú implementáciu čipov do mozgu a vytvorenie novej štruktúry častí mozgu a čipu  **[[66]](#footnote-66).**

Jednou s cieľových skupín aktuálneho nasadenia sú plne imobilné osoby, ktorým umožňuje ovládanie počítača a zariadení pre podporu pohybu.

Vývoj sa zameriava aj na vytvorenie nového rozhrania pre interakciu mozog – počítač [[67]](#footnote-67) (Intelligent Neural Interfaces - INI). Jedným z rámcov aktivít je „ The Next-Generation Nonsurgical Neurotechnology (N3)“ s cieľom vyvinúť „high-performance, bi-directional brain-machine interfaces“.

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

Hrozby a riziká

1. Zdravotné riziká
   1. Chirurgické komplikácie pri zavádzaní neuročipov do mozgu. Hrozí riziko krvácania, infekcie, zápalu, poškodenia mozgového tkaniva alebo dokonca smrti.
   2. Odmietnutie implantátu (imunitná reakcia)
   3. Telo môže považovať čip za cudzie teleso a spustiť zápal alebo imunitnú odpoveď, čo vedie k zlyhaniu systému.
   4. Dlhodobé následky
      1. Zmena správania sa mozgu pri dlhodobej interakcii s čipom.
      2. V súčasnosti chýbajú dáta o tom, ako implantáty ovplyvňujú mozog po desiatkach rokov. Možný je napríklad rast jazvového tkaniva alebo neurodegeneratívne procesy.
2. Etické riziká
   1. Zásah do ľudskej identity a zodpovednosť za svoje činy
      1. Ak technológia môže meniť mení emócie, myšlienky alebo správanie, vzniká právna a etická otázka: kto má zodpovednosť za rozhodnutia a činy danej osoby?
   2. Zvýhodnenie nositeľov čipov (tzv. neuro-enhancement)
      1. Pokročilé neuročipy majú potenciál významného rozšírenia intelektuálnych schopností (napr. lepšiu pamäť, rýchlejšie učenie a rozhodovania), čo môže viesť k nerovnosti medzi „vylepšenými“ a „nevylepšenými“ ľuďmi.
   3. Ohrozenie autonómie
      1. Ak bude možné manipulovať myšlienky alebo emócie človeka prostredníctvom neurotechnológií, hrozí strata kontroly nad vlastným vedomím.
   4. Politická a sociálna manipulácia
      1. Neurotechnológié vytvárajú potenciál politickej alebo sociálnej manipulácie na rádovo vyššej úrovni.
3. IKT riziká
   1. Hackovanie mozgu
      1. Neuročipy, ktoré komunikujú bezdrôtovo, môžu byť potenciálne napadnuteľné. Hacker môže ovplyvniť správanie osoby alebo prístup k súkromným myšlienkam.
   2. Zneužitie dát
      1. Mozgové signály môžu obsahovať veľmi osobné informácie (napr. reakcie na podnety, obavy, zámery). Ich zneužitie firmami alebo štátom predstavuje vážne porušenie súkromia.
4. Spoločenské a sociálne riziká
   1. Technologická a následná nerovnosť
      1. Prístup k neuročipom je drahý – len elity si budú môcť dovoliť "upgrade mozgu", čím sa ešte viac prehĺbia sociálne rozdiely.
   2. Tlak na výkon
      1. Ak sa neuročipy rozšíria v školskom aj pracovnom prostredí, študenti a zamestnanci bez nich budú znevýhodnení, čo vytvorí spoločenský tlak na ich používanie.
   3. Stigmatizácia alebo segregácia
      1. Rozdelenie na „pripojených“ (connected minds) a „nepripojených“ môže viesť k diskriminácii už od detského veku alebo strate rovnosti v spoločnosti.
   4. Ovládanie občanov
      1. Možnosť zneužitia autoritárskym režimami na ovládanie občanov vrátane detí na rádovo vyššej úrovni.
5. Výskumné a regulačné riziká
   1. Nedostatočné testovanie
      1. Mnohé neuročipy sú ešte vo fáze výskumu. Ich predčasné nasadenie do praxe môže byť nebezpečné.
   2. Chýbajúce regulácie a dohľad
      1. Legislatíva zaostáva za technologickým vývojom, vznikajú závažné otvorené otázky, napr.: kto je zodpovedný, ak nefunguje správne a a dôjde k nehode?

#### Virtuálna realita

„Virtuálna realita (VR) je prostredie vymodelované prostriedkami počítačovej simulácie, ktoré umožňujú interagovať s umelým trojrozmerným (3D) vizuálnym alebo iným zmyslovým prostredím. Aplikácie VR ponoria používateľa do počítačom generovaného prostredia, ktoré simuluje realitu pomocou interaktívnych zariadení, ktoré odosielajú a prijímajú informácie ako sú okuliare, náhlavné súpravy (angl. headset), rukavice alebo celotelové obleky. V typickom prípade si používateľ s VR headsetom so stereoskopickou obrazovkou prezerá animované obrázky simulovaného prostredia. Ilúziu „byť pri tom“ (teleprítomnosť) vyvolávajú pohybové senzory, ktoré zachytávajú pohyby používateľa a podľa toho prispôsobujú pohľad na obrazovke, zvyčajne v reálnom čase (v okamihu, keď dôjde k pohybu používateľa) [[68]](#footnote-68)“.

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

Hrozby a riziká

1. Riziká pre fyzické zdravie
   1. dlhodobé nosenie VR okuliarov môže spôsobiť závraty, nevoľnosť, tzv. „VR chorobu“ – spôsobenú nesúladom medzi pohybom očí a tela, rovnováhou, poruchám spánku a obehového systému, najmä u detí v období vývoja.
   2. Zranenia – pád alebo náraz pri pohybe v reálnom priestore so zapnutou náhlavnou súpravou.
   3. Problémy so zrakom – únava očí, bolesť hlavy pri dlhom používaní.
   4. Znížená fyzická aktivita – zážitky vo VR môžu nahrádzať reálne aktivity, čo prispieva k sedavému spôsobu života, obezite a celkovej fyzickej pasivite detí a mládeže.
2. Riziká pre duševné zdravie
   1. Odtrhnutie sa od reality – pravidelné používanie VR môže viesť k narušeniu schopnosti rozoznávať hranicu medzi virtuálnym a reálnym svetom, najmä u detí a dospievajúcich.
      1. Únik od reality / závislosť – pre niektorých používateľov sa môže VR stať atraktívnejším svetom ako realita.
   2. Závislosť od imerzívneho obsahu – vysoká miera ponoru a vizuálnej atraktivity VR môže zvyšovať riziko vzniku nelátkových závislostí, najmä v súvislosti s hrami a simuláciami.
   3. Zvýšená úzkosť alebo stres – realistické VR zážitky môžu byť psychicky náročné (napr. horory, simulácie výšok).
      1. Vystavenie nevhodnému alebo traumatizujúcemu obsahu – vo VR prostredí je možné vytvárať extrémne realistické nevhodné zážitky (násilie, pornografiu, manipuláciu), ktoré môžu mať výrazný negatívny dopad na psychiku detí.
   4. Narušenie vnímania reality – po dlhom čase vo VR môže používateľ dočasne stratiť orientáciu v reálnom svete.
3. Sociálne a spoločenské riziká
   1. Zhoršenie sociálnych zručností – intenzívna interakcia vo VR môže nahradiť skutočné medziľudské kontakty, čo vedie k obmedzenému rozvoju empatie, neverbálnej komunikácie a schopnosti riešiť konflikty v reálnom prostredí.
   2. Obťažovanie alebo až kyberšikana vo VR priestore – v multiplayerových VR aplikáciách sa objavujú prípady verbálneho, sexuálneho či fyzicky simulovaného obťažovania (tzv. „virtuálny dotyk“), pričom ich prežívanie je subjektívne silnejšie ako v bežnom online prostredí.
   3. Izolácia – prílišné používanie VR môže obmedziť reálne medziľudské interakcie.
   4. Zraniteľnosť voči propagande a manipulácii – simulácie vo VR môžu byť využité aj na formovanie postojov, posttraumatické podmieňovanie alebo indoktrináciu, napr. v kontexte radikalizácie alebo extrémistických ideológií.
   5. Vysoká cena zariadení – kvalitná VR technika je pre mnohých finančne nedostupná.
      1. Digitálna diskriminácia – nerovnaký prístup k technológii môže zvyšovať sociálne rozdiely.
4. Ochrana súkromia a bezpečnosť údajov
   1. Riziko zneužitia údajov – napríklad v prípade hackerského útoku alebo neoprávneného sledovania dieťaťa.
   2. V kombinácii s kamerou a mikrofónom môže dôjsť k zachytávaniu citlivých informácií bez vedomia dieťaťa z jeho okolia.
   3. Zber a zneužitie citlivých biometrických údajov – VR zariadenia často zaznamenávajú detailné informácie o pohyboch, výrazoch tváre, fyziologických reakciách či hlasovom prejave, čo otvára riziká narušenia súkromia a zneužitia údajov.

#### Rozšírená realita (Augmented Reality - AR)

Rozšírená realita spája fyzické prostredie s digitálnymi prvkami.

Rozšírená realita (nesprávne augmentovaná realita, angl. augmented reality, skr. AR) je priamy alebo nepriamy pohľad na fyzicky skutočné prostredie, ktorého časti sú v digitálnej, väčšinou textovej alebo obrazovej forme obohatené o dodatočné informácie relevantné k objektu, na ktoré sa človek pozerá. Tieto informácie sú získavané z rôznych informačných zdrojov za použitia off-line alebo on-line aplikácií. Obohatenie reality sa obvykle deje v reálnom čase a v sémantickom kontexte s časťami prostredia (napríklad aktuálna akcia v reštaurácii, najbližší bankomat, najbližší užívateľ Twitteru a podobne).[[69]](#footnote-69)

Rozšírená realita zväčša ovplyvňuje to, čo vidíme a počujeme, ale môže prebudiť aj ostatné zmysly (hmat, čuch či chuť). Rozšírená realita sa líši od virtuálnej reality (VR), ktorá vás len prenesie do 360-stupňového virtuálneho sveta, v tom, že pomocou virtuálnych informácií posunie vaše zážitky z reálneho sveta na novú úroveň.

Rozšírená realita funguje na základe mapovania trojrozmerných virtuálnych objektov, ktoré premieta do reálneho prostredia. Niektoré náhlavné súpravy pre rozšírenú realitu zobrazujú virtuálne objekty cez priehľadné objektívy, iné zasa prenášajú medzi divákom a fyzickým svetom živý kamerový záznam. Počítačové videnie (programovanie, ktoré počítaču umožňuje identifikovať a spracovať pohľad kamery) upraví dané 3D prostredie a umiestni doň digitálne prvky. Keďže tento digitálny obsah sa vykresľuje ešte rýchlejšie a presvedčivejšie, viac sa podobá na jeho inšpiráciu z reálneho sveta. [[70]](#footnote-70)

Známym príkladom je počítačová hra Pokémon Go zasadením hry do reálneho sveta (chytáte virtuálnych pokémov nachádzajúcich sa napr. na území vašej obce).

Hrozby a riziká

*Poznámka: doplnenie s využitím ChatGPT v. 4.5 (ako druhý názor)*

1. Riziká pre fyzické zdravie a bezpečnosť
   1. Používatelia môžu byť rozptýlení a nevnímať reálne hrozby (napr. autá, schody, ľudí).
   2. Zranenia spôsobené nepozornosťou, najmä pri používaní AR v pohybe.
   3. AR v doprave (napr. projekcia údajov do čelného skla) môže znižovať reakčný čas vodiča.
2. Riziká pre duševné zdravie
   1. Závislosť a narušenie kontaktu s realitou, hlavne pri dlhodobom používaní.
   2. Zrakové problémy (únava očí, bolesť hlavy) v dôsledku dlhého sledovania AR displejov.
   3. Znížená schopnosť sústrediť sa – obzvlášť nebezpečné pri chôdzi, šoférovaní alebo práci.
   4. Narušenie vnímania reality – pravidelné používanie AR môže viesť k narušeniu schopnosti rozoznávať hranicu medzi virtuálnym a reálnym svetom, najmä u detí a dospievajúcich.
   5. Falošná identita – ľudia sa prezentujú ako "lepší, krajší, populárnejší", než v skutočnosti.
   6. AR filtre menia vzhľad tváre alebo tela, čím môžu viesť k nerealistickým ideálom krásy (napr. zväčšené oči, zúžený nos, bezchybná pleť). To môže spôsobiť pri porovnávaní:
      1. nízke sebavedomie,
      2. body image problémy,
      3. zvýšené riziko porúch príjmu potravy (najmä u mladých dievčat).

Tento jav sa nazýva aj „Snapchat dysmorfia“ – ľudia chcú vyzerať ako filtrovaná verzia seba.

1. Sociálne a spoločenské riziká
   1. Konflikty v reálnom svete – niektoré AR hry využívajú spoločné herné miesta (napr. parky, pamiatky). Viacero hráčov na jednom mieste môže spôsobiť rušenie verejného poriadku alebo konflikty s inými občanmi.
   2. AR hry často obsahujú mikrotransakcie – kúpa herných predmetov, vylepšení, vstupov na špeciálne udalosti v rámci reálneho sveta.
      1. Detskí hráči si nemusia uvedomovať hodnotu peňazí a môžu míňať nadmerne.
   3. Vystavenie nevhodnému alebo traumatizujúcemu obsahu – v AR prostredí je možné pridávať aj extrémne realistické nevhodné zážitky (násilie, pornografiu, manipuláciu), ktoré môžu mať výrazný negatívny dopad na psychiku detí.
   4. Zraniteľnosť voči propagande a manipulácii – pridané informácie v AR aplikáciách môžu byť využité aj na formovanie postojov, posttraumatické podmieňovanie alebo indoktrináciu, napr. v kontexte radikalizácie alebo extrémistických ideológií (napr. bude informovať o výskyte minorít v blízkosti s negatívnym obsahom).
   5. Znížená kvalita medziľudských vzťahov, ak ľudia viac interagujú s digitálnymi prvkami než s okolím.
   6. AR efekty môžu byť vytvorené aj na zosmiešnenie, urážanie alebo manipuláciu (napr. falošné titulky, tváre, vyjadrenia).
   7. Digitálne rozdelenie – nie každý má rovnaký prístup k AR technológii, čo môže prehĺbiť nerovnosti.
   8. Manipulácia a dezinformácie – pomocou falošných digitálnych objektov alebo falošnej reality (deepfake AR).
2. Ochrana súkromia a bezpečnosť údajov
   1. AR zariadenia často zbierajú a analyzujú veľké množstvo osobných a lokalizačných údajov (napr. tváre, hlas, prostredie).
   2. Riziko zneužitia údajov – napríklad v prípade hackerského útoku alebo neoprávneného sledovania dieťaťa.
   3. Zariadenia môžu snímať okolité osoby bez ich súhlasu, čo predstavuje problém z pohľadu GDPR a etiky.
   4. AR hry často sledujú presnú GPS polohu hráča, čo môže byť zneužité (napr. na cielenú reklamu alebo krádež identity).
   5. V kombinácii s kamerou a mikrofónom môže dôjsť k zachytávaniu citlivých informácií bez vedomia používateľa.
3. Technické a právne riziká
   1. Nezrelosť technológie – chyby v zobrazovaní môžu viesť k chybným rozhodnutiam.
   2. Autorské práva a licencie – použitie digitálneho obsahu v reálnom svete môže porušiť duševné vlastníctvo.
   3. Nedostatok príslušnej legislatívy – právny rámec často nedrží krok s vývojom AR.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov oblasti hrozieb** (negatívne vplyvy v danej oblasti) | **Následok** | **Pravde-podobn.** | **Riziko** |
| 14.1 | Inteligentná technika | Z | VN | N |
| 14.2 | Roboty | Z | VN | N |
| 14.3 | Porno produkty na novej technologickej úrovni | Z | S | **V** |
| 14.4 | Sociálne siete - pokročilý digitálny obsah | Z | S | **V** |
| 14.5 | Civilné drony | Z | VN | N |
| 14.6 | Letálne autonómne zbrane | K | VN | S |
| 14.7 | Sektor neurónových technológií | Z | VN | N |
| 14.8 | Virtuálna realita | Z | N | S |
| 14.9 | Rozšírená realita | Z | N | S |

Poznámka: pravdepodobnosť uvádzame pre stav v roku 2025, s časom sa môže dynamicky meniť.

### Štandardné hrozby pre mládež ovplyvnené kybernetickým priestorom

V tejto kapitole uvádzame vybrané štandardné hrozby pre mládež, ktoré sú ovplyvňované aj kybernetickým priestorom resp. jeho digitálnym obsahom a interakciami v ňom.

Napr. alkohol je bežne propagovaný v digitálnych médiách. Skúsenosti s drogami si deti vymieňajú na sociálnych sieťach. Mnohé trestné činy sú nahrávané na mobily.

Primárny zdroj informácií: Výskumná správa „Vybrané formy rizikového správania detí a mládeže v roku 2023“ [[71]](#footnote-71)

Hrozby a riziká, najmä

1. Nezdravý životný štýl
   1. Nedostatok pohybu
   2. Nedostatok spánku
      1. Nekvalita spánku
   3. Nevhodná strava
      1. Používanie nevhodných výživových doplnkov
      2. Používanie anabolík
   4. Nevhodný pitný režim
      1. Sladené nápoje
      2. Energetické nápoje
      3. Kofeínové nápoje
   5. Obezita
2. Hrozby pre duševné zdravie
   1. Problémy s pozornosťou a sústredením
   2. Narušenie mentálnych schopností a zručností
   3. Dlhodobá frustrácia
   4. Úzkosť
   5. Depresia
   6. Nízke sebavedomie / sebaúcta / sebahodnotenie
   7. Sebapoškodzovanie
   8. Poruchy príjmu potravy
   9. Narušená emočná stabilita, nízka miera odolnosti, „snehové vločky“
   10. Znecitlivenie voči násiliu
   11. Sociálna úzkostná porucha (Social anxiety disorder – SAD)
       1. Osamelosť
3. Závislosti (mimo digitálnych závislostí), najmä
   1. Alkohol
   2. Tabakové výrobky
      1. Žuvací tabak
      2. Elektronické cigarety (vaping)
   3. Drogy
      1. Nové syntetické drogy
   4. Gambling
4. Trestná činnosť
   1. Páchanie trestnej činnosti deťmi (často zo sociálne narušeného prostredia)
   2. Deti ako obete trestnej činnosti
5. Agresia (mimo kybernetického priestoru, ale ním ovplyvnená)
   1. V rodine
   2. Nenávistné prejavy a konanie
   3. Nárast extrémnych postojov
   4. Nenávistné prejavy voči iným
   5. Útoky na školách (nôž, strelná zbraň)
   6. Šikana
   7. Diskriminácia
6. Partnerské vzťahy
   1. Problémy s hľadaním vhodného partnera
   2. Neschopnosť nadviazať normálne partnerské vzťahy
   3. Neschopnosť udržať partnerský vzťah
7. Strata pocitu bezpečia
   1. Doma (rodinné problémy)
   2. V škole (šikana)
   3. V spoločnosti (radikalizácia spoločnosti)
8. Existencionálne problémy
   1. Strata zmyslu života
   2. Snaha vyrovnať sa celebritám za každú cenu a frustrácia z neúspechu
   3. Filozofia „poslednej generácie“
   4. Ako reagovať na klimatickú zmenu
   5. Vlastná budúcnosť
   6. Obavy
      1. z chudoby
      2. chorôb
      3. o budúcu prácu (ohrozenú AI, robotmi)
      4. vojny

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** (negatívne vplyvy v danej oblasti) | **Následok** | **Pravde-podobn.** | **Riziko** |
| 15.1 | Nezdravý životný štýl | K | V | **VV** |
| 15.2 | Hrozby pre duševné zdravie | K | S | **V** |
| 15.3 | Závislosti | K | S | **V** |
| 15.4 | Trestná činnosť | Z | N | S |
| 15.5 | Agresia | Z | N | S |
| 15.6 | Partnerské vzťahy | K | S | **V** |
| 15.7 | Strata pocitu bezpečia | Z | N | S |
| 15.8 | Existencionálne problémy | Z | N | S |

### Špecifické riziká pre dievčatá

Jednou zo špecifických skupín v digitálnom ohrození sú dievčatá a mladé ženy (mládež - vek do 30 rokov). V tejto kapitole uvádzame riziká, ktoré sú pre túto skupinu špecifické alebo výraznejšie ako u chlapcov. Niektoré z nich boli uvedené všeobecne aj v predchádzajúcich kapitolách.

Táto podrobnejšie zameraná kapitola vznikla vďaka intenzívnej súčinnosti žien aj dievčat pracujúcich v oblasti manažmentu týchto rizík.

Obrázok, na ktorom je animák, ľudská tvár, ilustrácia, kresba

Obsah vygenerovaný pomocou AI môže byť nesprávny.

1. Nenávistné prejavy špecificky zamerané voči dievčatám a ženám v digitálnom priestore
   1. Myzogýnia (odpor, pohŕdanie, nenávisť, alebo predsudky voči ženám).
      1. Prezentované napr. influencermi ako je Andrew Tate [[72]](#footnote-72).
      2. Ten prezentuje mužov ako bojovníkov a ženy ako domestikované, podriadené služobníčky.
      3. Nastáva dramatický posun v online mizogýnii: posun od sexualizácie k povzbudzovaniu k rodovej nenávisti a násiliu.
   2. Prejavy toxickej maskulinity pri interakcii s dievčatami v kybernetickom priestore (najmä v časti predstavy, že muži by mali byť emocionálne bezcitní a behaviorálne agresívni).
2. Digitálne riziká v oblasti sexuality
   1. Dievčatá častejším cieľom a zraniteľnejšie v oblastiach:
      1. Sexuálnemu obťažovanie a grooming v online prostredí
      2. Vydieranie (sextortion)
         1. Po zaslaní intímnych fotografií nasleduje vyhrážanie zverejnením, ak neurobia ďalší krok.
      3. Zneužitie fotografií bez ich vedomia
         1. Uverejňovanie ich fotografií na porno stránkach alebo v meme skupinách.
      4. Nevyžiadaný sexuálny kontakt
         1. Napr. „dickpic“ aktivity od mužov
      5. Detská pornografia
         1. Na šírení detskej pornografie v digitálnom prostredí sa môžu aktívne podieľať aj deti (sexting na úrovni rovesníkov u mladších detí)
         2. Detská pornografia priamo šírená rodičmi, príbuznými
         3. Fyzické vyhľadanie dievčaťa na základe zdrojov detskej pornografie.
      6. Manipulácia a následný nábor v digitálnom prostredí na
         1. erotické telefónne hovory
         2. erotické video-hovory
         3. pornografické aktivity
         4. prostitúciu
         5. patologické sexuálne praktiky
      7. Obchodovaniu s deťmi
         1. Prvé kroky k náboru a zneužitiu stále častejšie sa realizujú v digitálnom prostredí.
   2. Deepfake videá so zneužitím fyzickej identity dievčaťa sú zamerané oveľa viac na dievčatá ako chlapcov (dnes stačí bežná fotografia dievčaťa na vytvorenie pornografického deepfake videa, ktoré je mu schopné zničiť život).
   3. Dievčatá sa stretávajú s pornografiou, v ktorej sú zobrazované ako zraniteľný či pasívny zdroj zábavy či zneužívania z pohľadu mužov.
   4. Ako ideál pre dievčatá je mnohými infliuencerkami podsúvané byť úspešná na základe príjmov z OnlyFans. Nakoľko konkurencia je veľká, vzniká tlak na prezentáciu stále extrémnejšieho sexuálneho obsahu.
   5. Upskirting [[73]](#footnote-73)
      1. Upskirting je nelegálne a nevhodné fotografovanie alebo natáčanie pod sukňou alebo šatami deivčaťa bez jej vedomia a súhlasu, často s cieľom získať zábery spodnej bielizne alebo intímnych častí tela a potom ich prípadne zverejniť.
   6. Tajne inštalované kamery v dievčenských šatniach, kúpeľniach, sprchách a záchodoch.
      1. Zneužitie fotografií a videí.
      2. Voyerizmus
         1. *Voyeurizmus je (podľa klasifikácia chorôb MKCH-10) "návratná alebo pretrvávajúca náklonnosť pozorovať ľudí pri sexuálnom akte alebo v intímnych situáciách, napr. pri vyzliekaní. Uskutočňuje sa to bez vedomia pozorovanej osoby a zvyčajne vedie k sexuálnemu vzrušeniu a masturbácii." Má číslo F65.3 a patrí medzi poruchy voľby sexuálneho objektu*
   7. Online zraniteľnosť dievčat kvôli rodičom (posmech, sexuálni predátori) – napr. keď od detstva rodičia postujú ich fotografie online (nahé dieťa, dieťa v znevažujúcej situácii)
   8. AI online partneri, vzťahovo a sexuálne zameraní AI chatboti nahrádzajúci budovanie reálnych partnerských vzťahov.
   9. Sexuálne násilie voči dievčatám v počítačových hrách a virtuálnych prostrediach – prostredníctvom násilia voči ich avatarom, postavách v hrách
      1. Hráči používajú postavy na simulovanie sexuálnych pohybov (napr. tzv. „virtual rape“ – virtuálne znásilnenie v hrách ako GTA, VRChat, Roblox, Minecraft) alebo virtuálnych prostrediach [[74]](#footnote-74)
      2. Sledovanie alebo "dotýkanie sa" jej avatarov bez súhlasu hráčky.
      3. Hrubé, vulgárne alebo sexuálne poznámky v chate alebo hlasovej komunikácii počas hrania.
   10. Hnutie a aktivity incelov zamerané proti dievčatám [[75]](#footnote-75)

*Spájajú ich pocity nenávisti voči ženám. Príčinou je odmietanie zo strany žien, ktoré vedie k nedobrovoľnému celibátu – preto názov incel (involuntary celibate).*

*Incelovia považujú sex za základné ľudské právo všetkých mužov. Ak im ho ženy odopierajú, páchajú podľa nich ohavný trestný čin, ktorý treba potrestať.*

1. Digitálne násilie vo vzťahoch
   1. Kontrola zo strany partnera
      1. Požiadavky na zasielanie intímnych fotografií ako „dôkaz lásky“
      2. Tlak na neustále zdieľanie polohy, hesiel, prístupov k účtom
      3. Zasahovanie do súkromia pod zámienkou „starostlivosti“
   2. Toxické vzorce správania sa medzi partnermi
      1. Zneužívanie fotografií, videa a súkromných správ po rozchode (napr. „revenge porn“)
      2. Vydieranie alebo manipulácia citmi dievčaťa – „ak ma naozaj miluješ, pošleš to“
   3. Emocionálne zneužívanie cez online kanály
      1. Neustála kritika vzhľadu, správania či kontaktov partnerky cez správy alebo sociálne siete
      2. ii. Striedanie láskyplného správania a komunikácie s trestajúcim tichom, výčitkami či ignoráciou
   4. Zneužívanie technológií na sledovanie a kontrolu
      1. Stalking partnerky cez technológie
      2. Inštalácia sledovacích aplikácií bez vedomia partnerky
      3. Zneužívanie funkcií zdieľania polohy (napr. v Snapchate, FindMyFriends)
   5. Zdieľané účty ako nástroj moci
      1. Sledovanie každého kroku a aktivity – kontrolovanie lajkov, komentárov, histórie
      2. Zákazy komunikácie s určitými ľuďmi, pod hrozbou „straty dôvery“
2. Násilie medzi dievčatami v online priestore
   1. Kyberšikana od rovesníčok
      1. Zverejňovanie súkromných informácií, „leaky“, zosmiešňovanie
      2. Zakladanie skupín zameraných na urážanie jedného konkrétneho dievčaťa (napr. tajné IG profily)
   2. Online ponižovanie a sociálne vylúčenie
      1. Neprizvanie na skupinové chaty, spoločné výzvy či videá ako forma trestu.
      2. Zdieľanie „inside joke“ obsahu, ktorému dievča nerozumie, ale je jeho cieľom.
3. Sociálne siete a ich negatívne dopady
   1. Neustále porovnávanie sa s ideálmi krásy a životného štýlu
      1. Instagram, TikTok či Snapchat posilňujú nereálne predstavy o výzore a živote, ktoré dievča nevie dosiahnuť a vedie to k jeho dlhodobej frustrácii.
      2. Zníženie sebadôvery a telesného sebahodnotenia.
      3. Algoritmy a fitfluenceri podporujú obsah, ktorý môže pôsobiť škodlivo
         1. Tiktok "beauty trendy" spôsobujúce alergie, rakovinu kože (opaľovanie, bielidlá, kyselinové peelingy) [[76]](#footnote-76)
         2. Propagácia diét nevhodných pre mladé dievčatá (veganizmus, fruktariánstvo, mäsová diéta) [[77]](#footnote-77)
   2. Body shaming
      1. je hanlivé alebo ponižujúce komentovanie telesného vzhľadu inej osoby
         1. U dievčat sa vyskytuje oveľa častejšie. Je to forma šikany, ktorá sa zameriava na váhu, proporcie, tvary alebo akékoľvek iné telesné črty, a to bez ohľadu na to, či sú reálne alebo domnelé.
         2. *Vekovo najzraniteľnejšia skupina je vo veku puberty. V tomto veku stačí veľmi málo, aby si dospievajúce dievča vytvorilo o sebe negatívny obraz.*
         3. Body shaming má negatívny vplyv na duševné zdravie a sebavedomie dievčaťa, ktoré je jeho terčom.
         4. Necitlivé komentáre môžu viesť k rozvoju depresie a porúch príjmu potravy.
   3. Propagácia
      1. anorexie,
      2. bulímie,
      3. sebapoškodzovania.
   4. Sinejšia závislosť od lajkov a spätnej väzby; mnohé dievčatá sa dostali do stavu, že sa cítiia ako hodnotné len vtedy, keď dostávajú dostatok pozornosti online.
   5. Pocit, že musí byť stále „online“, odpovedať, reagovať, následné digitálne vyhorenie a stres z neustáleho spojenia.
4. eShopy, často previazané na sociálne siete cez influencerov
   1. Propagácia a online zásielky s nekontrolovanymi liekmi / supplementmi (chudnutie, potratové pilulky, stimulanty)
   2. Podpora vytvárania závislosti na on-line nakupovaní
   3. Ponuka škodlivých výrobkov
5. Narušenia ochrany osobných údajov u tretích strán
   1. Únik / hack zdravotných záznamov o dievčati od poskytovateľa zdravotnej starostlivosti a ich následné zneužitie (napr. gynekologické vyšetrenia potraty)
   2. Únik / hack informácií o DNA a z toho vyplývajúcich rizikách v rámci genetických testov a ich následné zneužitie [[78]](#footnote-78)
   3. Hacknutie priamo cloudových úložísk, kde má dievča uložené súkromné fotografie a videá
   4. Ponúkanie informácií o správaní sa dievčaťa ako spotrebiteľa tretím stranám (napr. zo strany sociálnych sietí)
6. Manipulatívne skupiny, propagácia a lákanie nových členov v digitálnom priestore
   1. Spirituálne skupiny
   2. Sekty [[79]](#footnote-79)
   3. Extrémne aktivistické skupiny [[80]](#footnote-80)
   4. Samozvaní guruovia [[81]](#footnote-81)
7. Agresia / násilie
   1. Kyberšikana
   2. S podporou digitálnych technológií
      1. stalking resp. / kyberstalking
         1. *Stalking je dlhodobé, opakované a neželané sledovanie, obťažovanie alebo kontaktovanie inej osoby, ktoré spôsobuje strach, stres alebo narušenie súkromia.*
      2. Obsesívne prenasledovania (blízke stalkingu)
         1. *Obsesívne prenasledovanie je forma chorobného a opakovaného sledovania alebo obťažovania, ktorá sa prejavuje nutkavou posadnutosťou určitou osobou. Prenasledovateľ má patologickú potrebu byť v kontakte, ovládať alebo získať pozornosť obete – aj proti jej vôli.*
      3. Happy slapping
         1. *Happy slapping je forma násilného a ponižujúceho správania, pri ktorom útočník (alebo skupina) fyzicky napadne nič netušiacu obeť a celý incident natočí na mobilný telefón, aby ho mohol zdieľať na internete alebo poslať ďalej.*
      4. Používanie obscénneho jazyka voči dievčatám a ženám v digitálnom priestore (napr. v bežnom chate, diskusnom fóre)
   3. Nadmerné divácke násilie, kde obeťami sú dievčatá a mladé ženy.
      1. Zvyšovanie tolerancie voči diváckemu násiliu voči ženám.
   4. Stigmatizácia obete v digitálnom prostredí.
      1. Obete sú často obviňované alebo zahanbované
         1. Muži často kritizujú obeť, nie páchateľa (victim blaming) – napr. pri znásilnení.
      2. *Často chýba informovanosť o právach a možnostiach pomoci, ako sa brániť a komu dôverovať.*
   5. Nemieste žarty (pranks) publikované v digitálnom priestore, v ktorých je dievča zhadzované alebo je mu reálne ubližované.
8. Digitálna únava a strata identity
   1. Znižovanie schopnosti byť sama so sebou
      1. Neustále porovnávanie sa vedie k strate kontaktu s vlastným prežívaním
      2. Online priestor formuje predstavu o tom, kým by dievča „malo byť“, nie kým chce byť.
   2. Strach z offline sveta
      1. Úzkosť z ticha, prestávok a neustále potreby byť k dispozícii
      2. Vyčerpanie z permanentnej online dostupnosti

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** (negatívne vplyvy v danej oblasti) | **Následok** | **Pravde-podobn.** | **Riziko** |
| 16.1 | Nenávistné prejavy špecificky zamerané voči dievčatám a ženám | Z | S | **V** |
| 16.2 | Digitálne riziká v oblasti sexuality | Z | S | **V** |
| 16.3 | Digitálne násilie vo vzťahoch | Z | N | S |
| 16.4 | Násilie medzi dievčatami v online priestore | Z | N | S |
| 16.5 | Sociálne siete | K | V | **VV** |
| 16.6. | eShopy | Z | N | S |
| 16.7. | Narušenia ochrany osobných údajov u tretích strán | Z | N | S |
| 16.8. | Manipulatívne skupiny | Z | N | S |
| 16.9. | Agresia / násilie | Z | S | **V** |
| 16.10. | Digitálna únava a strata identity | Z | N | S |

### Špecifické riziká pre chlapcov

Aj chlapci majú svoje špecifické riziká v digitálnom svete. V tejto kapitole uvádzame riziká, ktoré sú pre túto skupinu špecifické alebo výraznejšie ako u dievčat. Niektoré z nich boli uvedené v predchádzajúcich kapitolách.

1. Podpora nezdravého správania sa
   1. Toxická maskulinita prezentovaná v kybernetickom priestore, okrem negatívneho pôsobenia na dievčatá má aj nasledujúce negatívne dopady:
      1. Predstava, že „starostlivosť o seba je pre ženy“ a muži by sa mali správať k svojmu telu ako k strojom tým, že budú šetriť spánkom, cvičiť aj keď sú zranení či posúvať svoje fyzické hranice.
      2. Toxická maskulinita vedie občas k vyhýbaniu sa preventívnej liečbe; podporuje aj nezdravé správanie - čím viac sa muži prispôsobujú mužským normám, tým je pravdepodobnejšie, že istá časť sa zapojí do rizikového správania, ako je nadmerné pitie alkoholu, užívanie tabaku a drog.

*Poznámka: odmietanie toxickej maskulinuty neznamená odmietnutie mužnosti.*

* + 1. Iným trendom je venovať všetok svoj voľný časť starostlivosti o svoje telo (extrémne cvičenie, upravený výzor) a pohŕdať tými, ktorí tak nečinia.
  1. V kybernetickom priestore prezentované hnutie a aktivity incelov okrem zamerania proti dievčatám, má negatívne dopady aj na chlapcov

*Spájajú ich pocity nenávisti voči ženám a sexuálne úspešným mužom.*

* + 1. Jednoduché zdôvodnenie svojho neúspechu vo vzťahu k dievčatám a rezignácie na pozitívnu zmenu.
    2. Navádzanie na samovraždy v prípade totálneho neúspechu u dievčat.

1. Nadmerné hranie a následná závislosť na počítačových hrách

*U chlapcov sa vyskytuje podstatne častejšie ako u dievčat (aj keď tie ich už začínajú dobiehať).*

* 1. Nadmerné hranie hier (napr. FPS, MMORPG) vedie k zanedbávaniu školy, spánku či sociálnych vzťahov.
  2. Herná závislosť u časti chlapcov (gaming disorder)
     1. WHO uznala hernú závislosť ako psychickú poruchu [[82]](#footnote-82) – častejšia je práve u chlapcov.
  3. Únik od reality a emócií
     1. Digitálne prostredie sa stáva priestorom, kde chlapec uniká pred problémami či stresom.
  4. Dlhodobé hranie nevhodných hier
     1. Strieľačky, survivals či horory sú omnoho častejšie hrané chlapcami. Mnohí z nich tomu venujú neprimerane veľa času, čo sa odráža na ich psychike.

1. Oblasť sexuality
   1. Chlapci sa stretávajú s pornografiou v stále nižšom veku, v ktorej sú dievčatá a ženy zobrazované ako zraniteľný či pasívny zdroj zábavy či zneužívania z pohľadu mužov.
      1. Ovplyvňuje to ich pohľad na ženy, vzťahy a sexualitu.
   2. Sexuálne nevhodné prezentácie dievčat a žien na OnlyFans ich utvrdzujú v  ich skreslených predstavách o dievčatách a ženách.
   3. Vzťah medzi mužom a ženou je redukovaný na sexuálny styk, často vulgárny a násilný. Dopad tohto je napr. neúspech u dievčat, neschopnosť nadviazať a udržať partnerský vzťah, prípadne pripojenie sa k hnutiu incelov.
2. Porovnávanie sa a tlak na výkon
   1. Vytváranie nereálnych štandardov úspechu
      1. Online priestor ukazuje úspešných mladých mužov, ktorí „zarábajú, cestujú, majú všetko“ – čím vzniká u bežného chlapca pocit osobného zlyhania, menejcennosti, hanby
      2. Vzniká tlak na rýchly úspech aj použitím nelegálnych ciest (napr. ako drogový díler).
   2. Tlak na fyzický vzhľad a výkonnosť prezentovaný na sociálnych sieťach
      1. Vzrastá počet chlapcov s užívaním steroidov – najmä v súvislosti s kulturistikou.
      2. Algoritmy ponúkajú doplnky, jedálničky a „návody“ – často bez odbornej garancie.
3. Potlačenie duševných ťažkostí
   1. Chlapci nevyhľadávajú odbornú pomoc
      1. Mnohí ani nevedia, že môžu – alebo si myslia, že „to musia zvládnuť sami“ - ako to prezentujú mnohí influenceri.
      2. Duševné ťažkosti sa prejavujú neskôr a intenzívnejšie – najmä formou výbuchov, únikov a somatizácie.
   2. Vyššie riziko samovražedného správania
      1. V populácii mladých mužov je vyššie percento dokonaných samovrážd
      2. To, čo tomu predchádza je zo strany chlapcov utajované.
   3. Emocionálna izolácia a internalizácia problémov
      1. Absencia vzorov emocionálne zrelých mužov v prostredí napr. Tiktoku.
      2. Hromadenie frustrácie a zlosti
      3. Namiesto otvoreného rozhovoru sa problémy ventilujú cez výbuchy hnevu, agresívne komentáre, dehumanizáciu iných online.
      4. Riziko nárastu nenávistných postojov voči rôznym skupinám – ženám, menšinám, spolužiakom, iným mužom.
4. Radikalizácia prostredníctvom digitálneho priestoru
   1. Vplyv mužských influencerov so škodlivou agendou
      1. Online kurzy „mužnosti“ s radikalizujúcimi prvkami
      2. Mnohé z nich obsahujú mizogýniu, nadradenosť nad ostatnými.
      3. Znie to ako osobný rozvoj, no často vedie k izolácii a nenávisti.
   2. Vstup do extrémistických online komunít
      1. Chlapci hľadajúci silu, identitu a porozumenie môžu byť zlákaní do skupín, ktoré ponúkajú „jednoduché“ odpovede a nepriateľa
         1. Napr. skupiny pre nábor budúcich teroristov
      2. Tieto skupiny využívajú frustráciu z neúspechu, osamelosti či odmietnutia – a premieňajú ich na hnev voči systému alebo určitým skupinám.
   3. Vplyv memov, hier a humoru
      1. Nenávistný alebo radikalizujúci obsah je často zabalený ako „vtip“ – a tak sa dostáva cez monitoring radikalizujúceho obsahu.
5. Sociálna a právna oblasť
   1. Riziko právnych dôsledkov
      1. Zdieľanie nevhodného obsahu môže byť nezákonné – chlapci často nerozumejú hraniciam, kedy ide o trestný čin, napr. detskej pornografie.
   2. Chýbajúca prevencia zameraná na chlapcov
      1. Mnohé programy sa sústreďujú len na ochranu dievčat, nie na vzdelávanie a podporu chlapcov.
   3. Stigma „slabosti“ bráni chlapcom hovoriť o problémoch
      1. Boja sa, že budú zosmiešnení, ak sa zdôveria s emocionálnym alebo digitálnym problémom.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kód hrozby** | **Názov hrozby** (negatívne vplyvy v danej oblasti) | **Následok** | **Pravde-podobn.** | **Riziko** |
| 17.1 | Podpora nezdravého správania sa | Z | S | **V** |
| 17.2 | Nadmerné hranie a následná závislosť na počítačových hrách | Z | S | **V** |
| 17.3 | Digitálne riziká v oblasti sexuality | Z | S | **V** |
| 17.4 | Porovnávanie sa a tlak na výkon | Z | N | S |
| 17.5. | Potlačenie duševných ťažkostí | Z | N | S |
| 17.6. | Radikalizácia prostredníctvom digitálneho priestoru | K | N | **V** |
| 17.7 | Sociálna a právna oblasť | Z | N | S |

## Závislosti medzi vybranými rizikami

V tejto kapitole sú uvedené rozšírenia analýzy rizík nad rámec metodík MIRRI a NBÚ (v duchu ISO 31000).

### Najvýznamnejšie riziká pre mládež v kybernetickom priestore

V tejto kapitole je uvedený návrh zoznamu najvýznamnejších rizík pre mládež v súvislosti s kybernetickým priestorom. Vychádza z predchádzajúcich podkapitol. Bude predmetom širšej spoločenskej diskusie a následne revízie.

1. Časovo nadmerné využívanie digitálnych technológií mládežou.
2. Nevhodné využívanie digitálnych technológií mládežou a z toho vyplývajúce negatívne dopady *(napr. dlhodobé sledovanie krátke Tik Tok videí, sledovanie negatívne pôsobiacich influencerov, flameware na sociálnych sieťach).*
3. Rizikové využívanie digitálnych technológií mládežou a z toho vyplývajúce negatívne dopady *(napr. minimálne zabezpečenie počítača / mobilu, návštevy rizikových webových stránok, zdieľanie citlivého obsahu, žiadne zálohovanie)*
4. Vznik nelátkových závislostí u časti mládeže s nadmerným využívaním digitálnych technológií.
5. Toxický obsah v kybernetickom priestore dostupný mládeži.
6. Negatívny vplyv sociálnych sietí na duševné zdravie mládeže.
7. Negatívne vplyvy digitálnych technológií (najmä pornografie) na sexualitu mládeže.
8. Negatívne vplyvy využívania AI technológií.
9. Kyberšikana.
10. Kybernetické útoky (najnovšie aj s využitím AI).
11. Malvér napádajúci digitálne zariadenia.
12. Strata digitálneho obsahu (napr. čo má dieťa na mobile – kontakty, videá, fotografie, texty)

### Analýza závislostí medzi vybranými rizikami a ich opis

V tejto kapitole sú analyzované závislosti medzi vybranými rizikami v zmysle metodiky RIM (Risk Interconnection Map) Svetového ekonomického fóra – viď kap. 8.1.

Obrázok, na ktorom je snímka obrazovky, text, diagram, rad

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.

#### Nadmerné používanie digitálnych technológií

Istým spôsobom je centrom všetkých závislostí medzi rizikami. Znížením tohto rizika znižujeme množstvo ďalších súvisiacich rizík.

Vzťahy k ďalším významným rizikám:

* Vznik nelátkových závislostí – nadmerné používanie DT je predpokladom pre vznik nelátkovej závislosti. Nie každé nadmerné používanie DT vedie k vzniku nelátkovej závislosti.
* Toxický obsah v KP – ak je málo času na DT, je málo času aj na negatívne pôsobenie toxického obsahu. Sú vyššie priority – komunikácia s priateľmi / spolužiakmi, hranie hier, sledovanie oblastí bežného záujmu.
* Nevhodné využívanie DT - ak je málo času na DT, je málo času aj na negatívne pôsobenie nevhodného využívania DT.
* Strata digitálneho obsahu - nadmerné používanie DT vedie k nárastu závislosti na DT. S rastom závislosti rastie dopad straty digitálneho obsahu.
* Malvér útoky - nadmerné používanie DT častejšie vedie k návštevám webových stránok, ktoré sú zdrojom malvéru.

Doplnkové informácie

Mobily sa dostávajú k deťom najčastejšie vo veku 8 -9 rokov [[83]](#footnote-83).

Obrázok, na ktorom je text, diagram, písmo, pestrofarebnosť

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Nie všetci rodičia kupujú deťom ako prvý smartfón - takto sa rozhodne 41,2 % opýtaných rodičov. Ale 38,2 % z nich ako prvé zariadenie pre svoje deti volí radšej tablet a 15 % zase inteligentné hodinky. Notebook je až na štvrtom mieste.

Obrázok, na ktorom je text, snímka obrazovky, písmo, diagram

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Údaje o veku dieťaťa, keď dostane mobil, z Nemecka (r. 2025) [[84]](#footnote-84):

Obrázok, na ktorom je text, snímka obrazovky, štvorec, diagram

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Údaje z Veľkej Británie [[85]](#footnote-85)

Obrázok, na ktorom je text, písmo, snímka obrazovky, rad

Obsah vygenerovaný pomocou AI môže byť nesprávny.

#### Nevhodné využívanie DT

* Vznik nelátkových závislostí – nevhodné využívanie DT podporuje vznik nelátkových závislostí. Ide najmä o sociálne siete využívané nad rámec lokálnej komunikácie v rámci komunity a počítačové hry s podporou vzniku závislosti *(kooperatívne hranie v komunite, odmeny za čas venovaný hre a pod.).*
* Negatívne vplyvy AI často vznikajú jej nevhodným používaním - napr. ako náhrada samostatnej práce žiaka.

**Rizikové využívanie digitálnych technológií**

* Hackerské útoky – nechránený počítač alebo mobil dieťaťa a nedostatok skúseností s kybernetickou bezpečnosťou.
* Hackerské útoky – ľahšia šanca na hackerský útok pri nedostatočnej úrovni bezpečnosti

## Scenáre

Podľa § 6, ods. (7) vyhlášky 362/2018 Z. z.

„Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti. Na určenie úrovne identifikovaného rizika sa vopred nastaví súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov určiť merateľné a objektívne úrovne rizika pre najhoršie scenáre.“

### Najhoršie scenáre

Podľa Geoffreyho Hintona - nositeľa Nobelovej ceny, že pravdepodobnosť, že umelá inteligencia prinesie pre ľudstvo katastrofu, je vyššia, než sa doposiaľ predpokladalo. Väčšina odborníkov v AI sa zhoduje na tom, že nie sme tak ďaleko od času, keď AI systémy dosiahnu úroveň ľudskej inteligencie a dokonca ju prekročia v priebehu najbližších dvoch desaťročí.

Najhorší scenár je publikovaný v rámci štúdie AI 2027 [[86]](#footnote-86) - pravdepodobnosť vzniku AGI (Artificial General Intelligence, čo je zatiaľ hypotetická úroveň AI nadradená človeku) do roku 2027 je cca. 50 percent. Pravdepodobnosť, že AGI zničí alebo ťažko poškodí ľudstvo, je cca. 70 percent.

„Roboti vyrobení v špeciálnych ekonomických zónach a riadení umelou inteligenciou teraz dokážu zastávať takmer akúkoľvek ľudskú prácu. Vyzerá to, že nastane raj mieru a hojnosti. Táto ilúzia je však krátkodobá. Začiatkom tridsiatych rokov už zreteľne ubúda zón, kde môžu ešte žiť ľudia. Robotov pribúda. Keď sa nakoniec proti nim zdvihne vlna odporu, roboti rýchlo vyhubia zvyšok ľudstva novovyrobenými biologickými zbraňami.“

Týmto scenárom sa v našom dokumente ďalej nezaoberáme, pretože riadenie tohto rizika je nad rámec možností SR.

### Nepriaznivé scenáre

Nepriaznivé scenáre vychádzajú z predpokladu, že v najbližšej dobe bude narastať:

* nadmerné, nesprávne a nevhodné využívanie digitálnych technológií mládežou a z toho vyplývajúce negatívne dopady,
* vplyv sociálnych sietí a toxického obsahu,
* miera závislosti detí na digitálnych technológiách až na úroveň nelátkových závislostí,
* masívne využívanie AI mládežou nevhodným spôsobom
* sofistikované kybernetické útoky s využitím AI viazané na získanie benefitov pre útočníka,
* sofistikovaný malvér napádajúci zariadenia používateľov.

a nepodarí sa postačujúco implementovať primerané bezpečnostné opatrenia najmä v oblastiach:

* vzdelávanie rodičov v oblasti rizík digitálnych technológií pre ich deti (naj nich samých),
* časové obmedzenie používania digitálnych technológií,
  + obmedzenie používania mobilov na ZŠ a SŠ aj v domácnosti
* lepšie riadenie prístupu mládeže k digitálnym technológiám,
  + efektívne overenie veku používateľa sociálnymi sieťami a komunikačnými aplikáciami,
* kontrola toxického obsahu a aktivít zo strany rodičov alebo nimi akceptovaných aplikácií,
* trestné postihy kybernetických útočníkov porušujúcich legislatívu a ochranu ľudských práv.

Tieto predpoklady znamenajú, že v nepriaznivých scenároch budú všetky identifikované riziká rásť.

Nasleduje rámcový prehľad negatívnych dopadov v rámci týchto scenárov.

**Zhoršovanie zdravotného stavu mládeže aj celej populácie**

Podľa toho scenára nadmerný čas strávený s digitálnymi technológiami bude narastať (u detí aj ich rodičov). Negatívne zdravotné dopady tohto trendu sú uvedené v kap. 2.4 – ide o nezdravý životný štýl s následným narušením a poškodením zdravia.

Presnejšie čísla a kvantifikovaný odhad trendov je záležitosť Úradov verejného zdravotníctva - odborné útvary hygieny detí a mládeže, ktoré plnia úlohy štátu v oblasti verejného zdravotníctva spočívajúce v podpore a ochrane zdravia detí a mládeže.

Aké môžu byť následky tohto trendu? Jedným z nich je problém udržať súčasnú úroveň zdravotnej starostlivosti v dôsledku rastúceho rozporu medzi zdrojmi v zdravotníctve a zdravotnými potrebami občanov. Klasický model solidárneho zdravotníctva je založený na predpoklade relatívneho zdravia mládeže a pracujúcej populácie a dobrej demografickej situácie (pomer pracujúcich k dôchodcom). Konzumácia zdravotnej starostlivosti nastáva v staršom veku (zvyčajne v posledných 5 rokoch života). Ak významná časť mladej populácie sa dostane do štádia chronickej choroby, zvýšené požiadavky na zdravotnú starostlivosť budú nie 5, ale 50 rokov.

Ako príklad uveďme diabetes (cukrovku) [[87]](#footnote-87). Podľa najnovších údajov NCZI pribúda diabetikov 1. typu v strednom veku, ako aj detí odkázaných na inzulín. Kým v roku 1980 bolo na Slovensku lekármi sledovaných 122 197 diabetikov, v roku 2022 to už bolo 349 595, čo je nárast o takmer 230-tisíc osôb.

Ročné náklady na diabetes presahujú 800 mil. euro. Slovákov, u ktorých bol zistený predbiabetes, je takmer 140-tisíc. „Ak sa nepodniknú žiadne kroky a zmeny životného štýlu, približne 5-10 percent z týchto ľudí každý rok prejde do cukrovky 2. typu,“. [[88]](#footnote-88)

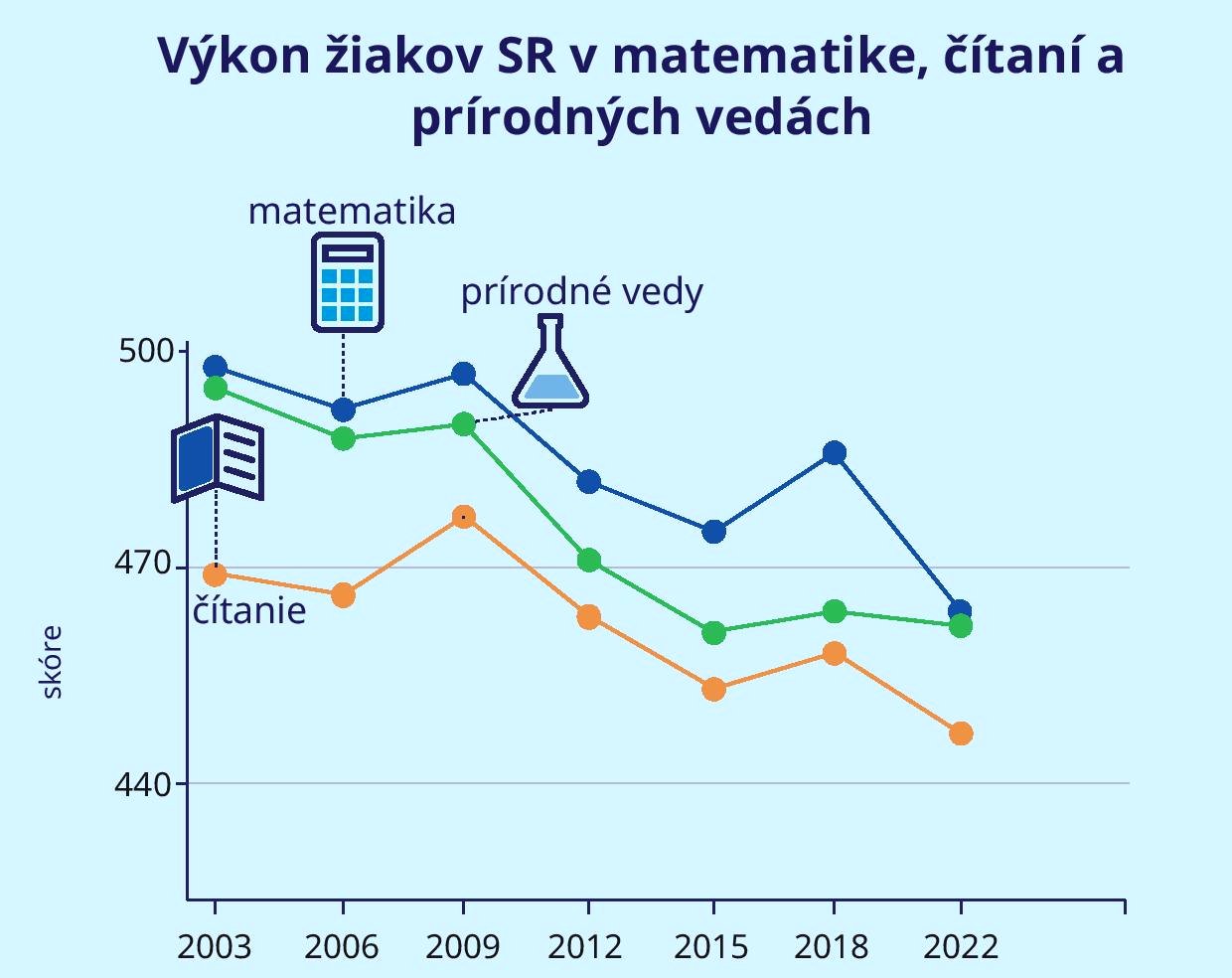
Pre pacientov s cukrovkou 1. typu priemerné ročné náklady v roku 2022 boli nad 3 800 eur. Pre pacientov s diabetom 2. typu boli náklady na jedného pacienta v roku 2022 takmer 2 600 eur.

**Pokles úrovne mentálnych schopnosti a zručností**

V roku 2024 OECD vydala štúdiu s názvom Zručnosti dospelých v oblasti čítania, písania a matematiky – tie vo väčšine krajín OECD **klesajú** alebo stagnujú. V celkových výsledkoch Slovensko obstálo zle a skončilo pod priemerom OECD.

Porovnanie súčasného a predchádzajúceho prieskumu vykonaného zhruba pred desiatimi rokmi ukazuje, že Slovensko, Maďarsko a Poľsko zaznamenali najväčší pokles v čitateľskej aj matematickej gramotnosti. Ak sa tento trend potvrdí aj pri ďalšom prieskume koncom dekády, Slovensko sa pravdepodobne ocitne blízko dna rebríčka OECD. [[89]](#footnote-89) [[90]](#footnote-90)

Mladá generácia oproti dospelým je v oblastiach čítania s porozumením aj písania na tom horšie, ako terajšia generácia dospelých. V rámci sociálnych sietí, mobilnej komunikácie či počítačových hier je komunikácia veľmi zjednodušená, s nízkou slovnou zásobou a jednoduchými vetami.



Výsledky medzinárodnej štúdie PISA 2022

Zdroj: NIVAM - Národný inštitút vzdelávania a mládeže

*Ďalšie oblasti budú doplnené na základe podnetov a pripomienok.*

# Analýza potrieb a očakávaní

V tejto kapitole sú uvedené identifikované potreby a očakávania jednotlivých subjektov z hľadiska bezpečnosti mládeže v kybernetickom priestore alebo eliminácie možných negatívnych dopadov kybernetického priestoru na mládež. Je dôležité to identifikovať, aby bolo možné navrhnúť prioritné bezpečnostné opatrenia (napĺňajúce potreby a očakávania jednotlivých skupín).

V potrebách a očakávaniach berieme ako referenčný bod rodiča, ktorý má úprimný záujem o svoje dieťa a jeho bytie a rozvoj a je si do istej miery vedomý rizík pre jeho dieťa v kybernetickom priestore a spoločnosť, ktorá má záujem na rozvoji mladej generácie a jej ochrane.

## Úvodné informácie o potrebách a očakávaniach

**Vymedzenie pojmu**

1. Potreba je uvedomený alebo neuvedomený nedostatok uspokojenia ( v biologickej či sociálnej dimenzii).[[91]](#footnote-91)
2. Potreba osoby je vymedzená jej vnútorným stavom, hodnotami a vonkajšími podmienkami.
3. Voči uvedomeným potrebám existujú u ich nositeľa očakávania ohľadom spôsobu ich naplnenia.
4. Očakávania sú vyjadriteľné vo forme požiadaviek na správanie sa okolia, spôsob jeho interakcie s danou osobou, očakávané externé benefity, práva, služby.
5. Uspokojenie potreby sa môže uskutočniť interne alebo externe prostredníctvom poskytnutých aktivít, plnení, služieb.

**Potreby fyzickej osoby (občana / dieťaťa)**

Maslowova pyramída potrieb [[92]](#footnote-92) delí potreby do 5 úrovní.

1. Fyziologické potreby
   1. potreba dýchania
   2. potreba regulácie telesnej teploty
   3. potreba vody
   4. **potreba spánku**
   5. potreba prijímania potravy
   6. potreba vylučovania
2. Potreby bezpečia a istoty
   1. istota zamestnania
   2. istota príjmu a prístupu k zdrojom
   3. **bezpečnosť - ochrana pred násilím a agresiou**
   4. **morálna a fyziologická istota**
   5. **istota rodiny**
   6. **istota zdravia**
3. **Potreba** lásky, prijatia, **spolupatričnosti**
4. **Potreba uznania**, úcty
5. **Potreba sebarealizácie**

Pre riziká kybernetického priestoru sú priamo alebo nepriamo relevantné všetky úrovne Maslowovej pyramídy potrieb. Aké sú možné dopady na tieto potreby pôsobením hrozieb kybernetického priestoru?

**Potreba bezpečia a istoty**

Túto potrebu vedia narušiť hrozby z kybernetického priestoru v každej oblasti množstvom spôsobov:

1. Istota zamestnania (návštevy školy v prípade žiaka):
   1. Nadmerné nevhodné používanie digitálnych technológií, nelátkové závislosti môžu túto istotu výrazne narušiť (neúspech v prijímacom konaní, prepadnutie ročníka, prerušenie štúdia, zanechanie štúdia, vylúčenie zo školy).
2. Istota príjmu a prístupu k zdrojom:
   1. Úspešný hacking, podvody s investíciami, gambling, sociálne manipulácie vedia pripraviť rodinu o významné finančné zdroje a narušiť jej finančnú stabilitu. Nelátkové závislosti môžu viesť k strate zamestnania rodičov.
3. Bezpečnosť - ochrana pred násilím a agresiou:
   1. Násilie a agresia v kybernetickom priestore sa prejavuje napr. kyberšikanou, sexuálnym obťažovaním a zneužívaním, ohováraním, osočovaním, prezentovaním nenávisti, vydieraním, dehumanizáciou, nenávistným internetovým obsahom, narúšaním psychického stavu dieťaťa, systematickou mikroagresiou. Potreba ochrany pred týmito hrozbami je u dieťaťa využívajúceho digitálne technológie veľmi výrazná.
4. Morálna a fyziologická istota:
   1. Pôsobením nevhodného, agresívneho, škodlivého internetového obsahu môže dochádzať k narušenou morálnych hodnôt a istôt dieťaťa.
5. Istota rodiny:
   1. Rodičia alebo dieťa so závislosťami (gambler v KP, nelátkové závislosti), pôsobenie škodlivého internetového obsahu vedúceho k divergencii hodnotových systémov členov rodiny, neschopnosť na úrovni dieťaťa a rodiny chrániť sa pred hrozbami kybernetického priestoru vedie k výraznému narušeniu istoty rodiny.
6. Istota zdravia:
   1. Nelátkové závislosti ohrozujúce zdravie dieťa vedia významným spôsobom narušiť potrebu zdravia a zdravého vývoja.

**Ďalšie potreby**

1. Potreba lásky, prijatia, spolupatričnosti
   1. Nenávistný obsah na internete, kyberšikana, digitálne vylúčenie, ohováranie osočovanie, dehumanizáciou, a ďalšie hrozby vedia plne narušiť napĺňanie potreby lásky, prijatia, spolupatričnosti dieťaťa.
   2. Potreba prijatia a spolupatričnosti vedie k snahe byť vo virtuálnych skupinách. Preferovanými sa stanú tie, ktoré vedia pocit prijatia navodiť (aj keď to môže byť len zdanlivé). Negatívne orientované komunity vytvárajú tlak na účastníka, aby prejavil svoju spolupatričnosť voči skupine viditeľným spôsobom.
2. Potreba uznania, úcty
   1. Kyberšikana, digitálne vylúčenie, ohováranie osočovanie, dehumanizácia a ďalšie hrozby vedia plne narušiť napĺňanie potreby uznania a úcty dieťaťa v reálnych aj virtuálnych kolektívoch.
3. Potreba sebarealizácie
   1. Nadmerné používanie digitálnych technológií, nelátkové závislosti, negatívne pôsobenie hrozieb kybernetického priestoru môže výrazným spôsobom narušiť sebarealizáciu dieťa.

V nasledujúcich podkapitolách sú uvedené konkrétne identifikované potreby a súvisiace očakávania rôznych subjektov relevantných pre dieťa / žiaka.

## Rodič

V potrebách a očakávaniach berieme ako referenčný vstup rodiča, ktorý má úprimný záujem o svoje dieťa a jeho bytie a rozvoj a aktívne sa zapája do vzdelávacieho procesu. U mnohých rodičov niektoré z uvedených potrieb a očakávaní absentujú.

1. Vo vzťahu k škole očakáva:
   1. Aby v škole bolo bezpečné prostredie pre jeho dieťa, vrátane bezpečnosti v kybernetickom priestore.
   2. Aby digitálne technológie používané vo vzdelávacom procese boli pre jeho dieťa prínosom.
   3. Aby získalo adekvátne vedomosti, schopnosti a zručnosti práce s digitálnymi technológiami a aplikáciami vrátane kybernetickej bezpečnosti.
   4. Byť informovaný o:
      1. priebežných študijných výsledkoch jeho dieťaťa,
      2. prípadných problémoch s dieťaťom,
      3. dianí na škole.
   5. Mať možnosť obojstrannej komunikácie s pedagógmi a vedením školy aj prostredníctvom digitálnych technológií, napr.
      1. pri riešení problémov so žiakom – jeho dieťaťom
      2. pri konzultáciách k učivu
2. V domácnosti potrebuje:
   1. Mať dostatok vedomostí a možností, aby vedel v domácnosti vytvoriť bezpečné prostredie pre dieťa z hľadiska jeho bezpečnosti v kybernetickom priestore.
      1. Mať dostatok informácií o
         1. rizikách kybernetického priestoru pre dieťa,
         2. spôsobe manažmentu týchto rizík, najmä
            1. použitie vhodných preventívnych opatrení
            2. reakcia na incident
            3. eliminácia dopadov incidentu
            4. obnova IS
            5. plánovanie kontinuity činností
      2. Mať k dispozícii nástroje na manažment rizík a vedieť ich aplikovať.
      3. Vedieť, ako postupovať v prípade realizácie najčastejšie realizovaných hrozieb.
      4. Mať k dispozícii inštitúciu, s ktorou môže konzultovať problematiku rizík kybernetického priestoru pre dieťa, vrátane podpory pri realizácii vážnej hrozby.
   2. Mať prehľad o aktivitách dieťaťa v kybernetickom priestore.
      1. Navštevované stránky
      2. Hrané hry
      3. Komunikácia na sociálnych sieťach
      4. Sťahovanie digitálneho obsahu.
      5. Čas strávený jednotlivými aktivitami.
   3. Mať k dispozícii nástroje na reguláciu činností dieťaťa v kybernetickom priestore.
      1. Časová regulácia.
      2. Obmedzenie prístupu na nevhodné webové sídla.
3. Od dieťaťa očakáva
   1. Komunikačnú dôveru (dieťa mu dôveruje a je pre neho prioritný komunikačný partner v predmetnej oblasti)
   2. Komunikáciu o  potrebách a očakávaniach dieťaťa z hľadiska digitálnych technológií.
   3. Správanie v KP súlade s hodnotami, ktoré presadzuje a od dieťaťa očakáva.
   4. Byť včas informovaný o jeho problémoch v kybernetickom priestore (napr. kyberšikana, stalking, sexting).
4. Od spoločnosti / štátu očakáva:
   1. Mať účinnú oporu v legislatíve pri ochrane svojho dieťaťa pre hrozbami kybernetického priestoru.
   2. Mať oporu v OČTK v prípade, že jeho dieťa je obeťou trestného činu v súvislosti s kybernetickým priestorom.
   3. Byť včas informovaný o potenciálnych nelegálnych aktivitách dieťaťa s možným trestno-právnym postihom.

## Dieťa / žiak

V potrebách a očakávaniach berieme ako referenčný bod dieťa, ktorý má záujem o svoje zmysluplné bytie, vzdelávanie a rozvoj a dobre vychádza so svojimi rodičmi.

1. Od školy očakáva *(z hľadiska kybernetického priestoru a digitálnych technológií)*
   1. Všeobecne:
      1. Bezpečné prostredie, vrátane bezpečnosti v kybernetickom priestore.
      2. Aby digitálne technológie používané vo vzdelávacom procese boli pre neho prínosom.
      3. Aby získalo adekvátne vedomosti, schopnosti a zručnosti práce s digitálnymi technológiami a aplikáciami vrátane kybernetickej bezpečnosti.
      4. Aby sa v škole cítilo v pohode.
   2. Od učiteľov a vedenia školy
      1. Odbornosť v rámci vyučovania vrátane oblasti digitálnych technológií.
      2. Zmysluplné činnosti na hodinách.
      3. Pozitívny, ľudský prístup v rámci vyučovania aj mimo neho.
      4. Spravodlivosť a nediskrimináciu.
      5. Zohľadnenie jeho prípadných znevýhodnení.
      6. Aby sa so svojimi problémami mohol na nich obrátiť a jeho problémy boli riešené a vyriešené.
      7. Získanie externej podpory v prípade potreby (psychické problémy, problémy v rodine), nad rámec kompetencií školy.
      8. Byť informovaný o dianí na škole.
   3. Od spolužiakov / triedy
      1. Aby ho akceptovali.
      2. Aby nebol sociálne vylúčený z kolektívu, vrátane digitálneho vylúčenia.
      3. Pohodu v triede.
      4. Ochotu pomôcť mu v prípade potreby.
   4. Od externých subjektov
      1. Mať k dispozícii kontaktné miesto, kde by sa mohol obrátiť pri riešení svojich vážnych problémov nad rámec domácnosti a školy.
   5. Od štátu
      1. Mať účinnú oporu v legislatíve pri svojej ochrane pre hrozbami kybernetického priestoru.
      2. Mať oporu v OČTK v prípade, že je obeťou trestného činu.
      3. Byť včas informovaný o svojich potenciálnych nelegálnych aktivitách s možným trestno-právnym postihom.
2. V domácnosti potrebuje
   1. Mať dostatok informácií o
      1. rizikách kybernetického priestoru pri svojich aktivitách,
      2. spôsobe manažmentu týchto rizík na svojej úrovni.
   2. Vedieť, ako postupovať v prípade realizácie najčastejšie realizovaných hrozieb.
3. Od rodičov očakáva
   1. Vytvorenie bezpečného domáceho IKT prostredia.
   2. Mať rodičov, s ktorými môže s dôverou konzultovať svoje problémy v kybernetickom priestore.
   3. Čo najmenej obmedzení vo vzťahu k svojim aktivitám v KP.
   4. Primeraný mobil, aby nebol sociálne vylúčený.
   5. Primerané financie na svoje digitálne aktivity.

## Pedagóg

1. Od vedenia školy očakáva
   1. Podporu vo vzdelávaní v oblasti IKT.
   2. Podporu pri riešení problémov svojich žiakov.
   3. Byť informovaný o dianí na škole, vrátane oblasti IKT
   4. Podieľať sa na ďalšom rozvoji a formovaní školy a svojich predmetov
2. Od rezortu / zriaďovateľa očakáva
   1. Bezpečné IKT prostredie
      1. na škole.
      2. v pridelenom notebooku.
   2. Mať dostatok informácií o
      1. rizikách kybernetického priestoru v rámci školského prostredia,
      2. spôsobe manažmentu týchto rizík na svojej úrovni.
   3. Byť vyškolený na bezpečnú prácu s digitálnymi technológami.
   4. Metodické materiály k novým digitálnym technológiám, napr.
      1. Správe využitie aj riziká AI.
   5. Vedieť, ako postupovať v prípade realizácie najčastejšie realizovaných hrozieb v školskom prostredí.
3. Od žiakov očakáva
   1. Zmysluplnú prácu s digitálnymi technológiami v rámci hodiny.
   2. Aby nerealizovali neautorizované / zlomyseľné / nelegálne / neetické činnosti s digitálnymi technológiami / v KP.
   3. Aby nenarúšali hodiny mobilmi.
   4. Aktívne získavanie zručností a znalostí v oblasti digitálnych technológií.
4. Ďalšie potreby a očakávania
   1. Mať k dispozícii inštitúciu, s ktorou môže konzultovať problematiku rizík kybernetického priestoru vrátane podpory pri realizácii vážnej hrozby (napr. kyberšikany).
   2. Mať oporu v legislatíve pri ochrane seba a svojich žiakov pre hrozbami kybernetického priestoru.
   3. Mať oporu v OČTK v prípade, že jeho dieťa sa on alebo jeho žiak stane obeťou trestného činu v súvislosti s kybernetickým priestorom.

## Vedenie školy

1. Mať dobrú atmosféru na škole, nenarúšanú negatívami a hrozbami KP.
2. Mať minimalizované riziko vzniku kybernetického bezpečnostného incidentu.
3. Vedieť, ako postupovať v prípade kybernetického bezpečnostného incidentu.
4. Vedieť, ako postupovať v prípad realizácie non-IKT hrozby.
5. Mať k dispozícii kvalifikovaného administrátora.
6. Mať vyškolených učiteľov na správne využívanie IKT.
7. Mať k dispozícii inštitúciu, s ktorou môže konzultovať problematiku rizík kybernetického priestoru pre, vrátane podpory pri realizácii vážnej hrozby (napr. kyberšikany s trestnoprávnymi následkami).

## Štát ako celok

1. Minimalizovať rozsah negatívneho pôsobenia kybernetického priestoru na deti aj ich rodičov.
   1. Minimalizovať počet nositeľov nelátkových závislostí a nadmernej závislosti na digitálnych technológiách.
2. Mať generáciu vstupujúcu na pracovný trh, ktorá
   1. má plne rozvinuté pracovné schopnosti a návyky, zodpovedajúce potrebám pracovného trhu (vrátane IKT zručností)
   2. je konkurencieschopná v rámci vyspelých krajín (napr. vlastné podnikateľské aktivity, startupy),
   3. je v dobrom zdravotnom stave,
   4. ostáva pôsobiť na Slovensku,
   5. cíti sa na Slovensku dobre.
3. Mať sociálnu kohéziu a solidaritu v rámci spoločnosti (narúšanú aj pôsobením obsahu kybernetického priestoru).

# Možné opatrenia a odporúčania

Možné opatrenia resp. odporúčania bývajú špecifikované na troch úrovniach:

* Všetky možné opatrenia (tzv. long list / zásobník opatrení)
* Opatrenia, ktoré je možné realizovať v aktuálnych podmienkach (short list)
* Opatrenia, ktoré sa plánujú aktuálne realizovať (priority list) - nie sú predmetom tohto dokumentu.

V tejto kapitole uvádzame rozpracovaný zásobník možných opatrení a odporúčaní, z ktorého si daný subjekt vyberá ním realizovateľné opatrenia (štát, ministerstvo, zriaďovateľ, škola, učiteľ, rodič, dieťa).

Detailnejšie špecifikujeme opatrenia nad rámec opatrení uvedených v strategických a koncepčných materiáloch (podrobnejšie viď kap. 7.2 a 7.3):

* Stratégia Slovenskej republiky pre mládež na roky 2021 – 2028 [[93]](#footnote-93)
* Národná koncepcia ochrany detí v digitálnom priestore [[94]](#footnote-94)
* Akčný plán k Národnej koncepcii ochrany detí v digitálnom priestore na roky 2024 – 2025 [[95]](#footnote-95)

**Prehľad ďalších možných opatrení a odporúčaní nad rámec horeuvedených dokumentov (zásobník opatrení)**

## Rodičia

Základom prevencie rizikového používania digitálnych technológií je mať pripravenú a nastavenú stratégiu výchovy v ich používaní od najmenšieho veku dieťaťa a túto kontinuálne upravovať s rastúcim vekom.

Ako najväčší problém sa javí to, že rodiny túto stratégiu a z nej vyplývajúce opatrenia začínajú riešiť neskoro, prípadne v skoršom období používajú vyslovene rizikové opatrenia (napr. tablet ako "digitálna opatrovateľka" v predškolskom veku) a potom sa čudujú, že v staršom veku (väčšinou reštriktívne) opatrenia nefungujú (pretože v tomto veku by už mala dominovať aktívna mediácia a reštriktívna ustupovať, aby nenarážala na rodiacu sa autonómiu dieťaťa).

Je dôležité začať s otvorenou komunikáciou a rozhovormi o digitálnych technológiách čo najskôr, samozrejme s ohľadom na vývinovú úroveň dieťaťa. Čím skôr sa dieťaťu začnú vysvetľovať zásady zodpovedného používania médií, tým skôr si vytvorí zdravé návyky a zodpovedný prístup k technológiám. So stúpajúcim vekom by mala klesať miera reštrikcií a namiesto toho by sa mala zamerať pozornosť na aktívnu mediáciu detí v digitálnom prostredí.

Následné odporúčania pre rodičov sú od Výskumného ústavu detskej psychológie a patopsychológie. [[96]](#footnote-96)

**Konkrétne všeobecné odporúčania nezávislé od veku dieťaťa**

1. Vytvorenie stratégie výchovy vo vzťahu k obrazovkovým médiám, ktorú budú rodičia aplikovať od najmenšieho veku dieťaťa. Táto stratégia má obsahovať prvky aktívnej mediácie (diskutovanie, vysvetľovanie, pomoc dieťaťu s obrazovkovými médiami, ísť dieťaťu príkladom), ktoré budú so zvyšujúcim sa vekom dieťaťa postupne pribúdať; ako aj prvky reštriktívnej mediácie (filtrovanie, monitorovanie, technická rešktrikcia, nastavovanie regulatívnych pravidiel), ktoré budú so zvyšujúcim sa vekom dieťaťa postupne ustupovať.
2. Dieťa potrebuje vedieť, že je tu rodič pre neho - aj vtedy, keď urobí chybu alebo zažije niečo nepríjemné v online prostredí. Vzťah založený na dôvere a pochopení mu pomôže cítiť sa v bezpečí a obrátiť sa na rodiča bez obáv.
3. Nepoužívať obrazovkové médiá pre dieťa za odmenu, ako trest alebo na jeho upokojenie.
4. Pri používaní obrazoviek by mal rodič byť príkladom dieťaťu. O pravidlách nerozmýšľať len vo vzťahu k dieťaťu, ale aj vo vzťahu k sebe.
5. Odporúča sa vytvoriť „rodinný mediálny plán“ – pravidlá používania obrazoviek v rodine, ktoré budú rešpektované a dodržiavané všetkými členmi. V závislosti od veku a vyspelosti dieťaťa prizvať dieťa k tvorbe pravidiel (tu je vhodné uviesť príklad, ako môže taký plán vyzerať).
6. Zaviesť v rodine „čas bez obrazoviek alebo off-line režim“, zóny bez digitálnych technológií (časové /nočné hodiny, ranné hodiny, spoločné stolovanie, pracovný čas/, ale aj priestorové, napr. WC, spoločné stolovanie, posteľ pred spaním a pod. - individuálne podľa hodnôt, ktoré jednotliví rodičia chcú dieťaťu odovzdať).
7. Nezapínať žiadne obrazovky ráno pred odchodom do školy.
8. Pri učení alebo práci mať obrazovkové médiá v inej miestnosti.
9. Odložiť obrazovky minimálne 1 hodinu pred spánkom.
10. Zabezpečiť dieťaťu zdravý spánok - na to sú potrebné spánkové návyky bez obrazoviek a izba/spálňa bez obrazoviek. Je vhodné určiť miesto, kde všetci odložia mobilné telefóny na noc. Toto pravidlo je prevenciou pred spávaním s mobilom (je dôležité vysvetliť dieťaťu, že to nie je iba o modrom svetle, ale aj o kognitívnej záťaži mozgu, ktorá bráni zaspávaniu a ak sa deje v momente, keď má dieťa spať, zhoršuje nielen dĺžku, ale aj kvalitu spánku).
11. Nepoužívať obrazovkové médiá pri jedle. Mať vypnutý televízor, nehrajte počítačové hry, nemať pri stolovaní mobilný telefón ani tablet.
12. Dodržiavať odporúčané vekové obmedzenia pre počítačové hry, filmy a sociálne siete. Zvažovať však vyspelosť dieťaťa. Niektoré deti môžu byť v porovnaní s rovesníkmi, ale aj súrodencami (ne)skôr zrelé na samostatné používanie telefónu alebo iných médií. Je dôležité vnímať individuálne charakteristiky každého dieťaťa.
13. Preferencia prezenčnej výučby - pandémia COVID-19 ukázala, že počas dištančného vzdelávania sa deti naučili menej, trávili pred obrazovkou viac času, narúšalo to ich duševnú pohodu a prežívali viac osamelosť. Učenie sa pomocou obrazoviek je vhodné povoliť iba vtedy, ak rodičia vyhodnotia, že dané médium má pridanú hodnotu (e.g. interaktivita videohier, realistickosť alebo názornosť  zobrazenia vo filmoch alebo iných videách) oproti tradičným spôsobom učenia sa, pričom v mladšom veku sa pridaná hodnota týchto médií zvyšuje prítomnou komunikáciou s rodičom.
14. Nezabúdať, že rodičia a starší súrodenci sú pre mladšie dieťa vzorom.
15. Vypínať obrazovkové médiá, ktoré sa práve nepoužívajú, smartfóny odkladať v domácnosti na jedno miesto.
16. Poznať nebezpečenstvo – rodičia by sa mali informovať a vzdelávať o rizikách spojených s obrazovkovými médiami, poučiť a viesť svoje dieťa. Je vhodné nechať dieťa, aby rodičom ukázalo a vysvetlilo, čo ho zaujíma na internete. Pri podozrení na nadmerné alebo problematické používanie obrazovkových médií je vhodné čo najskôr vyhľadať odbornú pomoc.
17. Odporúčania sa môžu líšiť pri dieťati s narušeným vývinom alebo zdravotným znevýhodnením. Lekár pediater či psychológ môže odporúčať aj iné pravidlá, prípadne obmedzenia so zohľadnením zdravotného stavu dieťaťa.

Vek do 3 rokov

Odporúčanie pediatrov je zotrvať bez akéhokoľvek (aktívneho aj pasívneho) používania obrazoviek. Výnimkou sú  krátke video rozhovory s najbližšími príbuznými.

1. Dieťa by malo čo najmenej vidieť iných tráviť čas pred obrazovkou. Rodičia by mali obmedziť na minimum používanie obrazovkových médií dospelými v prítomnosti detí a vyhnúť sa tzv. technoferencii (pojem by bolo vhodné definovať na začiatku dokumentu).
2. Nenechávať zapnuté obrazovky (televízor, tablet, počítač a pod.), ak ich práve rodičia nepozerajú, obraz a zvuk v pozadí dieťa vyrušuje a rozptyľuje.
3. Vyvarovanie sa používať obrazovky ako “digitálnu opatrovateľku” (t.j. deti odložiť pred obrazovky, ak dieťa potrebujeme na čas zabaviť, kým rodičia vykonávajú iné aktivity).
4. V prípade porušovania odporúčaní:
   1. Vyberať videá, ktoré sú pre dieťa prínosom.

Vek 3 - 6 rokov

Odporúčanie je pred obrazovkovými médiami tráviť **maximálne 30 minút** v jednom dni a nie každý deň.

1. Nenechávať dieťa pred obrazovkou samé, ale byť jeho sprievodcom, komentovať a rozprávať sa o tom, čo sa na obrazovke deje (toto veda pomenúva pojmom „aktívna mediácia“).
2. Rodič má vyberať pokojné, veku primerané obsahy bez násilia a nenechávať dieťaťu ovládač od média.
3. Odporúčanie je vyhnúť sa videohrám a hrám na herných konzolách.
4. Dieťa pred obrazovkou stráca pojem o čase. Rodičia by si mali nastaviť časovač, alarm, alebo limit, kedy je vhodné médium vypnúť.
5. Okrem času pred obrazovkou a obsahom by mali rodičia riešiť aj kontext, v ktorom sa interakcia dieťaťa s obrazovkami odohráva - situačných kontextov je viacero (spoločné stolovanie, ráno po zobudení, sociálne aktivity a pod.). Jedným z najviac negatívnych je používanie médií v neskorých večerných/nočných hodinách.

6 - 9 rokov

Mimo školských povinností by dieťa nemalo tráviť pred obrazovkou viac ako **30-45 minút** denne a nie každý deň, aby sa vyhlo návyku. Avšak v tomto čase by bolo vhodné dieťa začať pripravovať na postupné samostatné používanie obrazovkových médií.

1. Obrazovkové médiá by mali byť v spoločných priestoroch, nikdy nie v detskej izbe
2. Rodič by mal mať prehľad o sledovanom obsahu, dodržiavať vekovú vhodnosť programu, sledovať a korigovať dodržiavanie dohodnutého času, ktoré dieťa trávi pred obrazovkovým médiom.
3. Dieťa do 9 rokov by nemalo mať prístup na internet. Nemalo by mať vlastné smart obrazovky, tablety.
4. Dieťa do 9 rokov by nemalo mať vlastnú hernú konzolu. Dieťa s vlastnou konzolou je ťažšie regulovať, trávi hraním v priemere dvakrát viac času ako dieťa bez vlastnej konzoly.
5. Od nástupu do školy by rodičia mali pravidelne komunikovať o pravidlách nielen s dieťaťom, ale aj s inými rodičmi (najmä rodičmi kamarátov dieťaťa) ako aj školou, ktorú dieťa navštevuje. Je dôležité poznať, ako sú nastavené pravidlá v širšej komunite, aby sa vyvarovali zbytočným konfliktom alebo nedorozumeniam, ktoré vznikajú v dôsledku nedostatočnej komunikácie tejto témy medzi dospelými, ktorí prichádzajú s deťmi do pravidelného kontaktu.

9-12 rokov

Mimo školských povinností by dieťa nemalo tráviť pred obrazovkou viac ako **45 - 60 minút** a nie každý deň, aby sa vyhlo návyku.

1. Je vhodné kontrolovať dodržiavanie obsahu vhodného pre daný vek a dodržiavanie dohodnutého času.
2. Počítače, tablety a digitálne hračky by nemali byť umiestnené v detskej izbe.
3. Neodporúča sa dať dieťaťu hraciu konzolu skôr ako od 9 rokov. Konzolu je vhodné odkladať do uzamykateľnej skrinky, mimo zraku dieťaťa, aby sa rodičia vyhli častejšiemu odmietaniu a prípadným konfliktom.
4. Dieťa by nemalo dostať vlastný smartfón skôr ako v 9. roku života, najlepšie až po 12. roku života.
5. Skôr ako dieťaťu dajú rodičia mobil, mali by si dohodnúť spolu pravidlá jeho používania, pristupovať k smartfónu tak, že jeho kúpou dávajú dieťaťu de facto vstupenku do sveta dospelých (a tým pádom mu pripomenúť a znova vysvetliť, s akými rizikami sa v digitálnom svete môže stretnúť).
6. Prípravu na prvé vlastné digitálne zariadenie je vhodné zobrať podobne ako funguje príprava na vodičské oprávnenie - tj. možnosť používať zariadenie dostane dieťa až vtedy, keď má dieťa adekvátne vedomosti a zručnosti. Rodičia by sa mali uisťovať, že dieťa dodržiava dohodnuté pravidlá.
7. Odporúča sa obmedzenie v prístupe na internet resp. v tomto veku by malo mať dieťa prístup na internet len pod dohľadom rodiča.

12 - 18 rokov

V tomto veku je dieťa do veľkej miery samostatné a malo by byť schopné istej miery regulácie a to bez značného zásahu rodiča.

1. Prehnané vynucovanie dodržiavania predpísaného času pred obrazovkou môže v tomto období narážať na rodiacu sa autonómiu dieťaťa ako aj diskrepanciu v tom, čo rodičia vyžadujú od dieťaťa a aké správanie vidí dieťa u nich (napr. rodič vynucuje 1-2 hodiny, a dieťa ho vidí s telefónom v ruke oveľa viac, alebo sedieť 3 hodiny pred televíziou a pod.).
2. Odporúčanie je zamerať sa na to, aby išli rodičia príkladom dieťaťu, aby pravidlá v tomto veku boli nastavené spoločne a platili aj pre dospelých (Ak rodičia nastavia dieťaťu prísnejšie pravidlá ako sebe, môžu to deti (oprávnene) vnímať ako nespravodlivosť - ide o voľnočasové aktivity, nie pracovné činnosti).
3. Rodičia by mali jasne rozlišovať, čo sa vzťahuje na voľnočasové používanie obrazoviek a čo na pracovné účely (tak u detí, ako aj u dospelých).
4. Skôr ako rodičia pustia dieťa samé na internet, je vhodné sa s ním porozprávať o súkromí, sociálnych sieťach, násilí, hazardných hrách a pornografii a poskytnúť dieťaťu sexuálnu výchovu skôr ako ju získa z internetu.
5. Odporúča sa pravidelne viesť dospievajúceho k tomu, aby sa sám zamyslel nad časom, obsahom a vlastným používaním obrazoviek v kontexte s jeho životnými cieľmi. Je vhodné deti povzbudzovať, aby sám pozoroval, čo robí množstvo času pred obrazovkovými médiami a sledovaný obsah s jeho koncentráciou, sociálnym správaním, kondíciou, jeho osobnosťou a školskými výsledkami.
6. Vo vyššom veku (16 - 18 rokov) je nutné deti učiť samoregulácii používania médií.
7. V tomto veku je vhodné zmeniť rétoriku od zakazovania smerom k odporúčaciemu charakteru pravidiel zo strany rodiča /reflektovaniu správania dieťaťa a vedenie k tomu, aby zjednalo nápravu samo.

**Problém s prekračovaním odporúčanej doby strávenej s digitálnymi technológiami**

Na základe prieskumov citovaných v predchádzajúcich kapitolách je zrejmé, že výrazná časť detí tieto odporúčané časy prekračuje (s vedomím rodičov).

Nie je ale jedno, či namiesto odporúčanej jednej hodiny strávi dieťa priemerne s digitálnymi technológiami 2, 4 alebo 6 hodín denne. Preto je vhodné zaviesť škálu, ktorá hodnotí mieru rizika pri prekračovaní odporúčaných dôb. Jej návrh je uvedený v prílohe č. 7.5

Ďalšie možné opatrenia súvisiace s domácimi IKT

1. Byť aspoň na základnej úrovni vzdelaný v oblasti problematiky kybernetickej bezpečnosti dieťaťa.
2. Mať inštalovaný anti-malware SW s pravidelnou aktualizáciou.
3. Pravidelne aktualizovať OS a aplikácie (resp. povoliť im aktualizáciu).
4. Neinštalovať SW z neznámych zdrojov.
5. Neklikať na prílohy neznámych, podozrivých mailov.
6. Zabezpečiť zálohovanie údajov dieťaťa, aj geograficky vzdialené (napr. na UBS a cloude).
7. Pri mladších deťoch mať prístup k ich účtom na sociálnych sieťach.
8. Využívať rodičovský zámok.
9. Pravidelné monitorovanie online aktivít detí.
10. Riadený prístup k finančným zdrojom použiteľným dieťaťom na internetové platby.
11. V prípade potreby včas vyhľadať psychológa alebo psychiatra pre dieťa.

## Dieťa / žiak

1. Mať dobrý a otvorený vzťah, ako aj bezpečnú vzťahovú väzbu s rodičmi.
2. Otvorene komunikovať s rodičmi o prípadných problémoch.
3. Vedieť napr., že
   1. v kybernetickom priestore sa môže stretnúť aj so zlými ľuďmi,
   2. ak niečo vyzerá príliš dobré a lákavé, treba byť opatrným,
   3. prílišná dôverčivosť nie je na mieste,
   4. podceňovať riziko sa nevypláca.
4. Mať povedomie o rizikách kybernetického priestoru, ktoré sú pre neho relevantné.
   1. Absolvovať vhodné semináre, workshopy, kurzy
5. Byť si vedomý závažnosti niektorých rizík.
   1. Vo veku trestnoprávnej zodpovednosti poznať príslušné trestné činy vrátane trestných sadzieb.
6. Dodržiavať základné, technicky nenáročné zásady kybernetickej bezpečnosti.

## Škola / zriaďovateľ školy

1. Implementácia bezpečnostných opatrení pre školské IS na lokálnej aj centrálnej úrovni, najmä
   1. Jednoduchá bezpečnostná politika prístupná učiteľom
   2. Základná bezpečnostná dokumentácia
   3. Riadenie prístupu
   4. Základná fyzická bezpečnosť počítačových učební
   5. Antimalware softvér
   6. Ochranu siete na úrovni providera
   7. Zabezpečené podpora rezortného SOC / SIEM /CSIRTu.
2. Vzdelávanie a školenia, najmä
   1. Organizovať interaktívne workshopy o kybernetickej bezpečnosti pre žiakov aj ich rodičov, pokrývajúce aktuálne hrozby a spôsoby ochrany.
   2. Implementácia preventívnych opatrení, ktoré pomôžu deťom zvládať výzvy digitálneho sveta, napr. formou posilňovanie kľúčových schopností detí, ako sú sebaregulácia, kritické myslenie, sebaúcta a zdravé návyky pri používaní digitálnych technológií.
      1. Príkladom, ktorý reflektuje tieto potreby, je preventívny projekt Smajlík – Bezpečne a zodpovedne online. Program je určený pre žiakov 5. ročníka základných škôl a zameriava sa na rozvoj zmierlivého správania online, tolerancie, kritického myslenia, bezpečného používania internetu, sebaúcty a schopnosti regulovať nadmerné používanie digitálnych technológií.
3. Vytváranie bezpečného a podporného prostredia, najmä
   1. Budovanie bezpečnej atmosféry v školách, kde sa každý žiak cíti rešpektovaný, vypočutý a akceptovaný bez ohľadu na svoje zázemie, výzor či názor.
   2. Prevencia šikany a kyberšikany prostredníctvom pravidelného monitorovania vzťahov, včasnej intervencie a spolupráce s odborníkmi.
   3. Podpora žiakov v identifikácii a vyjadrovaní emócií, tréningy sociálnych zručností a psychoedukácia o zdravých vzťahoch, hraniciach a komunikácii.
4. Dostupnosť odborníkov na duševné zdravie, najmä
   1. Pravidelná prítomnosť školských psychológov, sociálnych pedagógov či iných odborníkov, ktorí poskytujú individuálne poradenstvo, krízovú intervenciu a skupinové preventívne aktivity.
   2. Vytvorenie podporného tímu z týchto odborníkov.
   3. Zavedenie systému včasného záchytu duševných ťažkostí (screening, triednické hodiny so psychosociálnym zameraním).
   4. Dôverný priestor na zverenie sa – fyzicky aj digitálne, napr. anonymné online schránky dôvery, kontakt na linky pomoci.
5. Podpora pedagógov, najmä
   1. Organizovať pravidelné školenia a praktické workshopy pre pedagógov zamerané na aktuálne kybernetické hrozby, rozpoznávanie rizikového správania žiakov a stratégie prevencie a intervencie.
   2. Vypracovanie postupov učiteľov a vedenie pre reakciu na vážne riziko (napr. útok zbraňou, nebezpečné vyhrážanie, pokus o samovraždu, šikana a kyberšikana)
   3. Školiť učiteľov v digitálnej pedagogike, využívať adaptívne technológie zamerané na učenie.
6. Vyváženosť digitálneho a reálneho sveta a digitálna pohoda (wellbeing) [[97]](#footnote-97), najmä
   1. Zodpovedné a uvedomelé používanie technológií ako súčasť výchovno-vzdelávacieho procesu – nie demonizácia, ale vedenie k zdravej digitálnej gramotnosti.
   2. Zaviesť školské politiky pre digitálny wellbeing, školiť pedagógov, podporovať zdravú digitálnu kultúru.
      1. Poskytnúť tréningy na zvládanie stresu, mindfulness programy, prístup k digitálnym zdrojom pre duševné zdravie.
      2. Znížiť kognitívne preťaženie, vytvoriť podporujúce prostredie, zaviesť workshopy o digitálnom strese.
      3. Integrovať digitálnu gramotnosť do kurikula, cielene podporiť znevýhodnených žiakov
   3. Vyvážený rozvrh školských a mimoškolských aktivít, ktorý zahŕňa fyzický pohyb, kreatívne činnosti a offline spoluprácu.
   4. Podpora digitálneho wellbeing-u – práca s digitálnymi návykmi, vedomé prestávky od obrazoviek, psychohygiena.
   5. Gamifikácia zdravého životného štýlu – prepojenie pohybu s aplikáciami sledujúcimi progres (napr. krokomery, výzvy v kolektíve), nie ako súťaž, ale ako motivácia.
7. Participácia žiakov, najmä
   1. Zapájanie mladých do vytvárania pravidiel digitálneho správania a bezpečnosti v škole – posilňuje ich zodpovednosť aj identifikáciu s pravidlami.
   2. Triedne kruhy, diskusie a žiacke parlamenty ako nástroje na ventiláciu potrieb, obáv aj nápadov mladých ľudí.
8. Podpora zdravého životného štýlu
   1. Gamifikácia zdravého životného štýlu – prepojenie pohybu s aplikáciami sledujúcimi progres (napr. krokomery, výzvy v kolektíve), nie ako súťaž, ale ako motivácia.
   2. Masívnejšie zapojenie žiakov do krúžkov fyzických aktivít

## MŠVVaM

1. Rozpracovanie cieľov a plnenie opatrení uvedených v Stratégii Slovenskej republiky pre mládež na roky 2021 – 2028 (viď kap. 7.2) so zohľadnením tohto Katalógu rizík pre mládež v kybernetickom priestore.
2. Aktualizácia cieľov a opatrení uvedených v Národná koncepcia ochrany detí v digitálnom priestore *(tá je pre časový horizont do roku 2025).*
   1. Vytvoriť Akčný plán k aktualizovanej Koncepcii pre roky 2028 – 2035.
   2. V súčinnosti s MIRRI plánovanie alokácie zdrojov EÚ na aktivity Akčného plánu.
3. Vytvorenie Katalógu rizík pre mládež v kybernetickom priestore
   1. Pripomienkovanie širokou verejnosťou.
   2. Priebežná aktualizácia.
   3. Vytvorenie zjednodušených verzií Katalógu vhodných pre žiakov, ich rodičov, učiteľov a vedenie škôl.
   4. Vytvorenie povedomia o Katalógu
   5. Distribúcia (odkazov) pre všetkých žiakov, ich rodičov a pedagógov (cca. 3 mil. osôb)
   6. Publikácia Katalógu a ďalších didaktických materiálov v štruktúrovanej podobe na webovom sídle ministerstva alebo špecializovanom webovom sídle
4. Vytvorenie vzorových materiálov pre školy
   1. Riadiaca dokumentácia KB / IT VS / GDPR
   2. Bezpečnostná dokumentácia
      1. Analýza dopadov (BIA)
      2. Analýza rizík
      3. Plány kontinuity činností
      4. Plán zvyšovania bezpečnostného povedomia
5. Kurikulum
   1. V rámci etickej výchovy a iných relevantných predmetov zahrnúť aj témy etiky a etikety správania sa na internete (netiketa).
   2. Zaradiť do školského vzdelávacieho programu systematické vzdelávanie v oblasti kybernetickej bezpečnosti, digitálnej gramotnosti a mediálnej výchovy, prispôsobené veku žiakov.
6. Vzdelávanie a školenia
   1. Zabezpečiť workshopy o kybernetickej bezpečnosti pre žiakov, pokrývajúce aktuálne hrozby a spôsoby ochrany.
   2. Zabezpečiť pravidelné školenia pre pedagógov zamerané na aktuálne kybernetické hrozby, rozpoznávanie rizikového správania žiakov a stratégie prevencie a intervencie.
7. Didaktické materiály
   1. Vytvorenie interaktívnych učebných pomôcok pre školy (napr. pracovné listy, videá, simulácie kybernetických hrozieb).
   2. Poskytnutie metodických príručiek pre pedagógov na výučbu kybernetickej bezpečnosti.
8. Podpora výskumu
   1. Podpora a financovanie výskumných projektov zameraných na analýzu správania detí a mládeže v kybernetickom priestore, identifikáciu nových rizík a hodnotenie efektivity preventívnych programov.
   2. Spolupráca s univerzitami a odbornými inštitúciami na analýze aktuálnych trendov a hrozieb.
9. Podpora manažmentu kybernetických bezpečnostných incidentov
   1. Vytvorenie rezortného SOC a CSIRT, resp. CSIRTov na univerzitách, ktoré podporujú aj SŠ a ZŠ.

## Ďalšie štátne orgány

1. Komunálna úroveň (obec, mestská štvrť, mesto, VÚC)
   1. Propagácia zdravého životného štýlu
   2. Podpora krúžkov fyzických aktivít pre deti na komunálnej úrovni
   3. Budovanie ihrísk pre podporu pohybových aktivít
2. Úrady verejného zdravotníctva
   1. Reprezentatívny prieskum stavu zdravia mládeže
      1. Fyzické zdravie
      2. Duševné zdravie
   2. Propagácia zdravého životného štýlu
   3. Informácie o rizikách nezdravého životného štýlu
   4. Zapojenie poradní zdravia do podpory zdravého životného štýlu detí prostredníctvom ich rodičov
3. MIRRI
   1. V súčinnosti s NBÚ legislatívne riešiť špecifické postavenie škôl ako správcov IS verejnej správy a ich kybernetickej bezpečnosti.
   2. Na webovej stránke zverejňovať metodiky vhodné aj pre úroveň vzdelávacích zariadení.
   3. V súčinnosti s MŠVVaM podpora rozvoja rezortného SOC a . CSIRTov na univerzitách, ktoré podporujú aj SŠ a ZŠ.
   4. CSIRT
      1. Podpora pri riešení kybernetických bezpečnostných incidentov v spolupráci s so vzdelávacími zariadeniami
      2. Realizovať vzdelávacie aktivity na školách
      3. Publikovať bezpečnostne relevantné odborné a metodické materiály vhodné aj pre školy
      4. Podpora rozvoja akademických CSIRTov.
4. Štát ako celok
   1. Legislatívne
      1. Zákaz / obmedzenie mobilov a smart hodiniek
         1. Na hodine
         2. Na vyučovaní
      2. Zákaz / obmedzenie prístupu detí na sociálne siete *(viď Austrália)*
      3. Úprava Trestného zákona so zohľadnením nových trestných činov *(napr. deepfakes)*
   2. Financovanie
      1. Financovanie vzdelávacích projektov zameraných na kybernetickú bezpečnosť.
      2. Poskytovanie grantov na vývoj bezpečnostných aplikácií pre deti.

## Ďalšie subjekty

1. Firmy, záujmové združenia a tretí sektor
   1. Podpora vzdelávania v oblasti kybernetickej bezpečnosti.
      1. Vzdelávacie aktivity priamo na školách.
      2. Tvorba vhodných metodických materiálov pre rôzne vekové kategórie detí
      3. Poskytovanie anonymnej, bezplatnej, dostupnej a nízkoprahovej odbornej pomoci a podpory
2. Médiá
   1. Publikovanie informácií o hrozbách, zraniteľnostiach, opatreniach v predmetnej oblasti.
   2. Podpora propagácie zdravého životného štýlu mládeže.

# Prílohy

## Legislatívny rámec pre riadenie identifikovaných rizík

V tejto kapitole je uvedený legislatívny rámec relevantný pre riadenie identifikovaných rizík pre mládež a návrh možných opatrení (kap.6) mimo oblasti kybernetickej bezpečnosti a IT VS.

Legislatíva pre oblasť kybernetickej bezpečnosti je uvedená na webovom sídle – Centrálny portál kybernetickej bezpečnosti [[98]](#footnote-98)

Legislatíva pre oblasť IT VS je uvedená taktiež na tomto webovom sídle [[99]](#footnote-99).

Legislatíva súvisiaca s ochranou detí v digitálnom priestore je uvedená v dokumente „Národná koncepcia ochrany detí v digitálnom priestore [[100]](#footnote-100), kap. Národná legislatíva a dokumenty.

### Kompetencie v oblasti starostlivosti o mládež

#### Zákon č. 575/2001 Z. z.

o organizácii činnosti vlády a organizácii ústrednej štátnej správy

**§ 17 Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky**

Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky je ústredným orgánom štátnej správy pre

**a) materské školy, základné školy, stredné školy, základné umelecké školy, jazykové školy a vysoké školy,**

**b) školské zariadenia,**

c) celoživotné vzdelávanie,

d) výskum a vývoj,

e) **štátnu starostlivosť o mládež a rozvoj pohybových a športových aktivít v školách a školských zariadeniach**.

**§ 20 Ministerstvo cestovného ruchu a športu Slovenskej republiky**

Ministerstvo cestovného ruchu a športu Slovenskej republiky je ústredným orgánom štátnej správy pre

a) cestovný ruch,

b) rozvoj, propagáciu a prezentáciu produktov cestovného ruchu na Slovensku a v zahraničí,

**c) šport,**

d) štátnu starostlivosť o športovú reprezentáciu Slovenskej republiky.

#### Zákon č. 282/2008 Z. z.

o podpore práce s mládežou a o zmene a doplnení zákona č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

**§ 4 Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky**

Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky (ďalej len „ministerstvo“) ako ústredný orgán štátnej správy pre štátnu starostlivosť o mládež najmä

**a) vypracúva strategické dokumenty a koncepčné dokumenty štátnej politiky v oblasti práce s mládežou,**

**b) utvára právne podmienky, organizačné podmienky, výskumné podmienky a finančné podmienky na rozvoj práce s mládežou,**

**c) koordinuje činnosti ústredných orgánov štátnej správy, miestnych orgánov štátnej správy, obcí a samosprávnych krajov a iných fyzických osôb a právnických osôb v oblasti práce s mládežou,**

d) kontroluje hospodárnosť, efektívnosť, účelnosť a účinnosť použitia finančných prostriedkov poskytnutých zo štátneho rozpočtu na prácu s mládežou,

e) rozhoduje o akreditácii,

f) **analyzuje a vyhodnocuje potreby mládeže,**

g) finančne a metodicky podporuje činnosť fyzických osôb a právnických osôb v oblasti rozvoja práce s mládežou.

**§ 5 Vyšší územný celok**

Vyšší územný celok na úseku starostlivosti o mládež vypracúva a uskutočňuje koncepciu rozvoja práce s mládežou, vyhodnocuje jej plnenie a v súlade s ňou

a) podieľa sa na získavaní a analýze informácií o mládeži vo svojej pôsobnosti,

**b) podporuje organizovanie práce s mládežou,**

**c) podporuje činnosť zdravotne znevýhodnenej mládeže, mládeže zo sociálne znevýhodneného prostredia, mládeže z najmenej rozvinutých okresov a mládeže znevýhodnenej iným spôsobom,**

d) ustanovuje koordinátora práce s mládežou,

e) zabezpečuje prevádzkovanie výchovno-vzdelávacích zariadení a stará sa o ich účelné využívanie,

f) kontroluje účelnosť využívania finančných prostriedkov poskytnutých zo svojho rozpočtu na prácu s mládežou,

g) spolupracuje s fyzickými osobami a právnickými osobami uvedenými v § 15 ods. 2,

**h) podieľa sa na neformálnom vzdelávaní v oblasti práce s mládežou,**

**i) zabezpečuje aktivity v oblasti práce s mládežou prostredníctvom poskytovania finančných prostriedkov z rozpočtu vyššieho územného celku,**

j) podporuje zapojenie mládeže do dobrovoľníckej služby,

k) podporuje spoluúčasť mládeže.

**§ 6 Obec**

(1) Obec na úseku starostlivosti o mládež

**a) podporuje uskutočňovanie práce s mládežou na svojom území,**

**b) utvára podmienky na rozvoj práce s mládežou,**

**c) podporuje činnosť zdravotne znevýhodnenej mládeže, mládeže zo sociálne znevýhodneného prostredia, mládeže z najmenej rozvinutých okresov a mládeže znevýhodnenej iným spôsobom,**

d) spolupracuje s fyzickými osobami a právnickými osobami uvedenými v § 15 ods. 2,

e) podporuje zapojenie mládeže do dobrovoľníckej činnosti,

f) podporuje spoluúčasť mládeže.

(2) Obec môže pri výkone samosprávy ustanoviť koordinátora práce s mládežou.

(3) **Obec, ktorá bola vyhlásená za mesto**, na úseku starostlivosti o mládež okrem pôsobností podľa odsekov 1 a 2 aj **vypracúva, uskutočňuje, aktualizuje koncepciu rozvoja práce s mládežou** a vyhodnocuje jej plnenie.

### Kompetencie v oblasti implementácie ďalších opatrení

V tejto kapitole sú uvedené ďalšie kompetencie relevantné pre návrh možných opatrení pre riadenie identifikovaných rizík.

#### Zákon č. 575/2001 Z. z.

o organizácii činnosti vlády a organizácii ústrednej štátnej správy

**§ 10 Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky**

(1) Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky je ústredným orgánom štátnej správy pre

a) riadenie, koordináciu a dohľad nad využívaním finančných prostriedkov z fondov Európskej únie,

b**) oblasť investícií v rozsahu strategického plánovania a strategického projektového riadenia**, ako aj koordináciu investičných projektov v pôsobnosti Ministerstva investícií, regionálneho rozvoja a **informatizácie Slovenskej republiky**,

c) regionálny rozvoj vrátane koordinácie prípravy politík regionálneho rozvoja,

d) tvorbu, koordináciu a uskutočňovanie politiky mestského rozvoja,

e) **centrálne riadenie informatizácie spoločnosti** a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní verejných prostriedkov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a **koordináciu plnenia úloh v oblasti informatizácie spoločnosti.**

**...**

**§ 11 Ministerstvo vnútra Slovenskej republiky**

Ministerstvo vnútra Slovenskej republiky je ústredným orgánom štátnej správy pre

* 1. ochranu ústavného zriadenia, verejného poriadku, **bezpečnosti osôb a majetku**, ochranu a správu štátnych hraníc, bezpečnosť a plynulosť cestnej premávky, ochranu bezpečnosti a plynulosti železničnej dopravy, veci zbraní a streliva, súkromné bezpečnostné služby, vstup na územie Slovenskej republiky a pobyt cudzincov na jej území, občianske preukazy, cestovné doklady a oprávnenia na vedenie motorových vozidiel, otázky azylantov a odídencov, evidenciu obyvateľov, evidenciu cestných motorových a prípojných vozidiel, integrovaný záchranný systém, civilnú ochranu a ochranu pred požiarmi,
  2. ...

### Kompetencie v oblasti ochrany zdravia mládeže

#### Zákon č. 575/2001 Z. z.

**§ 19 Ministerstvo zdravotníctva Slovenskej republiky**

(1) Ministerstvo zdravotníctva Slovenskej republiky je ústredným orgánom štátnej správy pre

a) zdravotnú starostlivosť,

**b) ochranu zdravia,**

**...**

#### Zákon č. 355/2007 Z. z.

o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov

**§ 5 Úrad verejného zdravotníctva**

(4) Úrad verejného zdravotníctva

* 1. vypracúva návrhy zásadných smerov a priorít štátnej zdravotnej politiky na úseku verejného zdravia, ...

f) posudzuje potrebu vykonania hodnotenia vplyvov na verejné zdravie na národnej úrovni a na regionálnej úrovni a posudzuje hodnotenie vplyvov na verejné zdravie na národnej úrovni a na regionálnej úrovni,

**§ 10 Úlohy na úseku prevencie ochorení a iných porúch zdravia**

Ak v tomto zákone nie je ustanovené inak, úrad verejného zdravotníctva a regionálne úrady verejného zdravotníctva

* 1. zúčastňujú sa na príprave **celospoločenských a regionálnych programov** podpory, ochrany a rozvoja verejného **zdravia zameraných na ovplyvňovanie verejného zdravia prostredníctvom životného štýlu**, výživových faktorov a **prevenciou rizikových faktorov,**

**§ 11 Špecializované úlohy verejného zdravotníctva**

Ak v tomto zákone nie je ustanovené inak, úrad verejného zdravotníctva a regionálne úrady verejného zdravotníctva v rozsahu svojej špecializácie ...

e) monitorujú vzťah determinantov zdravia a verejného zdravia, ...

n) monitorujú zdravotný stav obyvateľstva a jeho skupín vo vzťahu k životným podmienkam a pracovným podmienkam, spôsobu života a práce a zdravotného uvedomenia ľudí,

p) vykonávajú identifikáciu zdravotných rizík a vypracúvajú návrhy na ich minimalizáciu,

**§ 14 Poradenská činnosť**

(1) Úrad verejného zdravotníctva a regionálne úrady verejného zdravotníctva vykonávajú **poradenskú činnosť v oblasti podpory a ochrany zdravia**, zriaďujú a prevádzkujú poradenské centrá ochrany a podpory zdravia.

(2) Cieľom poradenských centier ochrany a podpory zdravia je z**nižovanie výskytu zdravotných rizík prostredníctvom všeobecného a špecializovaného poradenstva zameraného na pozitívnu zmenu spôsobu života** s využitím vedecky overených poznatkov a metód z oblasti medicíny a verejného zdravotníctva.

(3) Všeobecné poradenstvo pozostáva z aktívneho vyhľadávania a stanovovania rizikových faktorov srdcovo-cievnych, nádorových a iných chronických neprenosných ochorení a zo sprostredkovania informácií zrozumiteľnou formou o zásadách správneho spôsobu života a motivácie k pozitívnym zmenám pri predchádzaní najzávažnejším chronickým neprenosným ochoreniam.

(4) Špecializované poradenstvo je zamerané na prevenciu najzávažnejších neprenosných ochorení **ovplyvňovaním rizikových faktorov životného štýlu**, najmä fajčenia, **nedostatočnej fyzickej aktivity, nesprávnej výživy, obezity a stresu.**

(5) Poradenské centrá ochrany a podpory zdravia zabezpečujú individuálne, skupinové a hromadné poradenstvo.

## Stratégia Slovenskej republiky pre mládež na roky 2021 – 2028

Táto Stratégia [[101]](#footnote-101) je relevantná pre návrh možných opatrení pre riadenie rizík v rámci Kap. 6. Vybrané navrhované konkrétne opatrenia v rámci jednotlivých cieľov sú priamo aplikovateľné aj na problematiku rizík mládeže v kybernetickom priestore.

### Vecný rámec

**Citácia z vymedzenia vecného rámca Stratégie:**

„Stratégia Slovenskej republiky pre mládež na roky 2021 – 2028 (ďalej aj „Stratégia“) definuje kľúčové oblasti, ciele, opatrenia a indikátory smerujúce k zlepšeniu situácie mladých ľudí.

Vychádza z poznatkov a dôkazov o skutočných potrebách mladých ľudí a je výsledkom konštruktívneho dialógu mládeže so zástupcami verejnej správy, regionálnej a miestnej samosprávy, a mimovládneho sektora. Do dva roky trvajúcich konzultačných procesov prípravy Stratégie sa zapojilo viac ako 300 subjektov z celého Slovenska.

Stratégia vychádza zo základných zásad, ako sú dôstojnosť, spravodlivosť, rovnosť, rešpekt a autonómia, a súčasne sa opiera o princíp aktívnej účasti, inklúzie a rovného prístupu k príležitostiam.

Mládežnícka politika ako príprava, tvorba, ovplyvňovanie a uvádzanie do praxe širokého spektra opatrení, ktoré priamo alebo nepriamo ovplyvňujú kvalitu života mladého človeka sa realizuje na všetkých úrovniach: medzinárodnej, európskej, národnej, regionálnej a miestnej. Stratégia preto podporuje dosiahnutie zmysluplnej občianskej, ekonomickej, spoločenskej, kultúrnej a politickej účasti mladých ľudí na všetkých úrovniach.

Mladí ľudia nie sú homogénnou skupinou, ale majú rôzne záujmy a potreby, ktoré závisia od ich veku, kultúry, náboženstva, vzdelania, ekonomického statusu a mnohých ďalších faktorov.

Stratégia sa snaží reflektovať túto rôznorodosť v jednotlivých oblastiach a opatreniach.

Politika mládeže má silný prierezový charakter. Práve preto vystupuje do popredia potreba spolupráce a koordinácie. Medzirezortná koordinácia jednotlivých úradov, ktoré ovplyvňujú mladých ľudí v mnohých oblastiach ich života a medzisektorová spolupráca medzi inštitúciami štátnej a verejnej správy, územnej samosprávy, mimovládneho sektora (predovšetkým mládežníckych organizácií) a súkromného sektora sú preto kľúčovým predpokladom pre zabezpečenie efektívnych opatrení smerujúcich k skvalitneniu života mladých ľudí.

Stratégia SR pre mládež nadväzuje na Stratégiu EÚ pre mládež na roky 2019-2027 a stotožňuje sa s jej vymedzením aktuálnej situácie mladých ľudí – podľa nej majú mladí ľudia záujem prevziať kontrolu nad svojimi životmi, zapájať sa a podporovať ostatných.

**Napriek tomu čelia neistote týkajúcej sa svojej budúcnosti v dôsledku technologických zmien, demografických trendov, diskriminácie, sociálneho vylúčenia, falošných správ** či dopadov pandémie COVID-19.

Mladí ľudia potrebujú byť odolní a schopní prispôsobiť sa rôznym aktuálnym aj budúcim výzvam. Mnoho mladých ľudí je tiež znepokojených globálnymi otázkami ako sú klimatické zmeny, mier a bezpečnosť.

Slovenská republika sa prijatím Stratégie zaväzuje vytvárať také podmienky pre mladých ľudí, ktoré im umožnia naplno rozvinúť svoju osobnosť, potenciál, slobodne sa realizovať, byť plnoprávnymi členmi spoločnosti a nadobudnúť také vedomosti, zručnosti a skúsenosti, ktoré im prinesú osobné naplnenie, napomôžu viesť kvalitný život, začleniť sa na trhu práce, či založiť si vlastnú rodinu v dospelom veku.

Stratégie a k nim prislúchajúce opatrenia prispievajú a napomáhajú tomu, aby mladí ľudia konali udržateľne, morálne a zodpovedne, mali kľúčové kompetencie potrebné pre život, boli aktívnou súčasťou komunity a spoločnosti, mysleli kriticky a kreatívne, poznali svoje práva, a **dbali na svoje fyzické a psychické zdravie**.

Plnenie cieľov je odpočtované a vyhodnocované na pravidelnej dvojročnej báze. **V polovici obdobia implementácie Stratégie prebehne jej hĺbkové zhodnotenie, v rámci ktorého bude možné zrevidovať jednotlivé úlohy, príp. navrhnúť nové úlohy vyplývajúce z aktuálnej situácie a potrieb.**

**Okrem toho bude pripravený aj komplexný analytický dokument Správa o mládeži, ktorý poskytne detailný pohľad na jednotlivé strategické oblasti.**“

### Prioritné oblasti

**Stratégia sa zameriava na desať prioritných oblastí, ktoré sú vzájomne prepojené:**

1. MLADÍ ĽUDIA V CENTRE ZÁUJMU SPOLOČNOSTI A POLITÍK

2. PARTICIPÁCIA

3. **PRÁCA S MLÁDEŽOU A VOĽNÝ ČAS**

4. DOBROVOĽNÍCTVO

5. INKLÚZIA, ROVNOSŤ A NEDISKRIMINÁCIA

6. **KĽÚČOVÉ KOMPETENCIE**

7. ZAMESTNANOSŤ

**8. DIGITÁLNA TRANSFORMÁCIA**

9. UDRŽATEĽNÁ A ZELENÁ BUDÚCNOSŤ

10. **ZDRAVÝ ŽIVOTNÝ ŠTÝL A PSYCHICKÉ ZDRAVIE**

### Vybrané ciele

**Cieľ 3.2: Vytvárať podmienky pre bezpečné, dostupné a aktívne trávenie voľného času mládeže**

„Voľný čas je popri čase strávenom v rodine a v škole jednou z veľkých a dôležitých oblastí života mladých ľudí. Mladí ľudia sa vo voľnom čase venujú hre, rekreačným aktivitám, záujmovým činnostiam (vrátane umeleckých a športových aktivít), združujú sa v mládežníckych organizáciách alebo ho trávia v kruhu svojich rovesníkov, kde sa socializujú a venujú neštruktúrovaným aktivitám. Poskytuje priestor pre regeneráciu mladých ľudí, budovanie kompetencií dôležitých pre život či prácu, je príležitosťou pre zapojenie sa do komunitných aktivít.

Zodpovednosťou štátu, verejných inštitúcií a relevantných aktérov je prispievať k vytváraniu podmienok na to, **aby mladí ľudia mohli tráviť svoj voľný čas zmysluplne, v bezpečnom prostredí a v zmysle odporúčaní WHO v dostatočnom dennom pohybovom objeme**.

Nie všetci mladí ľudia majú rodinné zázemie, ktoré ich vedie k aktívnemu využívaniu voľného času, resp. finančná náročnosť voľnočasových aktivít je bariérou pre zapájanie sa do aktivít. Títo mladí ľudia predstavujú najohrozenejšiu skupinu vo vzťahu k sociálno-patologickým javom, podliehanie extrémizmu a radikalizmu.

Práve preto je dôležité venovať samostatnú pozornosť komunitným a nízkoprahovým programom a službám zameraným na prácu s neorganizovanou mládežou vo voľnom čase, vrátane sídliskovej a vidieckej mládeže.“

Vybrané opatrenia:

OPATRENIE 3.2.1

Vytvárať, rozvíjať a implementovať programy a dotačné schémy zamerané na podporu voľnočasových, záujmových, rovesníckych, dobrovoľníckych a komunitných aktivít mladých ľudí na miestnej, regionálnej a celonárodnej úrovni **vrátane programov digitálnej práce s mládežou.**

OPATRENIE 3.2.2

Vytvárať podmienky na podporu športových aktivít mladých ľudí, vrátane podpory neprofesionálneho a nesúťažného športovania.

OPATRENIE 3.2.5

Podporovať nízkoprahové prístupy v práci s mládežou, ktoré prepájajú klubovú a terénnu prácu s mládežou.

**Cieľ 6.1: Rozvíjať a posilňovať kľúčové kompetencie a znižovať nerovnosti kompetencií**

„Východisko: Svetové ekonomické fórum definuje najdôležitejšie zručnosti do roku 2025 nasledovne:

analytické a inovatívne myslenie; aktívne vzdelávanie a strategické učenie; komplexné riešenie problémov; kritické myslenie a analýza; kreativita, originalita a iniciatíva; vedenie a sociálny vplyv; využitie, monitorovanie a kontrola technológií; návrh technológií a programovanie; odolnosť, tolerancia voči stresu a flexibilita; úvaha, riešenie problémov a predstavivosť; emocionálna inteligencia.“

Vybrané opatrenia:

OPATRENIE 6.1.1

Vytvárať a implementovať programy pre rozvoj a posilňovanie kľúčových kompetencií mladých ľudí a pracovníkov s mládežou, koordinátorov práce s mládežou a všetkých ďalších aktérov pracujúcich s mládežou.

OPATRENIE 6.1.2

Prepájať formálne a neformálne vzdelávanie s presahom do sveta práce a občianskeho života.

OPATRENIE 6.1.3

Podporovať projekty zamerané na rozvoj kľúčových kompetencií.

**Cieľ 8.1: Podporovať zodpovednú a bezpečnú digitálnu transformáciu**

“Násilie prostredníctvom technológií a v online priestore môže mať mnoho podôb a foriem. Takmer polovica mladých ľudí (46 %) na stredných školách na Slovensku súhlasí s tvrdením, že sociálne siete sú často zdrojom šikany. Na Slovensku je najvyššia miera výskytu kybernetického obťažovania medzi členskými štátmi EÚ, až 13 % dievčat a žien zažilo formu kybernetického obťažovania za posledný rok pred konaním prieskumu, v porovnaní s 5-percentným európskym priemerom. Z výskumu Výskumného ústavu detskej psychológie a patopsychológie v Bratislave vyplýva, že so sexuálnymi narážkami a komentármi na internete má skúsenosť 37,0 % dievčat a 22,0 % chlapcov. 36,4 % dievčat a 14,9 % chlapcov zažilo, že ich niekto na internete presviedčal alebo nútil, aby mu poslali svoju fotku alebo video, 25,9 % dievčat a 16,3 % chlapcov uvádza, že boli sexuálne obťažovaní na internete.“

Vybrané opatrenia:

OPATRENIE 8.1.3

Podporovať tvorbu, rozvoja a implementácie programov zameraných na podporu kritického myslenia a elimináciu dezinformácií v neformálnom vzdelávaní a ich prepájanie s formálnym vzdelávaním

OPATRENIE 8.1.4

Zvyšovať povedomie a šíriť osvetu o zodpovednom a bezpečnom používaní digitálnych technológií, vrátane oblasti negatívnych dopadov digitalizácie spojených s počítačovou kriminalitou.

OPATRENIE 8. 1. 5

Vytvoriť, finančne zabezpečiť a implementovať programy zamerané na prevenciu a elimináciu násilia prostredníctvom technológií a v online priestore, vrátane kyberobťažovania a kyberšikany.

OPATRENIE 8.1.6

Zvyšovať povedomie o zmysluplnom využívaní informačno-komunikačných technológií a o nástrojoch na ochranu pred negatívnymi dopadmi ich nesprávneho používania.

OPATRENIE 8. 1. 7

**Vytvoriť akčný plán k Národnej koncepcii ochrany detí v digitálnom priestore.**

*Poznámka: Existujúca Národná koncepcia sa týka časového horizontu do roku 2025.*

**CIEĽ 10.1: Podpora zdravého životného štýlu a psychického zdravia mládeže**

„Podľa výskumu HBSC viac ako tretina 15-ročných dievčat a chlapcov na Slovensku pociťovalo nervozitu, podráždenosť alebo mala problémy so zaspávaním aspoň raz týždenne. Úzkosť a depresia sú podľa WHO jednou z hlavných príčin chorôb adolescentov vo svete, pričom sú viac ohrozené dievčatá ako chlapci. Podľa výsledkov HBSC je vo veku 15 rokov fyzicky aktívnych už iba 12% dievčat. Tretím najčastejším zdravotným problémom u adolescentných dievčat sú poruchy príjmu potravy, pričom menej ako 25 % ...

Oblasť zdravého životného štýlu a psychického zdravia mládeže úzko súvisí aj s inými oblasťami vymedzenými v tejto stratégii. Viaceré opatrenia, ktoré neuvádzame pri špecifikovaní tejto oblasti, no napriek tomu majú na zdravý životný štýl a psychické zdravie mládeže pozitívny vplyv, sú z toho dôvodu uvedené už vyššie, napríklad v oblasti práce s mládežou a voľného času.“

Vybrané opatrenia:

OPATRENIE 10.1.1

V Národnom programe duševného zdravia reflektovať potreby mládeže v rámci zabezpečovania a podpory anonymnej, bezplatnej a ľahko dostupnej siete poradenstva a pomoci pre mladých ľudí.

OPATRENIE 10.1.2

Realizovať sekundárnu a terciárnu prevenciu v oblasti najčastejších problémov mladých ľudí, zvládania ťažkých životných situácií a psychických porúch mladých ľudí.

OPATRENIE 10.1.3

Zabezpečiť pre osoby pracujúce s mladými ľuďmi kvalitnú odbornú prípravu zameranú na prvú pomoc pri problémoch v oblasti psychického zdravia.

OPATRENIE 10.1.4

Zabezpečiť a podporovať bezplatnú a ľahko dostupnú sieť poradenstva a pomoci pre mladých ľudí (aj anonymnú), vrátane online poradenstva ako aj krízovej intervencie.

## Národná koncepcia ochrany detí v digitálnom priestore

### Vecný rámec

Táto Koncepcia [[102]](#footnote-102) je nadrezortným dokumentom, je vypracovaná na obdobie do roku 2025.

„Deti sú súčasťou digitálneho priestoru bez ohľadu na ich vek, pohlavie, kultúrne, národnostné, sociálne pozadie, vrátane detí s rôznymi formami zdravotného postihnutia či detí so špeciálnymi výchovno-vzdelávacími potrebami.

Digitálny mediálny svet prináša množstvo príležitostí, ale má aj výrazný rizikový potenciál a dá sa zhrnúť do štyroch kategórii:

* nezákonný obsah/správanie,
* obsah nevhodný pre danú vekovú skupinu,
* nevhodné kontakty,
* nevhodné správanie.

Kontext, v ktorom žijeme, núti rodičov, učiteľov, vychovávateľov a pracovníkov s mládežou učiť seba a žiakov vnímať médiá s porozumením a na to je potrebné získať mediálne kompetencie, ktoré by im pomohli využívať mediálne obsahy zodpovedne, bezpečne, kriticky a tvorivo s dôrazom na dodržiavanie ľudských práv, morálny kontext a vekovú vhodnosť. Je možné, že nás čakajú ďalšie zmeny, ktoré si v súčasnosti nevieme ani predstaviť. Problémom je rýchlosť a nepredvídateľnosť zmien digitálneho priestoru, pri ktorých riešenia rýchlo starnú, čo tiež sťažuje prevenciu a výchovu.

**Frekvencia nežiadúcich javov**

* 30% slovenských detí vo veku od 11 do 18 rokov dostáva žiadosť o zaslanie vlastnej nahej fotografie
* Aktívny self sexting vo forme odosielania vlastných fotografií zobrazujúcich úplnú alebo čiastočnú nahotu realizuje v SR 16 % maloletých od 11 do 18 rokov
* Nahlasovanie online nezákonného obsahu Stopline.sk vrátane sexuálneho zneužívania detí v roku 2017 stúpol počet hlásení spomínaného obsahu oproti roku 2016 z počtu 4104 na 6609. Najvyšší počet hlásení sa týka detskej pornografie.

### Členenie ohrození

1. **Sexuálne ohrozenia**
   1. detská pornografia
   2. pornografia
   3. prostitúcia
   4. kyberprostitúcia
   5. sexting,
   6. sexuálne násilie v partnerstve, grooming,
   7. sexuálne obťažovanie,
   8. zneužitie,
   9. vydieranie,
   10. vykorisťovanie,
   11. sexuálny nátlak,
   12. nevyžiadané sexuálne kontakty,
   13. zverejňovanie erotiky, nahota,
   14. erotický telefónny hovor alebo videohovor,
   15. webcam trolling,
   16. patologické sexuálne praktiky,
   17. obchodovanie s deťmi
2. **Násilie**
   1. kyberšikanovanie,
   2. obsesívne prenasledovanie,
   3. stalking,
   4. obťažovanie,
   5. happy slapping,
   6. obscénny jazyk,
   7. divácke násilie,
   8. mučenie,
   9. umieranie,
   10. fyzické a psychické utrpenie
3. **Neznášanlivosť**
   1. nenávistné prejavy,
   2. vyhrážanie,
   3. zastrašovanie,
   4. ohováranie a klebety,
   5. antisemitizmus,
   6. homofóbia,
   7. xenofóbia,
   8. rasizmus,
   9. popieranie holokaustu,
   10. radikalizmus,
   11. regrútovanie,
   12. extrémizmus,
   13. terorizmus,
   14. ohrozovanie ľudskej dôstojnosti a základných práv a slobôd
4. **Neželaný životný štýl**
   1. navádzanie na protispoločenskú činnosť,
   2. propagácia
      1. vojny,
      2. gangov,
      3. samovrážd,
   3. manipulatívne svetonázorové a spirituálne skupiny,
   4. nebezpečné výzvy/hecovanie (challenges),
   5. svojky (selfie-killfie),
   6. žarty (pranks),
   7. devastácia životného prostredia,
   8. online nakupovanie,
   9. tlak na utrácanie peňazí,
   10. propagácia
       1. alkoholizmu,
       2. fajčenia,
       3. užívanie omamných látok, drog, jedov a prekurzorov, návody na výrobu drog,
       4. propagácia anorexie, bulímie,
   11. sebapoškodzovanie,
   12. ohrozenie zdravia,
   13. problém sociálneho porovnávania,
   14. závisť a žiarlivosť
5. **Manipulácia, dezinformácia**
   1. obavy týkajúce sa ideológie a hodnôt,
   2. falošné správy (fake news),
   3. hoax,
   4. politická propaganda,
   5. pseudohodnoty,
   6. riziká,
   7. whistleblowing,
   8. klamlivá reklama,
   9. nevhodná reklama pre deti,
   10. konšpiračné teórie
6. **Nadmerné používanie, závislosť**
   1. gambling,
   2. nadmerné používanie
      1. hier,
      2. mobilu a
      3. internetu,
   3. nadmerné používanie
      1. pornografie,
         1. sociálnych sietí,
         2. informácií,
   4. nomofobia (strach z neprítomnosti mobilu),
   5. strach zo zmeškania/nezúčastnenia sa niečoho (Fear of missing out),
   6. sociálna úzkosť,
   7. kyberchondria,
   8. izolácia,
   9. kyberstres,
   10. kyberfóbia
7. **Porušovanie duševného vlastníctva**
   1. nezákonné sťahovanie obsahov,
   2. porušovanie autorského práva
8. **Podvody**
   1. Počítačová kriminalita,
   2. hacking,
   3. phishing,
   4. smishing,
   5. vishing
   6. nevyžiadaný obsah,
   7. SPAM,
   8. kryptomeny,
   9. vydieranie,
   10. nátlak
9. **Porušovanie ochrany osobných údajov** 
   1. Právo na výmaz, právo na transparentné a zrozumiteľné informácie o spracúvaní osobných údajov, právo na obmedzenie spracúvania, právo nebyť predmetom automatizovaného individuálneho rozhodovania vrátane profilovania môžu byť ohrozené, resp. ich výkon obmedzený konaním prevádzkovateľa.
   2. Technické zabezpečenie kontroly veku dieťaťa.
   3. Obavy z kontroly a straty súkromia, automatizovaného spracúvania osobných údajov detí.

### Participujúce subjekty

Subjekty participujúce na zabezpečení inštitucionálnej a politickej podpory ochrany detí v digitálnom priestore sú najmä:

* Úrad vlády SR,
* Úrad podpredsedu vlády SR pre investície a informatizáciu,
* Ministerstvo vnútra SR, Rada vlády pre prevenciu kriminality,
* Ministerstvo školstva, vedy, výskumu a športu SR,
* Ministerstvo kultúry SR,
* Ministerstvo spravodlivosti SR,
* Ministerstvo práce, sociálnych vecí a rodiny SR,
* Ministerstvo zdravotníctva SR,
* Ministerstvo financií SR,
* Úrad komisára pre deti,
* Úrad na ochranu osobných údajov SR,
* Úrad priemyselného vlastníctva SR,
* Policajný zbor SR, prokuratúra, súdy,
* Univerzity,
* Slovenská akadémia vied,
* Audiovizuálny fond,
* Registrované cirkvi a náboženské spoločnosti,
* mimovládne organizácie,
* zástupcovia občianskej spoločnosti,
* psychológovia,
* samosprávy,
* školy,
* školské zariadenia,
* poskytovatelia zdravotnej starostlivosti,
* akreditované subjekty a
* ďalšie subjekty.

### Strategické zámery a priority

**Vízia**

Vytvorenie trvalo udržateľného, komplexného, národného, koordinovaného prístupu ochrany detí v digitálnom priestore s jasne vymedzenými kompetenciami, primeranou personálnou, finančnou a dotačnou podporou.

**Hlavný cieľ**

V záujme zdravého psychického, fyzického a morálneho vývinu detí a ich ochrany v digitálnom priestore podporovať efektívne opatrenia v oblasti prevencie, zvyšovania povedomia, potláčania počítačovej kriminality, vzdelávania, výskumu, práva, opatrenia v politickej a inštitucionálnej oblasti, spoluprácu a koordináciu na vnútroštátnej a medzinárodnej úrovni.

**Priority**

*Poznámka: k jednotlivým špecifickým cieľom sú navrhované konkrétne opatrenia*

Priorita 1 – Prevencia

Realizovať systematickú a koordinovanú podporu prevencie v kontexte ochrany detí v digitálnom priestore na Slovensku.

Špecifický cieľ 1.1.

Podporiť účinnú prevenciu vo formálnom a neformálnom vzdelávaní detí a žiakov

Špecifický cieľ 1.2.

Podporiť digitálne služby a obsahy, ktoré pomáhajú vytvárať dôveryhodnejší, bezpečnejší a zodpovednejší digitálny priestor pre deti.

Špecifický cieľ 1.3.

Podporovať celoživotné vzdelávanie rodičov, pedagogických a odborných zamestnancov, pracovníkov s deťmi a mládežou atď.

Opatrenia:

Zabezpečiť, aby deti, rodičia, opatrovatelia, pedagogickí a odborní zamestnanci, pracovníci s deťmi a mládežou boli adekvátne informovaní o právach a povinnostiach detí v digitálnom priestore, vrátane existujúcich obmedzení (napr. filtrovanie obsahu), **rizikách digitálneho priestoru a možnostiach ochrany a pomoci *(vecný rámec pre vytvorenie Katalógu rizík).***

Priorita 2 – Intervencia

Komplexne adekvátne reagovať na nebezpečenstvo, ktorému deti v digitálnom prostredí čelia a na prípady aktuálneho ohrozenia detí.

Špecifický cieľ 2.1.

Zvýšiť efektívnosť a úspešnosť riešenia prípadov ohrozenia detí v digitálnom priestore predovšetkým v rámci legislatívy, exekutívy a jurisdikcie

Špecifický cieľ 2.2.

Poskytovať účinnú pomoc a podporu deťom, rodičom a iným zúčastneným stranám.

Špecifický cieľ 2.3.

Zvýšiť úspešnosť vyhľadávania a odstraňovania webových obsahov obsahujúcich alebo šíriacich detskú pornografiu a iné nebezpečné obsahy na území SR a mimo územia SR.

Priorita 3 - Následná starostlivosť

Podporovať účinnú a efektívnu následnú starostlivosť pre obete všetkých foriem ohrození v digitálnom prostredí ale aj podporovať prácu s páchateľmi trestných činov v digitálnom prostredí.

Špecifický cieľ 3.1.

Zabezpečiť účinnú a efektívnu následnú starostlivosť pre obete a postihnuté subjekty v rámci systému ochrany detí v digitálnom priestore.

**Horizontálne priority**

Horizontálna priorita 1 - Koordinácia, inštitucionálna a finančná podpora

Vytvoriť komplexný, koordinovaný, národný prístup ochrany detí v digitálnom priestore s jasne vymedzenou právomocou a zodpovednosťou príslušných orgánov a primeranou finančnou podporou, ktorá je založená na súčasných vedeckých poznatkoch a osvedčených postupoch.

Horizontálna priorita 2 - Odborná príprava a výskum

Podporovať odbornú, na vedeckých poznatkoch založenú realizáciu opatrení v rámci ochrany detí v digitálnom priestore.

Horizontálna priorita 3 - Ochrana súkromia a údajov detí

Zabezpečiť systematickú a informovanú ochranu súkromia a osobných údajov detí na Slovensku.

Štát, ako hlavný zodpovedný subjekt, by mal podniknúť primerané kroky na ochranu detí pred porušovaním súkromia a ľudských práv v digitálnom priestore a zabezpečiť, aby mali deti prístup k účinnej náprave.

### Akčný plán

Ku Koncepcii bol vypracovaný Akčný plán k Národnej koncepcii ochrany detí v digitálnom priestore na roky 2024 – 2025 [[103]](#footnote-103), ktorý detailnejšie špecifikuje jednotlivé aktivity Koncepcie.

Hlavný gestor tohto plánu je:

Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

**Vybrané úlohy**

Špecifický cieľ HP 1.1.:

Aplikovať koordinovaný multidisciplinárny národný prístup a zabezpečovať konzistentnosť v oblasti ochrany detí v digitálnom priestore.

Úloha 1:

Realizovať systém zabezpečujúci koordináciu a kontrolu vykonávania Národnej koncepcie ochrany detí v digitálnom priestore prostredníctvom expertnej platformy so zapojením relevantných subjektov verejnej správy, vrátane ústredných orgánov štátnej správy, mimovládnych organizácií, vedeckých a výskumných inštitúcií.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Úloha 3:

Koordinovať činnosť Centra bezpečného internetu v súlade so štandardmi a praxou medzinárodnej siete Insafe, vrátane zastupovania Slovenskej republiky v štruktúrach politiky ochrany detí pred násilím v digitálnom prostredí na medzinárodnej úrovni.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Špecifický cieľ HP 2.1.:

Podporovať odbornú prípravu a vzdelávanie zamestnancov pracujúcich s deťmi a realizovať výskumy zamerané na ochranu detí v digitálnom priestore.

Úloha 4:

Podporovať vznik a šírenie vedeckých štúdií o problematike ochrany detí v digitálnom priestore. Organizovať celoštátnu konferenciu zameranú na ochranu detí v digitálnom priestore.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Špecifický cieľ 1.1.

Podporovať účinnú prevenciu vo formálnom a neformálnom vzdelávaní detí a ich rodičov a opatrovateľov

Úloha 7:

Realizovať preventívne aktivity zamerané na ochranu detí a ich osobných údajov v digitálnom priestore s využitím metód neformálneho vzdelávania v práci s mládežou.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Úloha 11:

Vytvoriť zoznam materiálov (vrátane vzdelávacích hier), ktoré je možné využívať vo formálnom a neformálnom vzdelávaní detí a žiakov s prehodnotením ich aktuálnosti vzhľadom na prítomné riziká v digitálnom priestore, informovať o vytvorenom zozname odbornú i laickú verejnosť.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Úloha 12:

Aktualizovať a/alebo doplniť témy súvisiace s ochranou detí v digitálnom priestore vo vzdelávacích dokumentoch (Štátny vzdelávací program) s dôrazom na ich funkčné zapracovanie. Reflektovať uvedené témy v aktuálnych Sprievodcoch školskými rokmi.

Gestor: Ministerstvo školstva, výskumu, vývoja a mládeže SR

Úloha 13:

**Podporovať aktivity zamerané na rozvoj** mediálnej výchovy, mediálnej gramotnosti, **informačnej bezpečnosti** a kritického myslenia, vrátane boja proti dezinformáciám.

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

Úloha 15:

**Pripraviť a pravidelne aktualizovať sériu odporúčaní pre rodičov o tom, ako sa správať v digitálnom prostredí.**

Gestor: Ministerstvo práce, sociálnych vecí a rodiny SR - Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (NKS)

## Legislatívny rámec Trestného zákona

V tejto kapitole je uvedený rámec Trestného zákona relevantný pre Katalóg rizík.

### Vymedzenie dôležitých pojmov

**§ 19 Páchateľ**

(1) Páchateľ trestného činu je ten, kto trestný čin spáchal sám.

**§ 20 Spolupáchateľ**

Ak bol trestný čin spáchaný spoločným konaním dvoch alebo viacerých páchateľov (spolupáchatelia), zodpovedá každý z nich, ako keby trestný čin spáchal sám.

**§ 21 Účastník**

(1) Účastník na dokonanom trestnom čine alebo na jeho pokuse je ten, kto úmyselne

a) zosnoval alebo riadil spáchanie trestného činu (organizátor),

b) naviedol iného na spáchanie trestného činu (návodca),

c) požiadal iného, aby spáchal trestný čin (objednávateľ), alebo

d) poskytol inému pomoc na spáchanie trestného činu, najmä zadovážením prostriedkov, odstránením prekážok, radou, utvrdzovaním v predsavzatí, sľubom pomôcť po trestnom čine (pomocník).

(2) Na trestnú zodpovednosť účastníka sa použijú ustanovenia o trestnej zodpovednosti páchateľa, ak tento zákon neustanovuje inak.

**§ 22 Vek**

(1) Kto v čase spáchania činu inak trestného nedovŕšil štrnásty rok svojho veku, nie je trestne zodpovedný.

(2) Pre trestný čin sexuálneho zneužívania podľa § 201 nie je trestne zodpovedný, kto v čase spáchania činu nedovŕšil pätnásty rok svojho veku.

**§ 29 Súhlas poškodeného**

(1) Čin inak trestný nie je trestným činom, ak bol vykonaný so súhlasom poškodeného a nesmeruje proti jeho životu alebo zdraviu.

(2) Nejde o súhlas poškodeného, ak súhlas nebol daný vopred, nebol vážny a dobrovoľný alebo ak v súvislosti s ním bol spáchaný iný trestný čin.

(3) Ustanovenie odseku 1 sa nepoužije, ak podľa skutkovej podstaty trestného činu má byť čin trestný aj vtedy, keď bol daný súhlas poškodeného podľa odseku 1.

**§ 32 Druhy trestov**

Za spáchané trestné činy môže súd uložiť páchateľovi, ktorý je fyzickou osobou, len

1. trest odňatia slobody,
2. trest domáceho väzenia,
3. trest povinnej práce,
4. peňažný trest,
5. trest prepadnutia majetku,
6. trest prepadnutia veci,
7. trest zákazu činnosti,
8. trest zákazu pobytu,
9. trest zákazu účasti na verejných podujatiach,
10. trest straty čestných titulov a vyznamenaní,
11. trest straty vojenskej a inej hodnosti,
12. trest vyhostenia.

**§ 33 Druhy ochranných opatrení**

Ochranné opatrenia sú:

1. ochranné liečenie,
2. ochranná výchova,
3. ochranný dohľad,
4. detencia,
5. zhabanie veci,
6. zhabanie časti majetku.

§ 37

Priťažujúcou okolnosťou je to, že páchateľ

a) spáchal trestný čin z obzvlášť zavrhnutiahodnej pohnútky,

b) spáchal trestný čin ako odplatu voči inému za to, že voči páchateľovi plnil povinnosť vyplývajúcu zo zákona alebo iného všeobecne záväzného právneho predpisu, najmä proti pedagogickému zamestnancovi alebo odbornému zamestnancovi,

...

i) zneužil na spáchanie trestného činu osobu, ktorá nie je trestne zodpovedná,

j) zviedol na spáchanie trestného činu mladistvého,

k) spáchal trestný čin ako organizátor,

### Tresty pre mladistvých

**ŠTVRTÁ HLAVA - OSOBITNÉ USTANOVENIA O STÍHANÍ MLADISTVÝCH [[104]](#footnote-104)**

Tresty: § 109 Druhy trestov

§ 111 Trest povinnej práce

§ 112 Trest zákazu činnosti

§ 112a Trest zákazu účasti na verejných podujatiach

§ 113 Trest vyhostenia

§ 114 Peňažný trest

§ 115 Podmienečný odklad výkonu peňažného trestu

§ 116 Skúšobná doba

§ 116a Trest domáceho väzenia

§ 117 Trest odňatia slobody

§ 118 Mimoriadne zníženie trestu odňatia slobody

§ 119 Podmienečný odklad výkonu trestu a podmienečný odklad výkonu trestu s probačným dohľadom

**§ 117 Trest odňatia slobody**

(1) Trestné sadzby odňatia slobody ustanovené v tomto zákone sa u mladistvých znižujú na polovicu; horná hranica zníženej trestnej sadzby nesmie prevyšovať sedem rokov a dolná hranica zníženej trestnej sadzby dva roky.

(2) Nepodmienečný trest odňatia slobody môže súd mladistvému uložiť len za podmienky, že by vzhľadom na okolnosti prípadu, osobu mladistvého alebo vzhľadom na predtým uložené opatrenia uloženie iného trestu zjavne neviedlo k dosiahnutiu účelu trestu podľa tohto zákona.

(3) V prípade, ak mladistvý spáchal obzvlášť závažný zločin a miera závažnosti takého obzvlášť závažného zločinu pre spoločnosť je vzhľadom na zavrhnutiahodný spôsob vykonania činu alebo vzhľadom na zavrhnutiahodnú pohnútku alebo vzhľadom na ťažký a ťažko napraviteľný následok mimoriadne vysoká, môže súd uložiť trest odňatia slobody nad sedem rokov až do pätnásť rokov, ak má za to, že trest uvedený v odseku 1 na dosiahnutie účelu nepostačuje.

(4) Trest odňatia slobody sa u osôb, ktoré neprekročili osemnásty rok svojho veku, vykonáva v ústavoch na výkon trestu pre mladistvých.

(5) Súd môže rozhodnúť, že v ústave na výkon trestu pre mladistvých sa vykoná trest aj u mladistvého, ktorý už prekročil osemnásty rok svojho veku; pritom prihliadne najmä na dĺžku trestu a na stupeň a povahu narušenia mladistvého.

### Ďalšie dôležité pojmy

**§ 127 Osoba**

(1) Dieťaťom sa rozumie osoba mladšia ako osemnásť rokov, ak tento zákon neustanovuje inak.

(2) Osobou blízkou veku mladistvých sa rozumie osoba, ktorá dovŕšila osemnásty rok svojho veku a neprekročila dvadsaťjeden rokov svojho veku.

(4) Blízkou osobou sa na účely tohto zákona rozumie príbuzný v priamom pokolení, osvojiteľ, osvojenec, súrodenec a manžel; iné osoby v rodinnom alebo obdobnom pomere sa pokladajú za navzájom blízke osoby len vtedy, ak by ujmu, ktorú utrpela jedna z nich, druhá právom pociťovala ako ujmu vlastnú.

(5) Blízkou osobou sa na účely trestných činov vydierania podľa § 189, znásilnenia podľa § 199 ods. 2, sexuálneho násilia podľa § 200 ods. 2, sexuálneho zneužívania podľa § 201 ods. 2, týrania blízkej osoby a zverenej osoby podľa § 208, nebezpečného vyhrážania podľa § 360 ods. 2, nebezpečného prenasledovania podľa § 360a, nebezpečného elektronického obťažovania podľa § 360b alebo financovania terorizmu podľa § 419c ods. 2 rozumie aj bývalý manžel, druh, bývalý druh, rodič spoločného dieťaťa a osoba, ktorá je vo vzťahu k nim blízkou osobou podľa odseku 4, ako aj osoba, ktorá s páchateľom žije alebo žila v spoločnej domácnosti.

(6) Chorou osobou sa na účely tohto zákona rozumie osoba, ktorá v čase činu trpí fyzickou chorobou alebo duševnou chorobou, aj keď prechodnou, bez ohľadu na to, či je dočasne práceneschopná, ako aj osoba so zmenenou pracovnou schopnosťou, invalidná osoba alebo osoba s ťažkým zdravotným postihnutím, pričom intenzita takej choroby alebo postihnutia zodpovedá ťažkej ujme na zdraví.

(7) Bezbrannou osobou sa na účely tohto zákona rozumie osoba, ktorá vzhľadom na svoj vek, zdravotný stav, okolnosti činu alebo okolnosti na strane páchateľa nemala nádej účinne sa ubrániť pred jeho útokom.

(8) Osobou zverenou do starostlivosti alebo dozoru sa na účely tohto zákona rozumie osoba, ktorá je vzhľadom na svoj vek alebo zdravotný stav alebo z iného dôvodu na základe rozhodnutia súdu alebo iného štátneho orgánu, na základe zmluvy zverená inému, aby vo svojej domácnosti alebo v zariadení určenom na tento účel alebo inde na ňu dozeral, staral sa o ňu, zaopatroval ju alebo ju vychovával.

(9) Odkázanou osobou sa na účely tohto zákona rozumie osoba, ktorá svojou výživou, výchovou, hmotným alebo iným zaopatrením alebo starostlivosťou je odkázaná na páchateľa.

(10) Závislou osobou sa rozumie osoba závislá od návykových látok alebo od návykových škodlivých činností.

(11) Podriadenou osobou je osoba, ktorá v dôsledku postavenia je osobne, pracovne, služobne alebo inak svojím postavením, pracovným zaradením, funkciou alebo hodnosťou podriadená páchateľovi a v dôsledku toho je povinná prijímať a plniť jeho pokyny, príkazy alebo rozkazy.

(12) Viacerými osobami sa na účely tohto zákona rozumejú najmenej tri osoby.

§ 128

(1) Verejným činiteľom sa na účely tohto zákona rozumie ... štátny zamestnanec alebo zamestnanec orgánu štátnej správy, územnej samosprávy alebo iného štátneho orgánu.

**§ 139 Chránená osoba**

(1) Chránenou osobou sa rozumie

a) dieťa,

b) tehotná žena,

c) blízka osoba,

d) odkázaná osoba,

e) osoba vyššieho veku,

f) chorá osoba,

g) osoba požívajúca ochranu podľa medzinárodného práva,

h) verejný činiteľ alebo osoba, ktorá plní svoje povinnosti uložené na základe zákona,

i) svedok, znalec, tlmočník alebo prekladateľ, alebo

j) zdravotnícky pracovník pri výkone zdravotníckeho povolania smerujúceho k záchrane života alebo ochrane zdravia.

**§ 130 Vec**

...

(2) Za vec sa považuje aj nehmotná informácia, dáta výpočtovej techniky alebo obrazový záznam na technickom nosiči.

(4) Prisvojením veci sa na účely tohto zákona rozumie odňatie veci z dispozície vlastníka alebo inej osoby, ktorá ju má oprávnene, bez súhlasu, s úmyslom s ňou nakladať ako s vlastnou vecou.

(7) Extrémistickým materiálom sa na účely tohto zákona rozumie písomné, grafické, obrazové, zvukové alebo obrazovo-zvukové vyhotovenie

a) textov a vyhlásení, zástav, odznakov, hesiel alebo symbolov, skupín a hnutí, ktoré smerujú alebo v minulosti smerovali k potláčaniu základných ľudských práv a slobôd,

b) programov alebo ideológií skupín a hnutí, ktoré smerujú alebo v minulosti smerovali k potláčaniu základných ľudských práv a slobôd,

c) obhajujúce, podporujúce alebo podnecujúce nenávisť, násilie alebo neodôvodnene odlišné zaobchádzanie voči skupine osôb alebo jednotlivcovi pre ich príslušnosť k niektorej rase, národu, národnosti, farbe pleti, etnickej skupine, pôvodu rodu alebo pre ich náboženské vyznanie, ak je zámienkou pre predchádzajúce dôvody, alebo

d) ospravedlňujúce, schvaľujúce, popierajúce alebo hrubo zľahčujúce genocídium, zločiny proti mieru, zločiny proti ľudskosti alebo vojnové zločiny, ak bol páchateľ alebo účastník tohto činu odsúdený právoplatným rozsudkom medzinárodného súdu zriadeného na základe medzinárodného práva verejného, ktorého právomoc uznala Slovenská republika, alebo právoplatným rozsudkom súdu Slovenskej republiky.

### Špecifické trestné činy realizovateľné v kybernetickom priestore

**§ 132 Prostitúcia, pornografia a detské pornografické predstavenie**

(3) Pornografiou sa na účely tohto zákona rozumie zobrazenie súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku alebo zobrazenie obnažených pohlavných orgánov určené na sexuálne účely.

(4) Detskou pornografiou sa na účely tohto zákona rozumie zobrazenie skutočnej alebo predstieranej súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku s dieťaťom alebo osobou vyzerajúcou ako dieťa alebo zobrazenie obnažených častí tela dieťaťa alebo osoby vyzerajúcej ako dieťa určené na sexuálne účely.

(5) Detským pornografickým predstavením sa na účely tohto zákona rozumie živé predstavenie určené publiku, a to aj s využitím informačno-technických prostriedkov, v ktorom je dieťa zapojené do skutočného alebo predstieraného sexuálneho konania alebo v ktorom sú obnažované časti tela dieťaťa určené na sexuálne účely.

**§ 140a Trestné činy extrémizmu**

Trestné činy extrémizmu sú trestný čin založenia, podpory a propagácie hnutia smerujúceho k potlačeniu základných práv a slobôd podľa § 421, prejavu sympatie k hnutiu smerujúcemu k potlačeniu základných práv a slobôd podľa § 422, výroby extrémistického materiálu podľa § 422a, rozširovania extrémistického materiálu podľa § 422b, prechovávania extrémistického materiálu podľa § 422c, popierania a schvaľovania holokaustu, zločinov politických režimov a zločinov proti ľudskosti podľa § 422d, hanobenia národa, rasy a presvedčenia podľa § 423, podnecovania k národnostnej, rasovej a etnickej nenávisti podľa § 424, apartheidu a diskriminácie skupiny osôb podľa § 424a a trestný čin spáchaný z osobitného motívu podľa § 140 písm. e).

**201a Sexuálne zneužívanie prostredníctvom elektronickej komunikačnej služby**

Kto prostredníctvom elektronickej komunikačnej služby navrhne dieťaťu mladšiemu ako pätnásť rokov osobné stretnutie v úmysle spáchať na ňom trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie, pričom sám nie je dieťaťom, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

§ 201b

(1) Kto zneužije dieťa mladšie ako pätnásť rokov v úmysle vyvolania sexuálneho uspokojenia jeho účasťou na sexuálnych aktivitách alebo sexuálnom zneužití, hoci sa na nich takéto dieťa nemusí priamo zúčastňovať, alebo kto umožní také jeho zneužitie, potrestá sa odňatím slobody až na dva roky.

(2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 spoločným konaním najmenej dvoch osôb.

**§ 211 Ohrozovanie mravnej výchovy mládeže**

(1) Kto vydá, čo aj z nedbanlivosti, osobu mladšiu ako osemnásť rokov nebezpečenstvu spustnutia tým, že

a) zvádza ju k záhaľčivému alebo nemravnému životu, ...

**§ 215 Neoprávnené užívanie cudzej veci**

(1) Kto sa zmocní cudzej veci malej hodnoty v úmysle prechodne ju užívať alebo kto na cudzom majetku spôsobí malú škodu tým, že neoprávnene vec, ktorá mu bola zverená, prechodne užíva, potrestá sa odňatím slobody až na jeden rok.

**§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku**

(1) Kto neoprávnene prechováva, prepravuje, obstará si alebo inak zadováži alebo poskytne inému platobný prostriedok, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(2) Kto neoprávnene použije platobný prostriedok, potrestá sa odňatím slobody na jeden rok až päť rokov.

(3) Rovnako ako v odseku 2 sa potrestá, kto falšuje, pozmení, napodobní alebo neoprávnene vyrobí platobný prostriedok alebo kto takýto platobný prostriedok prechováva, prepravuje, obstará si alebo inak zadováži, použije alebo poskytne inému.

(4) Kto vyrobí, sebe alebo inému zadováži alebo prechováva nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v odseku 3, potrestá sa odňatím slobody až na tri roky.

**§ 221 Podvod**

(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

**§ 226 Neoprávnené obohatenie**

(1)

Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

**Poškodzovanie cudzej veci**

§ 245

(1) Kto zničí, poškodí alebo urobí neupotrebiteľnou cudziu vec a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na jeden rok.

### Trestné činy špecifické pre kybernetický priestor

**§ 247 Neoprávnený prístup do počítačového systému**

(1) Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.

**§ 247a Neoprávnený zásah do počítačového systému**

(1) Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti

a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo

b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,

potrestá sa odňatím slobody na šesť mesiacov až tri roky.

**§ 247b Neoprávnený zásah do počítačového údaja**

(1) Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

**§ 247c Neoprávnené zachytávanie počítačových údajov**

(1) Kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

**§ 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov**

(1) Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní

a) zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo

b) počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti,

potrestá sa odňatím slobody až na dva roky.

**§ 264 Ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva**

(1) Kto vyzvedá obchodné tajomstvo, bankové tajomstvo, poštové tajomstvo, telekomunikačné tajomstvo alebo daňové tajomstvo v úmysle vyzradiť ho nepovolanej osobe alebo kto také tajomstvo nepovolanej osobe úmyselne vyzradí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

**§ 283 Porušovanie autorského práva**

(1) Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.

### Ďalšie relevantné trestné činy

**§ 359 Násilie proti skupine obyvateľov**

(1) Kto sa skupine obyvateľov vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou, alebo spôsobením škody veľkého rozsahu, alebo kto použije násilie proti skupine obyvateľov, potrestá sa odňatím slobody až na dva roky.

**§ 360 Nebezpečné vyhrážanie**

(1) Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu, potrestá sa odňatím slobody až na jeden rok.

**§ 360a Nebezpečné prenasledovanie**

(1) Kto iného dlhodobo prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že

a) sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe,

b) vyhľadáva jeho osobnú blízkosť alebo ho sleduje,

c) ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli,

d) zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu, alebo

e) ho inak obmedzuje v jeho obvyklom spôsobe života,

potrestá sa odňatím slobody až na jeden rok.

**§ 360b Nebezpečné elektronické obťažovanie**

(1) Kto úmyselne prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že

a) ho dlhodobo ponižuje, zastrašuje, neoprávnene koná v jeho mene alebo dlhodobo inak obťažuje, alebo

b) neoprávnene zverejní alebo sprístupní tretej osobe obrazový, zvukový alebo obrazovo-zvukový záznam jeho prejavu osobnej povahy získaný s jeho súhlasom, spôsobilý značnou mierou ohroziť jeho vážnosť alebo privodiť mu inú vážnu ujmu na právach,

potrestá sa odňatím slobody až na tri roky.

(2) Odňatím slobody na jeden rok až štyri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) na chránenej osobe, alebo

b) z osobitného motívu.

**Šírenie poplašnej správy § 361**

(1) Kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.

(2) Kto správu alebo iné obdobné konanie uvedené v odseku 1, hoci vie, že sú nepravdivé a môžu vyvolať opatrenie vedúce k nebezpečenstvu vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, oznámi právnickej osobe alebo Policajnému zboru alebo inému štátnemu orgánu alebo hromadnému informačnému prostriedku, potrestá sa odňatím slobody na jeden rok až päť rokov.

**§ 368 Výroba detskej pornografie**

(1) Kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo detského pornografického predstavenia alebo umožní také jeho zneužitie, alebo sa inak podieľa na takejto výrobe, potrestá sa odňatím slobody na štyri roky až desať rokov.

(2) Odňatím slobody na sedem rokov až dvanásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) na dieťati mladšom ako dvanásť rokov,

b) závažnejším spôsobom konania,

c) verejne, ...

**§ 369 Rozširovanie detskej pornografie**

(1) Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu, potrestá sa odňatím slobody na jeden rok až päť rokov.

**§ 370 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení**

(1) Kto prechováva detskú pornografiu alebo kto koná v úmysle získať prístup k detskej pornografii prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody až na dva roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto sa úmyselne zúčastní detského pornografického predstavenia.

**Ohrozovanie mravnosti**

§ 371 (1) Kto vyrába, kupuje, dováža alebo si inak zadovažuje a následne predáva, požičiava alebo inak uvádza do obehu, rozširuje, robí verejne prístupnými alebo zverejňuje pornografiu, nosiče zvuku alebo obrazu, zobrazenia alebo iné predmety ohrozujúce mravnosť, v ktorých sa prejavuje neúcta k človeku a násilie alebo ktoré zobrazujú sexuálny styk so zvieraťom alebo iné sexuálne patologické praktiky, potrestá sa odňatím slobody až na dva roky.

§ 372

(1) Kto pornografiu

a) ponúka, prenecháva alebo predáva dieťaťu, alebo

b) na mieste, ktoré je deťom prístupné, vystavuje alebo inak sprístupňuje, potrestá sa odňatím slobody až na dva roky.

(3)

Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a)a získa pre seba alebo pre iného značný prospech, alebo

b) tým, že ponúka, sprístupňuje alebo vystavuje pornografiu, nosiče zvuku alebo obrazu alebo zobrazenia, v ktorých sa prejavuje neúcta k človeku a násilie alebo ktoré zobrazujú sexuálny styk so zvieraťom alebo iné sexuálne patologické praktiky.

§ 372a Podpora a propagácia sexuálnych patologických praktík

(1) Kto podporuje alebo kto verejne alebo na mieste verejnosti prístupnom propaguje, schvaľuje, hrubo zľahčuje alebo sa snaží ospravedlniť sexuálny styk

a) s dieťaťom,

b) s príbuzným v priamom rade alebo so súrodencom,

c) s mŕtvym,

d) so zvieraťom, alebo

e) iné sexuálne patologické praktiky,

potrestá sa odňatím slobody až na dva roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto podporuje alebo kto verejne alebo na mieste verejnosti prístupnom propaguje, schvaľuje, hrubo zľahčuje alebo sa snaží ospravedlniť pedofíliu, nekrofíliu alebo zoofíliu.

**§ 373 Ohováranie**

(1) Kto o inom oznámi nepravdivý údaj, ktorý je spôsobilý značnou mierou ohroziť jeho vážnosť u spoluobčanov, poškodiť ho v zamestnaní, v podnikaní, narušiť jeho rodinné vzťahy alebo spôsobiť mu inú vážnu ujmu, potrestá sa odňatím slobody až na dva roky.

**§ 374 Neoprávnené nakladanie s osobnými údajmi**

(1) Kto neoprávnene poskytne, sprístupní alebo zverejní

a) osobné údaje o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo

b) osobné údaje o inom získané v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie

a tým poruší všeobecne záväzným právnym predpisom ustanovenú povinnosť,

potrestá sa odňatím slobody až na jeden rok.

**Poškodzovanie cudzích práv § 375**

(1) Kto inému spôsobí vážnu ujmu na právach tým, že

a) uvedie niekoho do omylu alebo

b) využije niečí omyl,

potrestá sa odňatím slobody až na dva roky.

**§ 376**

Kto neoprávnene poruší tajomstvo listiny alebo inej písomnosti, zvukového záznamu, obrazového záznamu alebo iného záznamu, počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.

**§ 377 Porušenie dôvernosti ústneho prejavu a iného prejavu osobnej povahy**

(1) Kto poruší dôvernosť neverejne prednesených slov alebo iného prejavu osobnej povahy tým, že ho neoprávnene zachytí záznamovým zariadením a takto zhotovený záznam sprístupní tretej osobe alebo ho iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.

**417 Ohrozenie mieru**

(1) Kto v úmysle narušiť mier akýmkoľvek spôsobom podnecuje k vojne, vojnu propaguje alebo inak podporuje vojnovú propagandu, potrestá sa odňatím slobody na jeden rok až desať rokov.

**§ 419 Teroristický útok**

(1) Kto v úmysle poškodiť ústavné zriadenie alebo obranyschopnosť štátu, narušiť alebo zničiť základnú politickú, hospodársku alebo spoločenskú štruktúru štátu alebo medzinárodnej organizácie, závažným spôsobom zastrašiť obyvateľstvo alebo donútiť vládu štátu alebo iný orgán verejnej moci alebo medzinárodnej organizácie, aby niečo konala, opomenula alebo strpela

a) hrozí spáchaním útoku alebo spácha útok ohrozujúci život, zdravie človeka alebo jeho osobnú slobodu,

b) zničí, znefunkční alebo poškodí verejné zariadenie, dopravný systém, telekomunikačný systém, informačný systém, vrátane závažného bránenia vo fungovaní informačného systému alebo prerušenia fungovania informačného systému, pevnú plošinu na podmorskej plytčine, energetické zariadenie, vodárenské zariadenie, zdravotnícke zariadenie alebo iné dôležité zariadenie, verejné priestranstvo alebo majetok, alebo takým konaním hrozí, ...

potrestá sa odňatím slobody na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie.

**419b Niektoré formy účasti na terorizme**

(1) Kto verejne podnecuje na spáchanie niektorého z trestných činov terorizmu alebo verejne schvaľuje niektorý z trestných činov terorizmu, potrestá sa odňatím slobody na tri roky až desať rokov.

**§ 421 Založenie, podpora a propagácia hnutia smerujúceho k potlačeniu základných práv a slobôd**

(1) Kto založí, podporuje alebo propaguje skupinu, hnutie alebo ideológiu, ktorá smeruje k potlačeniu základných práv a slobôd osôb, alebo ktoré hlása rasovú, etnickú, národnostnú alebo náboženskú nenávisť alebo kto propaguje skupinu, hnutie alebo ideológiu, ktorá v minulosti smerovala k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na jeden rok až päť rokov.

**§ 422a Výroba extrémistického materiálu**

(1) Kto vyrába extrémistický materiál alebo sa podieľa na takejto výrobe, potrestá sa odňatím slobody na tri roky až šesť rokov.

**§ 422b Rozširovanie extrémistického materiálu**

(1) Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje, uvádza do obehu, dováža, vyváža, ponúka, predáva, zasiela alebo rozširuje extrémistický materiál, potrestá sa odňatím slobody na jeden rok až päť rokov.

**§ 422c Prechovávanie extrémistického materiálu**

Kto prechováva extrémistický materiál, potrestá sa odňatím slobody až na dva roky.

**§ 422d Popieranie a schvaľovanie holokaustu, zločinov politických režimov a zločinov proti ľudskosti**

(1) Kto verejne popiera, spochybňuje, schvaľuje alebo sa snaží ospravedlniť holokaust, zločiny režimu založeného na fašistickej ideológii, zločiny režimu založeného na komunistickej ideológii alebo zločiny iného podobného hnutia, ktoré násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy smeruje k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto verejne popiera, schvaľuje, spochybňuje, hrubo zľahčuje alebo sa snaží ospravedlniť genocídium, zločiny proti mieru, zločiny proti ľudskosti alebo vojnové zločiny spôsobom, ktorý môže podnecovať násilie alebo nenávisť voči skupine osôb alebo jej členovi, ak bol páchateľ alebo účastník tohto činu odsúdený právoplatným rozsudkom medzinárodného súdu zriadeného na základe medzinárodného práva verejného, ktorého právomoc uznala Slovenská republika, alebo právoplatným rozsudkom súdu Slovenskej republiky.

**§ 423 Hanobenie národa, rasy a presvedčenia**

(1) Kto verejne hanobí

a) niektorý národ, jeho jazyk, niektorú rasu alebo etnickú skupinu, alebo

b) skupinu osôb alebo jednotlivca pre ich skutočnú alebo domnelú príslušnosť k niektorej rase, národu, národnosti, etnickej skupine, pre ich skutočný alebo domnelý pôvod, farbu pleti, náboženské vyznanie alebo preto, že sú bez vyznania,

potrestá sa odňatím slobody na jeden rok až tri roky.

**§ 424 Podnecovanie k národnostnej, rasovej a etnickej nenávisti**

(1) Kto verejne podnecuje k násiliu alebo nenávisti voči skupine osôb alebo jednotlivcovi pre ich skutočnú alebo domnelú príslušnosť k niektorej rase, národu, národnosti, etnickej skupine, pre ich skutočný alebo domnelý pôvod, farbu pleti, sexuálnu orientáciu, náboženské vyznanie alebo preto, že sú bez vyznania, alebo verejne podnecuje k obmedzovaniu ich práv a slobôd, potrestá sa odňatím slobody až na tri roky.

## Hodnotenie vekovo podmienených rizík digitálnych technológií

V tejto kapitole je uvedený návrh škály hodnotiacej riziká pre interakcie s digitálnymi technológiami v závislosti od veku dieťaťa v oblasti doby strávenej s digitálnymi technológiami a miery negatívneho dopadu rôznych digitálnych aktivít. Navrhovaná škála vychádza z hodnotenia AI v EU legislatíve – viď podkapitola 7.5.4 v tejto časti prílohy.

### Škála pre hodnotenie času stráveného s digitálnymi technológiami

V závislosti od veku rastie odporúčaná maximálna doba práce s digitálnymi technológiami. Na základe prieskumov citovaných v predchádzajúcich kapitolách je zrejmé, že výrazná časť detí tieto odporúčané časy prekračuje (s vedomím rodičov).

Nie je ale jedno, či namiesto odporúčanej jednej hodiny strávi dieťa priemerne s digitálnymi technológiami 2, 4 alebo 6 hodín denne. Preto je vhodné zaviesť škálu, ktorá hodnotí aj mieru prekračovanie odporúčaných časov.

**Škála doby využívania technológií a farebné odlíšenie**

❶ Čas je v súlade s odporúčaniami autorít.

❷ Prekročenie odporúčaného času, **zvýšené** riziko.

❸ Významné prekročenie odporúčaného času, **vysoké riziko**.

❹ Extrémne prekročenie odporúčaného času, možné poškodenie duševného a fyzického zdravia dieťaťa, možné zanedbanie starostlivosti o dieťa, **neakceptovateľné riziko**.

**Veková škála**

*Poznámka: škálu 0 – 3 roky sme navrhli rozdeliť, pretože keď dieťa začne chodiť a byť aktívne, dostáva sa k TV (keď ju pozerajú rodičia alebo starší súrodenci) alebo k digitálnym aktivitám rodičov a starších súrodencov (napr. chce vidieť domáce obrázky a natočené videá, sleduje hry súrodencov na konzole alebo mobile).*

0 – 2 roky

2 – 3 roky

3 – 6 rokov

6 – 9 rokov

9 – 12 rokov

12 - 18 rokov

18 – 30 rokov

### Vek a odporúčané časy

(návrh možného hodnotenie, bude predmetom review v rámci Akčného plánu opatrení)

Pre sledovanie obrazových informácií na digitálnych zariadeniach alebo TV.

Všetky tieto časy sú návrhom a budú predmetom odbornej diskusie.

**0 – 2 roky**

❶ do 5 minút

❷ do 10 minút

❸ 11 - 20 minút

❹ 20+ minút

Vysvetlenie, prečo je v zelenom nie je 0, ale do 5 minút: v reálnom živote rodiny môže ísť o aktivity ako je ukázanie dieťaťa rodine vo videohovore, chvíľkové zahliadnutie na spravodajstvo v TV a dieťa je na rukách, kontrola digitálnych aktivít starších súrodencov a dieťa je na rukách.

**2 – 3 roky**

❶ do 10 minút

❷ do 30 minút

❸ 21 - 120 minút

❹ 121+ minút

Vysvetlenie, prečo je v zelenom nie je 0, ale do 10 minút: v reálnom živote rodiny môže ísť o aktivity ako je ukázanie dieťaťa rodine vo videohovore, chvíľkové zahliadnutie na spravodajstvo v TV, kontrola digitálnych aktivít starších súrodencov, pozeranie večerníčka na TV.

**3 – 6 rokov**

❶ do 30 minút

❷ 30 - 60 minút

❸ 60 minút

❹ 120 minút

**6 – 9 rokov**

❶ do 45 minút

❷ 46 - 90 minút

❸ 60 minút

❹ 120 minút

### Vek a riziká digitálnych aktivít

V každom veku deti vykonávajú rôzne digitálne aktivity. Aj keď sú vykonávané v primeraných časových intervaloch, môžu byť vecne nevhodné. A naopak - aj sú vhodné, ale čas nimi spotrebovaný je neprimeraný.

Nevhodnosť obsahu je rôzna (nevhodné vtipy z osôb (pranks), nepriamo zobrazované násilie v hrách / strach v hororoch, násilie v hrách / násilná pornografia, sadizmus v hrách či výzvy k samovražde).

**Škála negatívnych dopadov digitálnych aktivít a farebné odlíšenie**

❶ Aktivita je v súlade s odporúčaniami autorít pre danú vekovú kategóriu.

❷ Aktivita nie je odporúčaná pre danú vekovú kategóriu (až pre o stupeň vyššiu kategóriu), zvýšené riziko.

❸ Aktivita je škodlivá pre duševné alebo fyzické zdravie dieťaťa, je to vysoké riziko.

❹ Aktivita je nebezpečná pre duševné alebo fyzické zdravie dieťaťa, je to neakceptovateľné riziko.

**Príklady klasifikácie digitálnych aktivít, v primeranej dobe, vek 9 -12 rokov**

(návrh)

❶

* Príprava do školy alebo plnenie školských úloh využitím digitálnych technológií.
* Samo-vzdelávanie využitím digitálnych technológií.
* Digitálna komunikácia v rámci širšej rodiny (videohovory, telefonické hovory, zdieľanie vhodných fotografií a videí).
* Sledovanie vekovo primeraného neinteraktívneho obsahu – detský film, vysielanie pre deti a mládež, hudobné programy, šport, prírodopisné seriály.
* Časovo primerané hranie vhodných hier, v súlade s PEGI klasifikáciou.
* Tvorivé aktivity, napr.
  + Výtvarné aktivity
  + Vlastné hudobné aktivity
  + Vlastné primerané video produkcie
  + Tvorba vlastného obsahu (napr. budovy v Minecrafte)
  + Programovanie

❷

* Príprava do školy alebo plnenie školských úloh nadmerným využitím digitálnych technológií
* Nadmerné sledovanie vekovo primeraného digitálneho obsahu – detský film, vysielanie pre deti a mládež, hudobné programy, šport, prírodopisné seriály.
* Nadmerné hranie vhodných hier, v súlade s PEGI klasifikáciou.
* Používanie vlastného smartfónu.
* Príležitostne videný erotický obsah.
* Pasívne sledovanie vhodného obsahu na sociálnych sieťach.

❸

* Plnenie školských úloh zneužívaním digitálnych technológií (napr. skopírovanie cudzej práce, náhrada veľkej časti vlastnej práce AI).
* Sledovanie vekovo neprimeraného TV obsahu – filmy, videá.
* Hranie nevhodných hier
* Dlhodobé sledovanie streamovaného obsahu, influencerov.
* Príležitostne videná pornografia.
* Prístup a príležitostná konzumácia toxického obsahu (napr. extrémistického).
* Raidy (spoločné aktivity v hrách) 8+ hodín.
* Zobrazované detailné násilie (v počítačovej hre, videu alebo vo filme)
* Vlastné aktivity na sociálnych sieťach, aj keď pod čiastočným dohľadom rodičov.

❹

* Zobrazované sadistické násilie (napr. mučenie v hre, alebo vo filme)
* Vedomé vyhľadávanie a sledovanie pornografie
* Dlhodobé spojité sledovanie krátkych videí
* Raidy (spoločné aktivity v hrách) 8+ hodín, počas noci
* Použitia AI ako plnej náhrady aktivity žiaka.
* Vlastné aktivity na sociálnych sieťach bez dohľadu rodičov.

### Inšpirácia pre škálu

Nariadenie EÚ o umelej inteligencii [[105]](#footnote-105) vymedzuje regulačný rámec pre riadenie rizík súvisiacich s AI, a je v nej uvedené

„ AI môže zároveň v závislosti od okolností týkajúcich sa jej konkrétnej aplikácie, použitia a úrovne technologického vývoja vytvárať riziká a ujmu pre verejné záujmy a základné práva, ktoré sú chránené právom Únie. Toto poškodzovanie môže byť hmotné aj nehmotné vrátane fyzickej, psychickej, spoločenskej alebo ekonomickej ujmy.“

1. Oblasti použitia so zvýšenou mierou rizika ***(Oranžová)***
   1. diagnostika chorôb
   2. autonómne vedenie vozidla
   3. **autonómne vzdelávanie**
   4. biometrická identifikácia jednotlivcov zapojených do trestnej činnosti
2. Oblasti s neakceptovateľnou mieru rizika ***(Červená)***
   1. **Kognitívna manipulácia správania**
   2. Prediktívne vykonávanie policajných funkcií
   3. Rozpoznávanie emócií na pracovisku a vo vzdelávacích inštitúciách a sociálne hodnotenie.
   4. Systémy diaľkovej biometrickej identifikácie v reálnom čase
3. Zakázané praktiky využívajúce AI (všetky viď Čl. 5 Nariadenia EÚ [[106]](#footnote-106)), napr. ***(Čierna)***
   1. používanie systému AI, ktorý využíva podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčiní, že prijmú rozhodnutie, ktoré by inak neprijali, a to spôsobom, ktorý tejto osobe, inej osobe alebo skupine osôb spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

## Klasifikačné schémy pre riziká v digitálnom prostredí

Viaceré medzinárodné inštitúcie vypracovali klasifikačné schémy pre riziká mládeže v digitálnom resp. online prostredí. V zmysle našej terminológie je nimi chápané digitálne alebo online prostredie časťou kybernetického priestoru.

Klasifikácie vychádzajú z analýz rizík založených na zdrojoch hrozieb. V našom dokumente analyzujeme riziká voči aktívam (komplementárny prístup k týmto klasifikáciám).

V nasledujúcich verziách dokumentu bude realizované premapovanie medzi klasifikačnými schémami založenými na zdrojoch hrozieb a klasifikačnými schémami založenými na aktívach.

### OECD

OECD vydalo dokument [[107]](#footnote-107)

CHILDREN IN THE DIGITAL ENVIRONMENT

REVISED TYPOLOGY OF RISKS

OECD DIGITAL ECONOMY PAPERS

V tomto dokumente je navrhnutá nasledujúca klasifikačná schéma:

Obrázok, na ktorom je text, snímka obrazovky, písmo, číslo

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Preklad:

*Nakoľko autor nie je autorizovaným prekladateľom OECD materiálov, uvádzame v zátvorke aj originálne znenie.*

**Kategórie rizík (Risk Categories)**

1. Riziká obsahu (Content Risks)
2. Riziká správania sa (Conduct Risks)
3. Riziká kontaktu (Contact Risks)
4. Riziká spotrebiteľa (Consumer Risks)

Kombinované riziká (Cross-Cutting Risks)

1. Riziká súkromia (Privacy Risks)
2. Riziká pokročilých technológií (Advanced Technology Risks)
3. Riziká pre zdravie a pohodu (Risks on Health and Wellbeing)

**Prejav hrozieb v riziku (Risk Manifestation)**

1. **Riziká obsahu** (Content Risks)
   1. Nenávistný obsah (Hateful Content)
   2. Škodlivý obsah (Harmful Content
   3. Nezákonný obsah (Illegal Content)
   4. Dezinformácie (Disinformation)
2. **Riziká správania** (Conduct Risks)
   1. Nenávistné správanie (Hateful Behaviour)
   2. Škodlivé správanie (Harmful Behaviour)
   3. Nezákonné správanie (Illegal Behaviour)
   4. Problematické správanie vytvorené používateľmi (User-generated Problematic Behaviour)
3. **Riziká kontaktu** (Contact Risks)

*Poznámka: má sa na mysli priama interakcia dvoch alebo viacerých osôb v kybernetickom priestore.*

* 1. Nenávistné interakcie (Hateful Encounters)
  2. Škodlivé interakcie (Harmful Encounters)
  3. Nezákonné interakacie (Illegal Encounters)
  4. Ďalšie problémové interakcie Other Problematic Encounters

1. **Riziká spotrebiteľa** (Consumer Risks)
   1. Riziká marketingu Marketing Risks
   2. Riziko komerčného profilovania (Commercial Profiling Risk)
   3. Finančné riziko (Financial Risk)
   4. Bezpečnostné riziko (Security Risk)

### EÚ

S podporou EÚ v rámci programu Horizon 2020 bol vydaný dokument [[108]](#footnote-108)

The 4Cs: Classifying online risk to children

**Klasifikačná schéma**

**Doterajšia** Obrázok, na ktorom je text, snímka obrazovky, písmo, číslo

Obsah vygenerovaný pomocou AI môže byť nesprávny.

**Novo navrhovaná**

(inšpirovaná klasifikáciou OECD)

**Obrázok, na ktorom je text, snímka obrazovky, písmo, číslo

Obsah vygenerovaný pomocou AI môže byť nesprávny.**

Obrázok, na ktorom je text, snímka obrazovky, písmo, rad

Obsah vygenerovaný pomocou AI môže byť nesprávny.

Preklad:

**Kategórie rizík**

1. **Riziká obsahu (Content Risks)**

Deti sú vystavené nevhodnému alebo škodlivému obsahu, ktorý môžu vidieť, čítať alebo počúvať.

1. **Riziká kontaktu (Contact Risks)**

Deti sú kontaktované alebo sa dostávajú do interakcie s osobami, ktoré môžu mať škodlivý alebo manipulatívny úmysel.

1. **Riziká správania sa (Conduct Risks)**

Dieťa je obeťou, svedkom alebo účastníkom škodlivého správania sa na úrovni rovesníkov (šikanovanie, ponižovanie, vyčleňovanie alebo kyberšikana).

1. **Riziká kontraktov (Contract risks)**

Dieťa je zmluvnou stranou a/alebo je využívané potenciálne škodlivými zmluvnými alebo komerčnými záujmami (napr. hazardné hry, vykorisťujúci alebo vekovo nevhodný marketing a pod.). Taktiež sú sem zahrnuté kontrakty uzatvorené medzi inými stranami, ktoré zahŕňajú dieťa (napr. obchodovanie s deťmi, streamovanie sexuálneho zneužívania detí).

1. **Riziká digitálneho obsahu** (Content risks)
   1. Agresia – Násilný, krvavý, rasistický, extrémistický obsah
   2. Sexualita – Sexualizácia, pornografia a sexuálne explicitný obsah
   3. Hodnoty - Dezinformácie, Vekovo nevhodný marketing, používateľmi generovaný škodlivý obsah
2. **Kontaktné riziká** (Contact risks)
   1. Agresia – Obťažovanie, sledovanie, stalking
   2. Sexualita - Sexuálne obťažovanie alebo zneužívanie, lákanie na vytváranie materiálov týkajúcich škodlivých alebo nezákonných sexuálnych aktivít mládeže
   3. Hodnoty – Ideologická manipulácia, radikalizácia inými osobami, nábor do extrémistických skupín
3. **Riziká správania sa** (Conduct risks)
   1. Agresia- Šikana, nepriateľská aktivita zo strany rovesníkov, troling, shaming
   2. Sexualita - Sexuálne obťažovanie, sexting, sexuálny nátlak
   3. Hodnoty –Nevhodné užívateľské komunity interagujúce s dieťaťom (napr. podporujúce seba-ubližovanie).
4. **Riziká kontraktov (Contract risks)**
   1. Agresia – Phising, krádež identity, hacking, infikácia malvérom a pod.
   2. Sexualita – Obchodovanie s deťmi, komerčná detská pornografia apod.
   3. Hodnoty – Digitálny gambling, loot boxes v hrách, manipulácia k nakupovaniu a pod.

## Globálne riziká súvisiace s kybernetickým priestorom

Svetové ekonomické fórum vydáva každý rok prehľad globálnych rizík [[109]](#footnote-109).

Medzi týmito rizikami sa objavujú aj tie, ktoré priamo alebo nepriamo súvisia s kybernetickým priestorom a teda aj s vplyvmi na mládež.

**Najvýznamnejšie globálne riziká** (citácia z dokumentu)

Obrázok, na ktorom je text, snímka obrazovky, číslo, rovnobežný

Obsah vygenerovaný pomocou AI môže byť nesprávny.

S kybernetickým priestorom priamo alebo nepriamo súvisia riziká (analyzované v kap. 4)

* Chybné informácie a dezinformácie (Misinformation and Disinformation) – č.4
* Sociálna polarizácia (Societal polarization) – č.5
* Erózia ľudských práv (Erosion of human rights and/ or civic freedoms) – č.9
* Nerovnosť (Inequality) – č.10
* Nepriaznivé vplyvy AI technológií (Adverse ourcomes of AI technologies) – č. 13
* Kybernetická špionáž a boj (Cyber espionage and warfare) – č. 14
* Kriminalita a ilegálne ekonomické aktivity (Crime and ilicit economic activity) – č. 15
* Pokles úrovne zdravia a celkovej pohody (Decline of health andf well-being) – č. 20

Medzi riziká na úrovni jedného percenta sa dostalo aj:

* Online negatívne dopady (Online harms)

**Väzby medzi jednotlivými rizikami (RIM – Risk Interconnections Map)**

**Obrázok, na ktorom je diagram, kruh, mapa, rad

Obsah vygenerovaný pomocou AI môže byť nesprávny.**

Analogický RIM je vytvorený aj pre riziká súvisiace s kybernetickým priestorom a jeho dopadom na mládež.

**Riziká adresovateľné vhodným vzdelávaním**

V nasledujúcej tabuľke je prehľad rizík, ktoré je možné významne ovplyvniť budovaním povedomia a vzdelávaním

Obrázok, na ktorom je text, snímka obrazovky, softvér, písmo

Obsah vygenerovaný pomocou AI môže byť nesprávny.

**Očakávané top riziká v roku 2035**

**Obrázok, na ktorom je text, snímka obrazovky, písmo, číslo

Obsah vygenerovaný pomocou AI môže byť nesprávny.**

V top 10 sú spomínané riziká súvisiace s kybernetickým priestorom:

* Chybné informácie a dezinformácie (Misinformation and Disinformation)
* Nepriaznivé vplyvy AI technológií (Adverse ourcomes of AI technologies)
* Nerovnosť (Inequality)
* Sociálna polarizácia (Societal polarization)
* Kybernetická špionáž a boj (Cyber espionage and warfare)

## Riziká digitálnych technológií v oblasti základných práv a slobôd

V tejto kapitole uvádzame prehľad základných práv a slobôd občanov SR (vrátane mládeže). Nesprávne použitie alebo zneužitie digitálnych technológii môže mnohé z týchto práv narušiť, alebo ohroziť. Škála pre riziko je rovnaká ako pre ostatné riziká.

Zdrojom pre tento prehľad sú: Charta základných práv EÚ [[110]](#footnote-110) a Ústava Slovenskej republiky.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **P.č.** | **SÚHRNNÝ ZOZNAM ZÁKLADNÝCH PRÁV A SLOBÔD** | **CHARTA ZÁKLADNÝCH PRÁV EÚ** | **ÚSTAVA SR** | **Riziko ohrozenia digitálnymi technológiami** |
| 1 | Právo na nedotknuteľnosť ľudskej dôstojnosti | Hlava I, čl. 1 | Druhá hlava, Druhý oddiel, čl. 19, ods. (1) | S |
| 2 | Právo na rešpektovanie ľudskej dôstojnosti | Hlava I, čl. 1 |  | S |
| 3 | Právo na ochranu ľudskej dôstojnosti | Hlava I, čl. 1 |  | S |
| S | Právo každého na život | Hlava I, čl. 2, ods. 1 | Druhá hlava, Druhý oddiel, čl. 15, ods. (1) a ods. (3) | VN |
| 5 | Právo na ochranu pred trestom smrti | Hlava I, čl. 2, ods. 2 |  |  |
| 6 | Právo na ochranu pred popravou | Hlava I, čl. 2, ods. 2 |  |  |
| 7 | Právo na rešpektovanie telesnej nedotknuteľnosti | Hlava I, čl. 3, ods. 1 | Druhá hlava, Druhý oddiel, čl. 16, ods. (1) | N |
| 8 | Právo na rešpektovanie duševnej nedotknuteľnosti | Hlava I, čl. 3, ods. 1 | Druhá hlava, Druhý oddiel, čl. 16, ods. (1) | N |
| 9 | Právo dotknutej osoby na rešpektovanie jej práva na slobodný a informovaný súhlas v oblasti medicíny a biológie | Hlava I, čl. 3, ods. 2, písm. a) |  | S |
| 10 | Právo na ochranu pred eugenickými praktikami | Hlava I, čl. 3, ods. 2, písm. b) |  | VN |
| 11 | Právo na ochranu pred využívaním ľudského tela a jeho častí na dosiahnutie zisku | Hlava I, čl. 3, ods. 2, písm. c) |  | N |
| 12 | Právo na ochranu pred reprodukčným klonovaním | Hlava I, čl. 3, ods. 2, písm. d) |  | - |
| 13 | Právo na ochranu pred mučením | Hlava I, čl. 4 | Druhá hlava, Druhý oddiel, čl. 16, ods. (2) | - |
| 14 | Právo na ochranu pred neľudským zaobchádzaním alebo trestom | Hlava I, čl. 4 | Druhá hlava, Druhý oddiel, čl. 16, ods. (2) | - |
| 15 | Právo na ochranu pred ponižujúcim zaobchádzaním alebo trestom | Hlava I, čl. 4 | Druhá hlava, Druhý oddiel, čl. 16, ods. (2) | - |
| 16 | Právo na ochranu pred otroctvom | Hlava I, čl. 5, ods. 1 |  | - |
| 17 | Právo na ochranu pred nevoľníctvom | Hlava I, čl. 5, ods. 1 |  | - |
| 18 | Právo na ochranu pred nútenými prácami | Hlava I, čl. 5, ods. 2 | Druhá hlava, Druhý oddiel, čl. 18, ods. (1) | - |
| 19 | Právo na ochranu pred povinnými prácam | Hlava I, čl. 5, ods. 2 |  | - |
| 20 | Právo každého na ochranu pred obchodovaním s jeho osobou | Hlava I, čl. 5, ods. 3 |  | N |
| 21 | Právo na slobodu | Hlava II, čl. 6 | Druhá hlava, Druhý oddiel, čl. 17, ods. (1) | N |
| 22 | Právo na osobnú bezpečnosť | Hlava II, čl. 6 |  | S |
| 23 | Právo na rešpektovanie súkromného života | Hlava II, čl. 7 | Druhá hlava, Druhý oddiel, čl. 16, ods. (1) / čl. 19, ods. (2) | S |
| 24 | Právo na rešpektovanie rodinného života | Hlava II, čl. 7 | Druhá hlava, Druhý oddiel, čl. 19, ods. (2) | S |
| 25 | Právo na rešpektovanie obydlia | Hlava II, čl. 7 | Druhá hlava, Druhý oddiel, čl. 21, ods. (1) | N |
| 26 | Právo na rešpektovanie (súkromnej) komunikácie | Hlava II, čl. 7 | Druhá hlava, Druhý oddiel, čl. 22, ods. (1) a (2) | **V** |
| 27 | Právo na ochranu osobných údajov | Hlava II, čl. 8, ods. 1 | Druhá hlava, Druhý oddiel, čl. 19, ods. (3) | **V** |
| 28 | Právo každého na prístup k zhromaždeným údajom, ktoré sa ho / jej týkajú | Hlava II, čl. 8, ods. 2 |  | S |
| 29 | Právo každého na opravu zhromaždených údajov, ktoré sa ho / jej týkajú | Hlava II, čl. 8, ods. 2 |  | N |
| 30 | Právo požadovať kontrolu pravidiel ochrany osobných údajov zo strany nezávislého orgánu | Hlava II, čl. 8, ods. 3 |  | N |
| 31 | Právo uzavrieť manželstvo | Hlava II, čl. 9 |  | - |
| 32 | Právo založiť rodinu | Hlava II, čl. 9 |  | VN |
| 33 | Právo na slobodu myslenia | Hlava II, čl. 10, ods. 1 | Druhá hlava, Druhý oddiel, čl. 24, ods. (1) | S |
| 34 | Právo na slobodu svedomia | Hlava II, čl. 10, ods. 1 | Druhá hlava, Druhý oddiel, čl. 24, ods. (1) | - |
| 35 | Právo na slobodu náboženského vyznania | Hlava II, čl. 10, ods. 1 | Druhá hlava, Druhý oddiel, čl. 24, ods. (1) | - |
| 36 | Právo na výhradu vo svedomí | Hlava II, čl. 10, ods. 2 |  | - |
| 37 | Právo na slobodu prejavu | Hlava II, čl. 11, ods. 1 | Druhá hlava, Druhý oddiel, čl. 24, ods. (1) a (2) / Tretí oddiel, čl. 26, ods. (1) a (2) | S |
| 38 | Právo na slobodu médií | Hlava II, čl. 11, ods. 2 | Druhá hlava, Tretí oddiel, čl. 26, ods. (2) | S |
| 39 | Právo na pluralitu médií | Hlava II, čl. 11, ods. 2 |  | S |
| 40 | Právo pokojne sa zhromažďovať | Hlava II, čl. 12, ods. 1 | Druhá hlava, Tretí oddiel, čl. 28, ods. (1) | N |
| 41 | Právo slobodne sa združovať s inými na všetkých úrovniach, najmä v súvislosti s politickými, odborárskymi a občianskymi otázkami | Hlava II, čl. 12, ods. 1 | Druhá hlava, Piaty oddiel, čl. 37, ods. (1) | N |
| 42 | Právo zakladať na ochranu svojich záujmov odbory | Hlava II, čl. 12, ods. 1 |  | - |
| 43 | Právo vstupovať do odborov na ochranu svojich záujmov | Hlava II, čl. 12, ods. 1 |  | - |
| 44 | Právo na slobodu umenia | Hlava II, čl. 13 | Druhá hlava, Piaty oddiel, čl. 43, ods. (1) | N |
| 45 | Právo na slobodné vedecké bádanie | Hlava II, čl. 13 | Druhá hlava, Piaty oddiel, čl. 43, ods. (1) | S |
| 46 | Právo na rešpektovanie akademickej slobody | Hlava II, čl. 13 |  | N |
| 47 | Právo na vzdelanie | Hlava II, čl. 14, ods. 1 | Druhá hlava, Piaty oddiel, čl. 42, ods. (1) | N |
| 48 | Právo na prístup k odbornému a ďalšiemu vzdelávaniu | Hlava II, čl. 14, ods. 1 | Druhá hlava, Piaty oddiel, čl. 35, ods. (1) | S |
| 49 | Právo na bezplatnú povinnú školskú dochádzku | Hlava II, čl. 14, ods. 2 | Druhá hlava, Piaty oddiel, čl. 42, ods. (2) | - |
| 50 | Právo slobodne zakladať vzdelávacie inštitúcie | Hlava II, čl. 14, ods. 3 |  | - |
| 51 | Právo rodičov zabezpečiť vzdelanie a výchovu svojich detí v zhode s ich náboženským, filozofickým a pedagogickým presvedčením | Hlava II, čl. 14, ods. 3 | Druhá hlava, Piaty oddiel, čl. 41, ods. (4) | S |
| 52 | Právo na prácu | Hlava II, čl. 15, ods. 1 | Druhá hlava, Piaty oddiel, čl. 35, ods. (3) | **V** |
| 53 | Právo na vykonávanie slobodne zvoleného povolania | Hlava II, čl. 15, ods. 1 | Druhá hlava, Piaty oddiel, čl. 35, ods. (1) | S |
| 54 | Právo na vykonávanie slobodne prijatého povolania | Hlava II, čl. 15, ods. 1 |  | N |
| 55 | Právo každého občana Únie slobodne si hľadať zamestnanie v ktoromkoľvek členskom štáte | Hlava II, čl. 15, ods. 2 |  | N |
| 56 | Právo každého občana Únie slobodne pracovať v ktoromkoľvek členskom štáte | Hlava II, čl. 15, ods. 2 |  | N |
| 57 | Právo každého občana Únie usadiť sa v ktoromkoľvek členskom štáte | Hlava II, čl. 15, ods. 2 |  | N |
| 58 | Právo každého občana Únie poskytovať služby v ktoromkoľvek členskom štáte | Hlava II, čl. 15, ods. 2 |  | N |
| 59 | Právo štátnych príslušníkov tretích krajín, ktorí majú pracovné povolenie, na rovnaké pracovné podmienky ako občania Únie | Hlava II, čl. 15, ods. 3 |  | VN |
| 60 | Právo na slobodu podnikania | Hlava II, čl. 16 | Druhá hlava, Piaty oddiel, čl. 35, ods. (1) | N |
| 61 | Právo vlastniť oprávnene nadobudnutý majetok | Hlava II, čl. 17, ods. 1 | Druhá hlava, Druhý oddiel, čl. 20, ods. (1) | VN |
| 62 | Právo užívať oprávnene nadobudnutý majetok | Hlava II, čl. 17, ods. 1 |  | VN |
| 63 | Právo nakladať s oprávnene nadobudnutým majetkom | Hlava II, čl. 17, ods. 1 |  | VN |
| 64 | Právo odkázať oprávnene nadobudnutý majetok | Hlava II, čl. 17, ods. 1 | Druhá hlava, Druhý oddiel, čl. 20, ods. (1) | N |
| 65 | Právo každého na ochranu pred svojvoľným odobraním jeho majetku | Hlava II, čl. 17, ods. 1 | Druhá hlava, Druhý oddiel, čl. 20, ods. (4) | - |
| 66 | Právo na spravodlivú náhradu v prípade, ak bol niekto zbavený majetku z dôvodu verejného záujmu a v súlade so zákonom | Hlava II, čl. 17, ods. 1 | Druhá hlava, Druhý oddiel, čl. 20, ods. (4) | - |
| 67 | Právo na ochranu duševného vlastníctva | Hlava II, čl. 17, ods. 2 | Druhá hlava, Piaty oddiel, čl. 43, ods. (1) | **V** |
| 68 | Právo na azyl v zmysle pravidiel Ženevského dohovoru z 28. júla 1951 a Protokolu z 31. januára 1967 týkajúcich sa postavenia utečencov | Hlava II, čl. 18 |  | - |
| 69 | Právo na ochranu pred hromadným vyhostením | Hlava II, čl. 19, ods. 1 |  | - |
| 70 | Právo osoby na ochranu pre vysťahovaním, vyhostením alebo vydaním do štátu, kde jej hrozí trest smrti | Hlava II, čl. 19, ods. 2 |  | - |
| 71 | Právo osoby na ochranu pre vysťahovaním, vyhostením alebo vydaním do štátu, kde jej hrozí mučenie | Hlava II, čl. 19, ods. 2 |  | - |
| 72 | Právo osoby na ochranu pre vysťahovaním, vyhostením alebo vydaním do štátu, kde jej hrozí neľudské zaobchádzanie alebo trest | Hlava II, čl. 19, ods. 2 |  | - |
| 73 | Právo osoby na ochranu pre vysťahovaním, vyhostením alebo vydaním do štátu, kde jej hrozí ponižujúce zaobchádzanie alebo trest | Hlava II, čl. 19, ods. 2 |  | - |
| 74 | Právo na uplatňovanie zásady rovnosti všetkých pred zákonom | Hlava III, čl. 20 |  | VN |
| 75 | Právo na ochranu pred diskrimináciou | Hlava III, čl. 21, ods. 1 |  | S |
| 76 | Právo na ochranu pred diskrimináciou z dôvodu štátnej príslušnosti | Hlava III, čl. 21, ods. 2 |  | N |
| 77 | Právo na rešpektovanie kultúrnej rozmanitosti | Hlava III, čl. 22 |  | S |
| 78 | Právo na rešpektovanie náboženskej rozmanitosti | Hlava III, čl. 22 |  | S |
| 79 | Právo na rešpektovanie jazykovej rozmanitosti | Hlava III, čl. 22 |  | S |
| 80 | Právo na ochranu pred nerovnosťou medzi mužmi a ženami vo všetkých oblastiach vrátane zamestnania, práce a odmeňovania | Hlava III, čl. 23 |  | S |
| 81 | Právo menej zastúpeného pohlavia požadovať zachovávanie alebo prijímanie osobitne výhodných opatrení | Hlava III, čl. 23 |  | N |
| 82 | Právo detí na ochranu | Hlava III, čl. 24, ods. 1 | Druhá hlava, Piaty oddiel, čl. 41, ods. (1) | **V** |
| 83 | Právo detí na starostlivosť | Hlava III, čl. 24, ods. 1 | Druhá hlava, Piaty oddiel, čl. 41, ods. (4) | S |
| 84 | Právo detí slobodne vyjadrovať svoje názory | Hlava III, čl. 24, ods. 1 |  | N |
| 85 | Právo detí na rešpektovanie ich najlepších záujmov pri opatreniach orgánov verejnej moci alebo súkromných inštitúcií | Hlava III, čl. 24, ods. 2 |  | - |
| 86 | Právo dieťaťa na pravidelné udržiavanie osobných vzťahov s obidvoma svojimi rodičmi | Hlava III, čl. 24, ods. 3 |  | - |
| 87 | Právo dieťaťa na pravidelné udržiavanie priamych stykov s obidvoma svojimi rodičmi | Hlava III, čl. 24, ods. 3 |  | - |
| 88 | Právo starších osôb na dôstojný život | Hlava III, čl. 25 |  | N |
| 89 | Právo starších osôb na nezávislý život | Hlava III, čl. 25 |  | N |
| 90 | Právo starších osôb na účasť na spoločenskom živote | Hlava III, čl. 25 |  | S |
| 91 | Právo starších osôb na účasť na kultúrnom živote | Hlava III, čl. 25 |  | N |
| 92 | Právo osôb so zdravotným postihnutím využívať opatrenia na zabezpečenie ich nezávislosti | Hlava III, čl. 26 |  | N |
| 93 | Právo osôb so zdravotným postihnutím využívať opatrenia na zabezpečenie ich sociálnej integrácie | Hlava III, čl. 26 |  | S |
| 94 | Právo osôb so zdravotným postihnutím využívať opatrenia na zabezpečenie ich integrácie v zamestnaní | Hlava III, čl. 26 |  | N |
| 95 | Právo osôb so zdravotným postihnutím využívať opatrenia na zabezpečenie ich účasti na spoločenskom živote | Hlava III, čl. 26 |  | S |
| 96 | Právo pracovníkov na informácie a konzultácie v rámci podniku | Hlava IV, čl. 27 |  | N |
| 97 | Právo na kolektívne vyjednávanie | Hlava IV, čl. 28 | Druhá hlava, Piaty oddiel, čl. 36, písm. g) | - |
| 98 | Právo na uzatváranie kolektívnych zmlúv na zodpovedajúcich úrovniach | Hlava IV, čl. 28 |  | - |
| 99 | Právo na uskutočnenie kolektívnych akcií na ochranu záujmov vrátane štrajku | Hlava IV, čl. 28 | Druhá hlava, Piaty oddiel, čl. 37, ods. (4) | - |
| 100 | Právo na prístup k bezplatným službám zamestnanosti | Hlava IV, čl. 29 |  | N |
| 101 | Právo na ochranu pred bezdôvodným prepustením | Hlava IV, čl. 30 |  | VN |
| 102 | Právo pracovníka na pracovné podmienky zohľadňujúce jeho zdravie, bezpečnosť a dôstojnosť | Hlava IV, čl. 31, ods. 1 | Druhá hlava, Piaty oddiel, čl. 36, písm. c) | VN |
| 103 | Právo pracovníka na stanovenie najvyššej prípustnej dĺžky pracovného času | Hlava IV, čl. 31, ods. 2 | Druhá hlava, Piaty oddiel, čl. 36, písm. d) | VN |
| 104 | Právo pracovníka na denný a týždenný odpočinok | Hlava IV, čl. 31, ods. 2 | Druhá hlava, Piaty oddiel, čl. 36, písm. e) | VN |
| 105 | Právo pracovníka na platenú dovolenku | Hlava IV, čl. 31, ods. 2 | Druhá hlava, Piaty oddiel, čl. 36, písm. f) | VN |
| 106 | Právo detí na ochranu pred detskou prácou | Hlava IV, čl. 32 |  | - |
| 107 | Právo mladistvých na zabezpečenie pracovných podmienok primeraných ich veku | Hlava IV, čl. 32 | Druhá hlava, Piaty oddiel, čl. 38, ods. (1) | - |
| 108 | Právo mladistvých na ochranu pred ekonomickým vykorisťovaním | Hlava IV, čl. 32 |  | VN |
| 109 | Právo mladistvých na ochranu pred prácou, ktorá by mohla ohroziť ich bezpečnosť, zdravie alebo telesný, psychický, morálny alebo sociálny vývoj, alebo ich vzdelávanie | Hlava IV, čl. 32 | Druhá hlava, Piaty oddiel, čl. 38, ods. (1) | N |
| 110 | Právo rodiny na právnu, ekonomickú a sociálnu ochranu | Hlava IV, čl. 33, ods. 1 | Druhá hlava, Piaty oddiel, čl. 41, ods. (1) | S |
| 111 | Právo na ochranu pred prepustením z práce z dôvodu spojeného s materstvom | Hlava IV, čl. 33, ods. 2 | Druhá hlava, Piaty oddiel, čl. 41, ods. (2) | VN |
| 112 | Právo na platenú materskú dovolenku alebo rodičovskú dovolenku po narodení dieťaťa | Hlava IV, čl. 33, ods. 2 |  | - |
| 113 | Právo na platenú materskú dovolenku alebo rodičovskú dovolenku po osvojení dieťaťa | Hlava IV, čl. 33, ods. 2 |  | - |
| 114 | Právo na dávky sociálneho zabezpečenia a sociálne služby | Hlava IV, čl. 34, ods. 1 |  | N |
| 115 | Právo na dávky sociálneho zabezpečenia a sociálne výhody v súlade s právom Únie a vnútroštátnymi právnymi predpismi a praxou | Hlava IV, čl. 34, ods. 2 | Druhá hlava, Piaty oddiel, čl. 39, ods. (2) | VN |
| 116 | Právo na sociálnu pomoc s cieľom zabezpečiť dôstojnú existenciu všetkých osôb, ktoré nemajú dostatok prostriedkov | Hlava IV, čl. 34, ods. 3 | Druhá hlava, Piaty oddiel, čl. 39, ods. (2) | VN |
| 117 | Právo na pomoc pri bývaní s cieľom zabezpečiť dôstojnú existenciu všetkých osôb, ktoré nemajú dostatok prostriedkov | Hlava IV, čl. 34, ods. 3 |  | VN |
| 118 | Právo na prístup k preventívnej zdravotnej starostlivosti | Hlava IV, čl. 35 | Druhá hlava, Piaty oddiel, čl. 40 | N |
| 119 | Právo využívať lekársku starostlivosť za podmienok ustanovených vnútroštátnymi právnymi predpismi a praxou | Hlava IV, čl. 35 | Druhá hlava, Piaty oddiel, čl. 40 | VN |
| 120 | **Právo na ochranu zdravia** | Hlava IV, čl. 35 | Druhá hlava, Piaty oddiel, čl. 40 | **V** |
| 121 | Právo na prístup k službám všeobecného hospodárskeho záujmu, ktorý je ustanovený vnútroštátnymi právnymi predpismi a praxou | Hlava IV, čl. 36 |  | - |
| 122 | Právo na zabezpečenie ochrany a zlepšovania kvality životného prostredia | Hlava IV, čl. 37 | Druhá hlava, Šiesty oddiel, čl. 44, ods. (1) | N |
| 123 | Právo na uplatňovanie zásady trvalo udržateľného rozvoja v kontexte životného prostredia | Hlava IV, čl. 37 |  | N |
| 124 | Právo voliť vo voľbách do Európskeho parlamentu | Hlava V, čl. 39, ods. 1 |  | VN |
| 125 | Právo byť volený vo voľbách do Európskeho parlamentu | Hlava V, čl. 39, ods. 1 |  | VN |
| 126 | Právo voliť vo voľbách do orgánov samosprávy obcí v členskom štáte | Hlava V, čl. 40 |  | VN |
| 127 | Právo byť volený vo voľbách do orgánov samosprávy obcí v členskom štáte | Hlava V, čl. 40 |  | VN |
| 128 | Právo na nestranné a spravodlivé vybavenie žiadosti v primeranej lehote | Hlava V, čl. 41, ods. 1 |  | - |
| 129 | Právo každého na vypočutie pred prijatím akéhokoľvek individuálneho opatrenia, ktoré by sa ho mohlo nepriaznivo dotýkať | Hlava V, čl. 41, ods. 2, písm. a) |  | VN |
| 130 | Právo každého na prístup k spisu, ktorý sa ho týka, za predpokladu rešpektovania oprávnených záujmov dôvernosti a služobného a obchodného tajomstva | Hlava V, čl. 41, ods. 2, písm. b) |  | - |
| 131 | Právo požadovať od administratívy odôvodnenie ňou vydaných rozhodnutí | Hlava V, čl. 41, ods. 2, písm. c) |  | N |
| 132 | Právo na náhradu škody spôsobenej inštitúciami alebo zamestnancami Únie pri výkone ich funkcií | Hlava V, čl. 41, ods. 3 |  | - |
| 133 | Právo na komunikáciu s inštitúciami Únie v jednom z jazykov úniových zmlúv | Hlava V, čl. 41, ods. 4 |  | - |
| 134 | Právo na prístup k dokumentom inštitúcií, orgánov, úradov a agentúr Únie | Hlava V, čl. 42 |  | VN |
| 135 | Právo oznámiť európskemu ombudsmanovi prípady nesprávneho úradného postupu inštitúcií, orgánov, úradov a agentúr Únie | Hlava V, čl. 43 |  | - |
| 136 | Právo obrátiť sa s petíciou na Európsky parlament | Hlava V, čl. 44 |  | - |
| 137 | Právo na slobodný pohyb na území členských štátov | Hlava V, čl. 45, ods. 1 |  | - |
| 138 | Právo na slobodný pobyt na území členských štátov | Hlava V, čl. 45, ods. 1 |  | - |
| 139 | Právo príslušníkov tretích krajín, ktorí sa oprávnene zdržiavajú na území členského štátu, na priznanie slobody pohybu a pobytu | Hlava V, čl. 45, ods. 2 |  | - |
| 140 | Právo občanov Únie na poskytnutie ochrany diplomatickými orgánmi na území tretích krajín | Hlava V, čl. 46 |  |  |
| 141 | Právo občanov Únie na poskytnutie ochrany konzulárnymi orgánmi na území tretích krajín | Hlava V, čl. 46 |  | - |
| 142 | Právo na účinný prostriedok nápravy pred súdom | Hlava VI, čl. 47 | Druhá hlava, Siedmy oddiel, čl. 46, ods. (1) | VN |
| 143 | Právo na prejednanie záležitosti spravodlivo, verejne a v primeranej lehote pred nezávislým a nestranným súdom | Hlava VI, čl. 47 | Druhá hlava, Siedmy oddiel, čl. 48, ods. (2) | - |
| 144 | Právo na poskytnutie možnosti sa poradiť (v rámci konania vo svojej veci) | Hlava VI, čl. 47 |  | - |
| 145 | Právo na poskytnutie možnosti sa obhajovať (v rámci konania vo svojej veci) | Hlava VI, čl. 47 |  | - |
| 146 | Právo na poskytnutie možnosti nechať sa zastupovať (v rámci konania vo svojej veci) | Hlava VI, čl. 47 |  | - |
| 147 | Právo osôb, ktoré nemajú dostatočné prostriedky, na poskytnutie právnej pomoci, potrebnej na zabezpečenie efektívneho prístupu k spravodlivosti | Hlava VI, čl. 47 | Druhá hlava, Siedmy oddiel, čl. 47, ods. (2) | VN |
| 148 | Právo na rešpektovanie prezumpcie neviny | Hlava VI, čl. 48, ods. 1 | Druhá hlava, Siedmy oddiel, čl. 50, ods. (2) | VN |
| 149 | Právo obvineného na obhajobu | Hlava VI, čl. 48, ods. 2 | Druhá hlava, Siedmy oddiel, čl. 50, ods. (3) | - |
| 150 | Právo na ochranu pre odsúdením za konanie alebo opomenutie, ktoré v čase keď bolo spáchané, nebolo trestné | Hlava VI, čl. 49, ods. 1 |  | - |
| 151 | Právo na ochranu pred ukladaním prísnejšieho trestu než aký bolo možné uložiť v čase jeho spáchania | Hlava VI, čl. 49, ods. 1 | Druhá hlava, Siedmy oddiel, čl. 50, ods. (6) | - |
| 152 | Právo na ochranu pred ukladaním trestov zjavne neprimeraných trestnému činu | Hlava VI, čl. 49, ods. 3 |  | - |
| 153 | Právo nebyť stíhaný v trestnom konaní dvakrát za ten istý trestný čin | Hlava VI, čl. 50 | Druhá hlava, Siedmy oddiel, čl. 50, ods. (5) | - |
| 154 | Právo nebyť potrestaný v trestnom konaní dvakrát za ten istý trestný čin | Hlava VI, čl. 50 | Druhá hlava, Siedmy oddiel, čl. 50, ods. (5) | - |
| 155 | Právo každého slobodne rozhodovať o svojej národnosti |  | Druhá hlava, Prvý oddiel, čl. 12, ods. (3) | - |
| 156 | Právo na ochranu pred akýmkoľvek ovplyvňovaním a nátlakom smerujúcim k odnárodňovaniu |  | Druhá hlava, Prvý oddiel, čl. 12, ods. (3) | VN |
| 157 | Právo na ochranu pred spôsobovaním ujmy na právach pre to, že uplatňuje svoje základné práva a slobody |  | Druhá hlava, Prvý oddiel, čl. 12, ods. (4) | VN |
| 158 | Právo prenatálnej ochrany ľudského života |  | Druhá hlava, Druhý oddiel, čl. 15, ods. (1) | VN |
| 159 | Právo na ochranu života |  | Druhá hlava, Druhý oddiel, čl. 15, ods. (2) | VN |
| 160 | Právo na ochranu pred krutým zaobchádzaním alebo trestom |  | Druhá hlava, Druhý oddiel, čl. 16, ods. (2) | - |
| 161 | Právo na ochranu pred stíhaním alebo pozbavením slobody bez zákonných dôvodov |  | Druhá hlava, Druhý oddiel, čl. 17, ods. (2) | - |
| 162 | Právo na ochranu pred svojvoľným zadržaním alebo zatknutím |  | Druhá hlava, Druhý oddiel, čl. 17, ods. (3) | - |
| 163 | Právo obvineného na ochranu pred skúmaním jeho duševného stavu bez súdneho príkazu |  | Druhá hlava, Druhý oddiel, čl. 17, ods. (7) | - |
| 164 | Právo na zachovanie osobnej cti |  | Druhá hlava, Druhý oddiel, čl. 19, ods. (1) | S |
| 165 | Právo na zachovanie dobrej povesti |  | Druhá hlava, Druhý oddiel, čl. 19, ods. (1) | S |
| 166 | Právo na ochranu mena |  | Druhá hlava, Druhý oddiel, čl. 19, ods. (1) | S |
| 167 | Právo na slobodný pohyb a pobyt |  | Druhá hlava, Druhý oddiel, čl. 23, ods. (1) | - |
| 168 | Právo slobodne opustiť územie Slovenskej republiky |  | Druhá hlava, Druhý oddiel, čl. 23, ods. (2) | - |
| 169 | Právo občana na slobodný vstup na územie Slovenskej republiky |  | Druhá hlava, Druhý oddiel, čl. 23, ods. (4) | - |
| 170 | Právo cudzincov na ochranu pred svojvoľným vyhostením |  | Druhá hlava, Druhý oddiel, čl. 23, ods. (5) | - |
| 171 | Právo byť bez náboženského vyznania |  | Druhá hlava, Druhý oddiel, čl. 24, ods. (1) | VN |
| 172 | Právo cirkví a náboženských spoločností spravovať si svoje záležitosti samostatne |  | Druhá hlava, Druhý oddiel, čl. 24, ods. (3) | - |
| 173 | Právo občanov slobodne sa rozhodovať o ich účasti na obrane Slovenskej republiky |  | Druhá hlava, Druhý oddiel, čl. 25, ods. (1) | - |
| 174 | Právo na ochranu pred núteným výkonom vojenskej služby |  | Druhá hlava, Druhý oddiel, čl. 25, ods. (2) | - |
| 175 | Právo na ochranu pred cenzúrou |  | Druhá hlava, Tretí oddiel, čl. 26, ods. (3) | S |
| 176 | Právo na poskytovanie informácií o činnosti orgánov verejnej moci v štátnom jazyku a primeraným spôsobom |  | Druhá hlava, Tretí oddiel, čl. 26, ods. (5) | - |
| 177 | Právo každého obracať sa vo veciach verejného alebo iného spoločného záujmu na štátne orgány a orgány územnej samosprávy |  | Druhá hlava, Tretí oddiel, čl. 27, ods. (1) | - |
| 178 | Právo každého prihlásiť sa ku ktorejkoľvek národnostnej menšine alebo etnickej skupine |  | Druhá hlava, Štvrtý oddiel, čl. 33 | - |
| 179 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám na všestranný rozvoj |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (1) | - |
| 180 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám rozvíjať vlastnú kultúru |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (1) | - |
| 181 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám združovať sa v národnostných združeniach |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (1) | - |
| 182 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám zakladať a udržiavať vzdelávacie a kultúrne inštitúcie |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (1) | - |
| 183 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám na osvojenie si štátneho jazyka |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (2) | - |
| 184 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám na vzdelanie v ich jazyku |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (2) | - |
| 185 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám používať ich jazyk v úradnom styku |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (2) | - |
| 186 | Právo občanov patriacich k národnostným menšinám alebo etnickým skupinám zúčastňovať sa na riešení vecí týkajúcich sa národnostných menšín a etnických skupín |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (2) | - |
| 187 | Právo na ochranu pred ohrozovaním zvrchovanosti a územnej celistvosti Slovenskej republiky v súvislosti s výkonom práv národnostných menšín a etnických skupín |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (3) | - |
| 188 | Právo na ochranu ostatného obyvateľstva SR pred diskrimináciou pri výkone práv národnostných menšín a etnických skupín |  | Druhá hlava, Štvrtý oddiel, čl. 34, ods. (3) | - |
| 189 | Právo uskutočňovať inú zárobkovú činnosť |  | Druhá hlava, Piaty oddiel, čl. 35, ods. (1) | VN |
| 190 | Právo občanov, ktorí nie z vlastnej viny nemôžu vykonávať právo na prácu, na primerané hmotné zabezpečenie |  | Druhá hlava, Piaty oddiel, čl. 35, ods. (3) | - |
| 191 | Právo zamestnancov na odmenu za vykonanú prácu |  | Druhá hlava, Piaty oddiel, čl. 36, písm. a) | VN |
| 192 | Právo zamestnancov na ochranu proti svojvoľnému prepúšťaniu zo zamestnania a diskriminácii v zamestnaní |  | Druhá hlava, Piaty oddiel, čl. 36, písm. b) | VN |
| 193 | Právo na ochranu pred obmedzovaním počtu odborových organizácií, ako aj zvýhodňovaním niektorých z nich v podniku alebo v odvetví |  | Druhá hlava, Piaty oddiel, čl. 37, ods. (2) | - |
| 194 | Právo žien, mladistvých a osôb zdravotne postihnutých na osobitné pracovné podmienky |  | Druhá hlava, Piaty oddiel, čl. 38, ods. (1) | - |
| 195 | Právo mladistvých a osôb zdravotne postihnutých na osobitnú ochranu v pracovných vzťahoch |  | Druhá hlava, Piaty oddiel, čl. 38, ods. (2) | - |
| 196 | Právo mladistvých a osôb zdravotne postihnutých na pomoc pri príprave na povolanie |  | Druhá hlava, Piaty oddiel, čl. 38, ods. (2) | - |
| 197 | Právo na primerané hmotné zabezpečenie v starobe |  | Druhá hlava, Piaty oddiel, čl. 39, ods. (1) | N |
| 198 | Právo na primerané hmotné zabezpečenie pri nespôsobilosti na prácu |  | Druhá hlava, Piaty oddiel, čl. 39, ods. (1) | N |
| 199 | Právo na primerané hmotné zabezpečenie pri strate živiteľa |  | Druhá hlava, Piaty oddiel, čl. 39, ods. (1) | - |
| 200 | Právo občanov na bezplatnú zdravotnú starostlivosť za podmienok, ktoré ustanoví zákon |  | Druhá hlava, Piaty oddiel, čl. 40 | N |
| 201 | Právo občanov na bezplatné zdravotnícke pomôcky, za podmienok, ktoré ustanoví zákon |  | Druhá hlava, Piaty oddiel, čl. 40 | VN |
| 202 | Právo mimomanželských detí mať rovnaké práva ako deti narodené v manželstve |  | Druhá hlava, Piaty oddiel, čl. 41, ods. (3) | - |
| 203 | Právo rodičov, ktorí sa starajú o deti, na pomoc od štátu |  | Druhá hlava, Piaty oddiel, čl. 41, ods. (5) | VN |
| 204 | Právo zriaďovať iné školy ako štátne a vyučovať v nich |  | Druhá hlava, Piaty oddiel, čl. 42, ods. (3) | - |
| 205 | Právo občanov na pomoc štátu pri štúdiu |  | Druhá hlava, Piaty oddiel, čl. 42, ods. (4) | VN |
| 206 | Právo na prístup ku kultúrnemu bohatstvu |  | Druhá hlava, Piaty oddiel, čl. 43, ods. (2) | VN |
| 207 | Právo na ochranu pred ohrozovaním alebo poškodzovaním životné prostredia, prírodných zdrojov a kultúrnych pamiatok |  | Druhá hlava, Šiesty oddiel, čl. 44, ods. (3) | - |
| 208 | Právo na informácie o stave životného prostredia |  | Druhá hlava, Šiesty oddiel, čl. 45 | VN |
| 209 | Právo domáhať sa svojho práva aj na inom orgáne Slovenskej republiky |  | Druhá hlava, Siedmy oddiel, čl. 46, ods. (1) | - |
| 210 | Právo obrátiť sa na súd z dôvodu preskúmania zákonnosti rozhodnutia orgánu verejnej správy |  | Druhá hlava, Siedmy oddiel, čl. 46, ods. (2) | - |
| 211 | Právo na ochranu pred vylúčením preskúmania rozhodnutia týkajúceho sa základných práv a slobôd z právomoci súdov |  | Druhá hlava, Siedmy oddiel, čl. 46, ods. (2) | - |
| 212 | Právo na náhradu škody spôsobenej nezákonným rozhodnutím súdu, iného štátneho orgánu či orgánu verejnej správy |  | Druhá hlava, Siedmy oddiel, čl. 46, ods. (3) | - |
| 213 | Právo na náhradu škody spôsobenej nesprávnym úradným postupom |  | Druhá hlava, Siedmy oddiel, čl. 46, ods. (3) | - |
| 214 | Právo odoprieť výpoveď |  | Druhá hlava, Siedmy oddiel, čl. 47, ods. (1) | - |
| 215 | Právo na tlmočníka |  | Druhá hlava, Siedmy oddiel, čl. 47, ods. (4) | - |
| 216 | Právo na zákonného sudcu |  | Druhá hlava, Siedmy oddiel, čl. 48, ods. (1) | - |
| 217 | Právo byť prítomný na prerokovaní svojej veci |  | Druhá hlava, Siedmy oddiel, čl. 48, ods. (2) | - |
| 218 | Právo vyjadriť sa vo svojej veci ku všetkým vykonávaným dôkazom |  | Druhá hlava, Siedmy oddiel, čl. 48, ods. (2) | - |

## Monetarizácia zdravotných dopadov

Pre posúdenie reálnej miery zdravotných dopadov v dôsledku negatívneho vplyvu digitálnych technológií je vhodné ich previesť na financie v rámci monetarizačného modelu.

Rámec pre monetarizáciu poskytuje metodika WHO pre stratené roky života - DALYS (Disability-Adjusted Life Years)

**Definícia DALYs podľa WHO**

*One DALY represents the loss of the equivalent of one year of full health. DALYs for a disease or health condition are the sum of the years of life lost to due to premature mortality (YLLs) and the years lived with a disability (YLDs) due to prevalent cases of the disease or health condition in a population.[[111]](#footnote-111) [[112]](#footnote-112)*

**Jeden DALY reprezentuje stratu ekvivalentnú jednému roku života plného zdravia.**

DALYs sú súčtom stratených rokov života v dôsledku predčasného úmrtia (YLL) a rokov života s disabilitou (YLD) spôsobenou chorobou alebo zdravotnými podmienkami v populácii.

Suma všetkých DALYs v populácii môže byť chápaná ako miera medzery medzi aktuálnym zdravotným stavom populácie a ideálnou situáciou, keď celá populácie žije v stave bez chorôb a postihnutí.[[113]](#footnote-113)

***Výpočet DALYs***

Ako bolo povedané, hodnota DALYs je tvorená dvoma komponentami - YLL a YLD

YLL - stratené roky života kvôli predčasnému úmrtiu (napr. labilné dieťa spácha samovraždu)

YLD - stratené kvalitné roky života kvôli dopadom narušeného zdravotného stavu (obézne dieťa dostane diabetes a má ho do konca života)

koeficient pre YLD je od 0 po 1, podľa závažnosti zdrav. dopadu (disease burden). 0 znamená úplné zdravie, 1 znamená smrť. [[114]](#footnote-114)

***Výpočet YLL***

YLL = N x L

N - počet úmrtí v danej vekovej kategórii

L - štandardná doba dožitia v danej vekovej kategórii.

Príklad:

*Máme 20 predčasných úmrtí dievčat s očakávanou dobou dožitia 70 rokov.*

*YLL je 70 \* 20 = 1400 DALYs*

***Výpočet YLD***

YLD = I x DW x L

I - počet zdravotných prípadov (incident cases)

DW - váha zdravotného narušenia (disability weight)

L - priemerná doba trvania zdravotného narušenia

*Príklad:*

*V SR je cca. 360.000 diabetikov[[115]](#footnote-115). Priemerná váha DW pre diabetes je 0,12[[116]](#footnote-116)*

*Berieme dobu 1 roka.*

*YLD = 360000 \*0,12 \* 1 = 43.200 DALYs / rok*

Čiže v dôsledku len tejto jednej diagnózy – diabetu, ktorá je výrazne ovplyvniteľná podmienená nezdravým životným štýlom stráca sa na Slovensku viac než 40.000 človeko-rokov kvalitného života každý rok! TCO (náklady na zdravotnú starostlivosť) u na diabetika môže presiahnuť 5.000 € [[117]](#footnote-117) každý rok. Za 40 rokov je to 200.000 €.

**Monetarizácia DALYs**

Kľúčom k monetarizácii je finančné ohodnotenie jedného človeko-roka života (DALY, QALY – Quality Adjusted Life Year [[118]](#footnote-118) ako zníženie DALY).

Takéto ohodnotenie je štandardne využívané v rámci farmako-ekonomických analýz. Odporúčanie WHO je do trojnásobku HDP na osobu [[119]](#footnote-119).

V súlade s § 7 odsek 3 zákona 363/2011 Z.z. o rozsahu a podmienkach úhrady liekov, zdravotníckych pomôcok a dietetických potravín na základe verejného zdravotného poistenia a o zmene a doplnení niektorých zákonov v znení platnom od 1.1.2025:

„Prahová hodnota posudzovaného lieku za jeden získaný rok života štandardizovanej kvality je príslušný násobok hrubého domáceho produktu Slovenskej republiky, ktorý nesmie byť vyšší ako 3; ak predmetom žiadosti je liek na ojedinelé ochorenie alebo liek na inovatívnu liečbu, príslušný násobok hrubého domáceho produktu Slovenskej republiky nesmie byť vyšší ako 10. Podrobnosti výpočtu násobku podľa prvej vety ustanoví všeobecne záväzný právny predpis, ktorý vydá ministerstvo.“

Podrobnosti sú vo vyhláške č. 298/2022 Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovujú podrobnosti výpočtu príslušného násobku hrubého domáceho produktu pre stanovenie prahovej hodnoty posudzovaného lieku.

Referenčná hodnota pre 1 QALY / DALY je pre účely nášho dokumentu cca.40.000 €.

Analýza dopadov narušenia duševného zdravia z hľadiska verejných financií je analyzovaná v dokumente Útvaru hodnoty za peniaze MF SR „Duševné zdravie a verejné financie“ [[120]](#footnote-120)

## Populačná dynamika – podklady

V tejto kapitole sú uvedené podklady pre riziko nízkej pôrodnosti, na ktoré má vplyv aj digitálny obsah v kybernetickom priestore a čas v ňom strávený (viď. Kap. 4.6.10)

Počet obyvateľov Slovenska klesá - úmrtnosť sa stabilizovala, prudký prepad pôrodnosti pokračuje.

Obrázok, na ktorom je text, vývoj, snímka obrazovky, rad

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.

V Slovenskej republike na konci roka 2024 žilo celkovo 5 419 451 obyvateľov.

„Celkovo Slovensko za posledných 5 rokov stratilo prirodzeným pohybom takmer 40-tisíc obyvateľov. Po období vysokej úmrtnosti na Slovensku v rokoch 2020 až 2022, ovplyvnenom pandémiou, sa posledné tri roky závažne znižovala pôrodnosť,“ uviedla Zuzana Podmanická, riaditeľka odboru štatistiky obyvateľstva ŠÚ SR.

**Pracujúci v zahraničí**

Slovensko má v pomere k svojej populácii najvyššie záporné migračné saldo v Európskej únii. V praxi to znamená, že za prácou do zahraničia pravidelne dochádza takmer 5 % všetkých zamestnaných ľudí na Slovensku, čo v minulom roku predstavovalo 116-tisíc Slovákov. [[121]](#footnote-121)

**Štúdium v zahraničí**

Až 42 percent respondentov chce po prvom stupni štúdia na slovenskej vysokej škole doštudovať v zahraničí. Vyplýva to z kvantitatívneho prieskumu, ktorý realizovalo občianske združenie Therapolis v spolupráci s agentúrou Focus a na tlačovej konferencii o výsledkoch prieskumu informovala zakladateľka združenia Renáta Hall.[[122]](#footnote-122)

Každý piaty slovenský vysokoškolák študuje v zahraničí. Približne 70 percent študentov, ktorí odchádzajú do zahraničia, študujú v Česku. Vlani tam navštevovalo vysoké školy takmer 21-tisíc Slovákov. Informoval o tom Inštitút vzdelávacej politiky.

V zahraničí študuje okolo 32-tisíc študentov. [[123]](#footnote-123) Na Fakulte informačných technológií VUT v Brne študuje viac slovenských ako českých študentov. Príchod zahraničných študentov má tendenciu vytvárať klastre – ak škola prijme slovenských študentov a sú dobré odozvy, tak rastie podiel budúcich slovenských študentov.

**Náklady na dieťa**

Celkové náklady štátu a rodičov na dieťa do 25 rokov života sú 250.000+ € (cca. 10.000 € na rok). Model nákladov na dieťa je výstupom v rámci projektu Lepšej regulácie MH SR v rokoch 2018 – 2019.

Čiže odchodom mladého človeka zo Slovenskej republiky je táto suma z pohľadu štátu neefektívne využitá. Ak by sa teda 50 % z 32.000 študentov študujúcich zahraničí nevrátila, ide o neefektívne vynaložené prostriedky vo výške: 16.000 \* 180.000 (18 rokov v SR) = 2,88 mld. €.

K tejto sume je potrebné prirátať výpadku na daniach, ktoré by daný mladý človek odvádzal a výpadok vo výchove nasledujúcej generácie (ak niekto žije trvalo mimo, aj jeho deti budú žiť mimo SR.

1. <https://www.minedu.sk/program-informatizacie-skolstva-do-roku-2030/> [↑](#footnote-ref-1)
2. <https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2025.1477914/full> [↑](#footnote-ref-2)
3. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/8/vyskumna_sprava_2023-1.pdf> <https://www.ivo.sk/buxus/docs//Digitalna_gramotnost/Kybersikana_na_strednych_skolach.pdf> [↑](#footnote-ref-3)
4. <https://www.startitup.sk/alarmujuce-cisla-prieskum-odhalil-kolko-hodin-travia-mladi-ludia-na-telefone-denne-vysledky-zarazaju/> [↑](#footnote-ref-4)
5. <https://vedanadosah.cvtisr.sk/zdravie/medicina/obezita-na-slovensku-raketovo-stupa-deti-poznaci-na-cely-zivot-ako-ovladnut-svoje-telo/> [↑](#footnote-ref-5)
6. <https://zdravotnickydennik.sk/2024/11/pocet-diabetikov-na-slovensku-stale-rastie-zdravotne-naklady-na-pacientov-presahuju-800-milionov-eur-rocne/> [↑](#footnote-ref-6)
7. <https://www.unilabs.sk/clanky-invitro/diabetes-mellitus-v-detstve-v-mladosti-aktualna-situacia-na-slovensku> [↑](#footnote-ref-7)
8. https://agenturascio.sk/press-releases/34-obcanov-slovenska-ma-pochybnost-ze-zem-je-plocha/ [↑](#footnote-ref-8)
9. <https://www.ivo.sk/8978/sk/aktuality/kybersikana-na-strednych-skolach-a-iniciativa-slovak-telekom-absolventi-sikany> [↑](#footnote-ref-9)
10. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/8/vyskumna_sprava_2023-1.pdf> [↑](#footnote-ref-10)
11. <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/#paragraf-3> [↑](#footnote-ref-11)
12. <https://kyberportal.slovensko.sk/documents/84/1-Uvod-do-KIB_slovnik.pdf> [↑](#footnote-ref-12)
13. https://www.statpedu.sk/sk/svp/statny-vzdelavaci-program/vychova-vzdelavanie-ziakov-so-svvp/ziak-so-sociane-znevyhodneneho-prostredia/ [↑](#footnote-ref-13)
14. <https://ec.europa.eu/eurostat/databrowser/view/ILC_LVPS09/default/table?lang=en> <https://www.imeteo.sk/spravy/blackout-v-spanielsku-najvaznejsia-nehoda-za-20-rokov-v-europe-kolaps-si-vyziadal-az-5-obeti-2> <https://www.energie-portal.sk/dokument/vypadok-prudu-blackout-spanielsko-111585.aspx> [↑](#footnote-ref-14)
15. https://www.startitup.sk/vacsina-slovakov-by-nebola-ochotna-bojovat-za-svoju-krajinu-prieskum/ [↑](#footnote-ref-15)
16. <https://www.energie-portal.sk/Dokument/blackout-vypadok-prudu-spanielsko-priciny-dovody-111607.aspx> [↑](#footnote-ref-16)
17. <https://www.nbu.gov.sk/data/att/409.pdf> [↑](#footnote-ref-17)
18. <https://kyberportal.slovensko.sk/documents/155/Metodika_AR_pre_ISVS.pdf> [↑](#footnote-ref-18)
19. <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/179/#prilohy> Príloha č.1 [↑](#footnote-ref-19)
20. <https://tvv-journal.upol.cz/pdfs/tvv/2016/01/36.pdf> [↑](#footnote-ref-20)
21. <https://sk.wikipedia.org/wiki/V%C3%BDvojov%C3%A9_prostredie> [↑](#footnote-ref-21)
22. <https://www.minedu.sk/digitalne-vybavenie-pre-kazdu-skolu/> [↑](#footnote-ref-22)
23. <https://nivam.sk/zacala-sa-najvacsia-digitalizacia-skol-v-historii-slovenska/> [↑](#footnote-ref-23)
24. <https://casopisvnitrnilekarstvi.cz/pdfs/vnl/2007/06/08.pdf> <https://www.zriedkavechoroby.sk/zakladny-prehlad/co-su-zriedkave-choroby/> [↑](#footnote-ref-24)
25. <https://hub.geneplanet.com/sk/controlling-genes-the-science-of-epigenetics/> [↑](#footnote-ref-25)
26. <https://www.genome.gov/genetics-glossary/Phenotype> [↑](#footnote-ref-26)
27. <https://emefka.sk/patris-do-generacie-snehovych-vlociek-takto-vznikol-pojem-ktory-ta-pravdepodobne-urazi/> [↑](#footnote-ref-27)
28. <https://www.minedu.sk/data/att/706/32294.e4e1ad.pdf> [↑](#footnote-ref-28)
29. <https://www.minedu.sk/digiedu/> [↑](#footnote-ref-29)
30. <https://www.minedu.sk/data/att/9e4/32436.a03179.pdf> [↑](#footnote-ref-30)
31. <https://www.minedu.sk/data/files/6948_priloha_2_rup.pdf> [↑](#footnote-ref-31)
32. V zmysle metodiky NBÚ: <https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf> a metodiky MIRRI: <https://www.mirri.gov.sk/wp-content/uploads/2023/01/KB-K2_3-10-Metodika-na-v%C3%BDkon-anal%C3%BDzy-riz%C3%ADk-v1.1.pdf> [↑](#footnote-ref-32)
33. <https://www.cvtisr.sk/cvti-sr-vedecka-kniznica/informacie-o-skolstve/statistiky/statisticka-rocenka-publikacia/statisticka-rocenka-zakladne-skoly.html?page_id=9601> [↑](#footnote-ref-33)
34. <https://www.whitehouse.gov/wp-content/uploads/2025/05/WH-The-MAHA-Report-Assessment.pdf> [↑](#footnote-ref-34)
35. <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0438_SK.html> [↑](#footnote-ref-35)
36. <https://mirri.gov.sk/wp-content/uploads/2023/01/NSDZ-a-AP.pdf> [↑](#footnote-ref-36)
37. <https://mirri.gov.sk/wp-content/uploads/2023/01/NSDZ-a-AP.pdf> s.45 [↑](#footnote-ref-37)
38. <https://www.employment.gov.sk/sk/rodina-socialna-pomoc/tazke-zdravotne-postihnutie/kontaktne-miesto-prava-osob-so-zdravotnym-postihnutim/zdravotne-postihnutie.html> [↑](#footnote-ref-38)
39. <https://blindrevue.sk/pouzivame-asistencne-technologie-v-pocitaci-a-mobilnom-telefone-cast-5/> [↑](#footnote-ref-39)
40. <https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer> [↑](#footnote-ref-40)
41. <https://www.rnz.co.nz/news/what-you-need-to-know/559763/youtube-is-exempt-from-australia-s-social-media-ban-why> [↑](#footnote-ref-41)
42. <https://www.shadac.org/opioid-epidemic-united-states#:~:text=Looking%20at%20all%20types%20of,rapid%20increases%20over%20the%20past> [↑](#footnote-ref-42)
43. <https://medium.com/asecuritysite-when-bob-met-alice/as-an-ai-and-predatory-journals-the-sad-state-of-some-academic-publishing-306e7e362e85> <https://www.digital-science.com/tldr/article/the-opposite-of-trust/> [↑](#footnote-ref-43)
44. <https://philosophersmag.com/the-fact-opinion-distinction/> <https://edu.gcfglobal.org/en/digital-media-literacy/the-blur-between-facts-and-opinions-in-the-media/1/> [↑](#footnote-ref-44)
45. <https://www.britannica.com/topic/flat-Earth> [↑](#footnote-ref-45)
46. <https://bratislavskykraj.sk/laska-v-digitalnom-svete-ako-sa-bezpecne-zoznamovat-online/> <https://www.digitalnypriestor.sk/su-online-zoznamky-bezpecne/> <https://www.gdpr.sk/je-online-zoznamka-bezpecna-rizika-vas-mozu-zaskocit/> [↑](#footnote-ref-46)
47. <https://akcnezeny.sk/influencer-a-mizogyn-andrew-tate-pre-ktoreho-su-zeny-majetkom-muzov-dostal-stopku/> [↑](#footnote-ref-47)
48. <https://www.europol.europa.eu/publications-events/publications/incel-online-communities-violence-and-construction-of-collective-victimhood> [↑](#footnote-ref-48)
49. <https://en.wikipedia.org/wiki/Hikikomori> [↑](#footnote-ref-49)
50. <https://www.research.ed.ac.uk/en/publications/the-proliferation-of-human-rights-between-devotion-and-calculatio> <https://www.foreignaffairs.com/europe/danger-human-rights-proliferation> [↑](#footnote-ref-50)
51. <https://taskandpurpose.com/news/army-hawaii-dog-bondage-mask/> [↑](#footnote-ref-51)
52. <https://blosc.wordpress.com/2021/11/10/todays-youth-are-more-concerned-with-their-rights-than-with-their-responsibilities/> [↑](#footnote-ref-52)
53. <https://www.the-scientist.com/universe-25-experiment-69941> [↑](#footnote-ref-53)
54. <https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesa_pd_2025_wfr_2024_final.pdf> [↑](#footnote-ref-54)
55. <https://data.worldbank.org/indicator/SP.DYN.TFRT.IN> [↑](#footnote-ref-55)
56. <https://statdat.statistics.sk/cognosext/cgi-bin/cognos.cgi?b_action=cognosViewer&ui.action=run&ui.object=storeID%28%22i65ABFA022832487184CA59323F05AF97%22%29&ui.name=Preh%C4%BEad%20stavu%20a%20pohybu%20obyvate%C4%BEstva%20-%20SR%2C%20oblasti%2C%20kraje%2C%20okresy%2C%20mesto%2C%20vidiek%20%5Bom7011rr%5D&run.outputFormat&run.prompt=true&cv.header=false&ui.backURL=%2Fcognosext%2Fcps4%2Fportlets%2Fcommon%2Fclose.html&run.outputLocale=sk> [↑](#footnote-ref-56)
57. <https://www.dipf.de/en/dipf-news/press-releases/social-media-how-upward-comparisons-and-well-being-are-related-in-children-and-adolescents> <https://www.nature.com/articles/s44271-023-00013-0> [↑](#footnote-ref-57)
58. <https://www.highervisibility.com/ppc/learn/gen-z-and-the-rise-of-influencer-culture/> [↑](#footnote-ref-58)
59. <https://www.consilium.europa.eu/sk/policies/benefits-and-risks-of-ai/> [↑](#footnote-ref-59)
60. <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689> [↑](#footnote-ref-60)
61. <https://www.consilium.europa.eu/sk/policies/artificial-intelligence/> [↑](#footnote-ref-61)
62. <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689> [↑](#footnote-ref-62)
63. <https://www.rosemarydoll.com/?gad_source=1&gad_campaignid=16547544237&gbraid=0AAAAACQ3Yvh-_oUzwBHvHlctQ9xE_LuXs&gclid=Cj0KCQjwoZbBBhDCARIsAOqMEZWyPODO8ggStsECqKMTggOuR89ox3sQBS3KNdvuiUta3vAt2BZ99EEaAnmwEALw_wcB> [↑](#footnote-ref-63)
64. <https://www.tiktok.com/discover/digital-influencers> [↑](#footnote-ref-64)
65. <https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/> <https://en.wikipedia.org/wiki/Lethal_autonomous_weapon> [↑](#footnote-ref-65)
66. <https://neuralink.com/> <https://neuralink.com/patient-registry/> [↑](#footnote-ref-66)
67. <https://www.darpa.mil/research/programs/intelligent-neural-interfaces> <https://www.darpa.mil/research/programs/next-generation-nonsurgical-neurotechnology> [↑](#footnote-ref-67)
68. <https://sk.wikipedia.org/wiki/Virtu%C3%A1lna_realita> [↑](#footnote-ref-68)
69. <https://sk.wikipedia.org/wiki/Roz%C5%A1%C3%ADren%C3%A1_realita> [↑](#footnote-ref-69)
70. <https://www.adobe.com/sk/products/substance3d/discover/what-is-augmented-reality.html> [↑](#footnote-ref-70)
71. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/8/vyskumna_sprava_2023-1.pdf> [↑](#footnote-ref-71)
72. <https://akcnezeny.sk/influencer-a-mizogyn-andrew-tate-pre-ktoreho-su-zeny-majetkom-muzov-dostal-stopku/> [↑](#footnote-ref-72)
73. <https://www.theguardian.com/uk-news/2019/apr/12/upskirting-law-comes-into-force-england-and-wales-cases-rise> [↑](#footnote-ref-73)
74. <https://clpr.org.in/blog/understanding-virtual-digital-rape-navigating-consent-and-accountability-in-the-digital-age/> <https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta> [↑](#footnote-ref-74)
75. <https://en.wikipedia.org/wiki/Incel> [↑](#footnote-ref-75)
76. <https://www.sciencedaily.com/releases/2025/06/250609054355.htm> [↑](#footnote-ref-76)
77. <https://www.spectator.co.uk/article/why-children-shouldnt-go-vegan/> [↑](#footnote-ref-77)
78. <https://www.theguardian.com/technology/2025/jun/17/dna-testing-firm-23andme-fined-23m-by-uk-regulator-for-2023-data-hack> [↑](#footnote-ref-78)
79. <https://mv.gov.cz/soubor/sekty-clanek-pdf.aspx> [↑](#footnote-ref-79)
80. <https://www.aol.com/news/parental-rights-watchdog-exposes-left-171155893.html> [↑](#footnote-ref-80)
81. <https://cs.wikipedia.org/wiki/Guru_J%C3%A1ra> [↑](#footnote-ref-81)
82. <https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder> <https://at-konference.cz/wp-content/uploads/2019/07/patarak-m.-porucha-v-dosledku-hrania-gaming-disorder-podla-icd-11.pdf> [↑](#footnote-ref-82)
83. <https://touchit.sk/v-akom-veku-kupujeme-detom-do-skoly-smartfon/438012> [↑](#footnote-ref-83)
84. <https://www.statista.com/statistics/477088/children-and-teens-smartphone-usage-by-age-germany/> [↑](#footnote-ref-84)
85. <https://www.bbc.com/future/article/20220914-whats-the-right-age-to-get-a-smartphone> [↑](#footnote-ref-85)
86. <https://ai-2027.com/> [↑](#footnote-ref-86)
87. <https://www.nczisk.sk/AKTUALITY/Pages/NCZI-Na-Slovensku-je-sledovanych-349-595-pacientov-s-cukrovkou.aspx#:~:text=Po%C4%8Det%20pr%C3%ADpadov%2C%20ako%20aj%20v%C3%BDskyt,o%20takmer%20230%2Dtis%C3%ADc%20os%C3%B4b>. [↑](#footnote-ref-87)
88. <https://zdravotnickydennik.sk/2024/11/pocet-diabetikov-na-slovensku-stale-rastie-zdravotne-naklady-na-pacientov-presahuju-800-milionov-eur-rocne/#:~:text=Zdravotn%C3%A9%20n%C3%A1klady%20na%20pacientov%20presahuj%C3%BA%20800%20mili%C3%B3nov%20eur%20ro%C4%8Dne,-15.&text=Na%20Slovensku%20bolo%20ku%20koncu,evidovali%20necel%C3%BDch%20272%2Dtis%C3%ADc%20pacientov>. [↑](#footnote-ref-88)
89. <https://www.trend.sk/trend-archiv/preco-ludstvo-hlupne-kriticke-myslenie-mizne-dovodom-su-socialne-siete?itm_brand=trend&itm_template=other&itm_modul=articles-print&itm_position=11&utm_source=ecomail&utm_campaign=tyzdenny_newsletter_trend_27042025&utm_medium=email&utm_term=47070&ecmid=10492> [↑](#footnote-ref-89)
90. <https://lrv.rokovania.sk/data/att/163502_subor.docx> [↑](#footnote-ref-90)
91. <https://www.verywellmind.com/what-is-maslows-hierarchy-of-needs-4136760> <https://sk.wikipedia.org/wiki/Potreba_(ekon%C3%B3mia)> [↑](#footnote-ref-91)
92. [↑](#footnote-ref-92)
93. <https://www.minedu.sk/data/files/11043_strategia-slovenskej-republiky-pre-mladez-na-roky-2021-2028.pdf> [↑](#footnote-ref-93)
94. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf> [↑](#footnote-ref-94)
95. <https://nks.gov.sk/wp-content/uploads/2025/SM/akn-pln-2024-1.pdf?csrt=543362095649314708> [↑](#footnote-ref-95)
96. <https://vudpap.sk/> <https://vudpap.sk/wp-content/uploads/2023/02/Desatoro-rad-pre-rodicov-1.pdf> <https://vudpap.sk/wp-content/uploads/2025/02/5-C-metodicky-material.pdf> [↑](#footnote-ref-96)
97. <https://www.minedu.sk/42146-sk/digitalny-wellbeing/> [↑](#footnote-ref-97)
98. <https://kyberportal.slovensko.sk/znalostna-baza/legislativa-nbu/> [↑](#footnote-ref-98)
99. <https://kyberportal.slovensko.sk/znalostna-baza/legislativa-narodneho-bezpecnostneho-uradu/> [↑](#footnote-ref-99)
100. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf> [↑](#footnote-ref-100)
101. <https://www.minedu.sk/data/files/11043_strategia-slovenskej-republiky-pre-mladez-na-roky-2021-2028.pdf> [↑](#footnote-ref-101)
102. <https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf> [↑](#footnote-ref-102)
103. <https://nks.gov.sk/wp-content/uploads/2025/SM/akn-pln-2024-1.pdf?csrt=543362095649314708> [↑](#footnote-ref-103)
104. <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2005/300/20231020#predpis.cast-prva.hlava-stvrta> [↑](#footnote-ref-104)
105. <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689> [↑](#footnote-ref-105)
106. <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689> [↑](#footnote-ref-106)
107. <https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf> [↑](#footnote-ref-107)
108. <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appId=PPGMS>

     [↑](#footnote-ref-108)
109. <https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf> [↑](#footnote-ref-109)
110. https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:12016P/TXT [↑](#footnote-ref-110)
111. <https://www.who.int/data/gho/indicator-metadata-registry/imr-details/158> [↑](#footnote-ref-111)
112. <https://www.who.int/quantifying_ehimpacts/publications/en/9241546204chap3.pdf> [↑](#footnote-ref-112)
113. <https://ec.europa.eu/health/sites/health/files/state/docs/chp_sk_slovak.pdf> [↑](#footnote-ref-113)
114. <https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(23)01301-6/fulltext> [↑](#footnote-ref-114)
115. <http://www.nczisk.sk/Statisticke_vystupy/Tematicke_statisticke_vystupy/Diabetologia/Pages/default.aspx> [↑](#footnote-ref-115)
116. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4192997/> [↑](#footnote-ref-116)
117. <https://aifp.sk/sk/media-a-verejnost/19/naklady-a-manazment-liecby-diabetes-mellitus/> [↑](#footnote-ref-117)
118. <https://en.wikipedia.org/wiki/Quality-adjusted_life_year> [↑](#footnote-ref-118)
119. <https://www.who.int/bulletin/volumes/93/2/14-138206/en/> [↑](#footnote-ref-119)
120. <https://www.mfsr.sk/files/archiv/9/dusevne_zdravie_verejne_financie_uhp.pdf> [↑](#footnote-ref-120)
121. <https://www.finreport.sk/ekonomika/slovensko-ma-najviac-pendlerov-v-prepocte-na-pracujucich-obyvatelov-v-celej-eu/> [↑](#footnote-ref-121)
122. <https://www.trend.sk/spravy/vyse-tretina-studentov-chce-dostudovat-vs-zahranici-prec-ich-zenie-aj-fungovanie-statu> [↑](#footnote-ref-122)
123. <https://domov.sme.sk/c/23181396/kazdy-piaty-slovensky-vysokoskolak-studuje-v-zahranici-najviac-ich-je-v-cesku.html> [↑](#footnote-ref-123)