

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti



PŘEDSTAVENÍ KONCEPCE VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Určeno

Poslanecké sněmovně Parlamentu České republiky

Výboru pro vědu, vzdělávání, kulturu, mládež a tělovýchovu

Informační a komunikační technologie (dále jen „ICT“ nebo „digitální technologie“) představují neodmyslitelnou součást každodenního života. S expanzí ICT do všech oborů lidské činnosti narůstá potřeba zajištění jejich bezpečného využívání. **Kybernetické hrozby** lze přitom významně minimalizovat bezpečnostním vzděláváním zohledňujícím dynamický vývoj ICT. Národní bezpečnostní úřad (dále jen „NBÚ“), jakožto gestor kybernetické bezpečnosti v ČR, v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 - 2020 a v jejím Akčním plánu identifikuje potřebu **modernizace kybernetické osvěty a vzdělávání**.

Kybernetických hrozeb neustále přibývá a nejčastěji vznikají z neznalosti nebo nedodržení základních bezpečnostních pravidel. Velkou výzvu představují negativní jevy spojené s virtualizací ICT. Pokračující laicizace, dostupnost ICT a jejich propojování s internetem navyšují závažnost a četnost možných škod způsobených **nekvalifikovanou manipulací**. Zvýšené nároky na zajištění bezpečnosti rovněž přináší trend používání stejných ICT v pracovním i soukromém životě. Problematickým může být zejména přístup uživatelů k dodržování **bezpečnostní hygieny**. Vedle neúmyslných chyb otevírá nedodržování pravidel kybernetické bezpečnosti prostor pro kybernetickou kriminalitu (*pozn.: kybernetická kriminalita je v gesci orgánů činných v trestním řízení*).

Koncepce NBÚ vychází z aktuálních domácích i zahraničních zkušeností, rozpracovává bezpečnostní vzdělávání pro jednotlivé cílové skupiny, odůvodňuje potřebu jejich vzdělávání a doporučuje vhodné nástroje. Úloha NBÚ spočívá vedle **poskytnutí vlastní expertízy** rovněž **v koordinaci vzdělávacích kapacit** národních i zahraničních partnerských organizací. NBÚ na tvorbě koncepce spolupracoval především s Ministerstvem školství, mládeže a tělovýchovy, včetně Národního ústavu pro vzdělávání a Ministerstvem práce a sociálních věcí, které se vzděláváním v ICT a zvyšováním digitální gramotnosti dlouhodobě zabývají.

Koncepce chápe osvětu a vzdělávání v kybernetické bezpečnosti jako **systematický a kontinuální proces**, který bezodkladně reaguje na aktuální potřeby i trendy v užívání ICT. Zatímco v rámci obecného vzdělávání je primárním cílem vštípit a automatizovat základní návyky bezpečnostní hygieny, ve specifickém vzdělávání pokročilých uživatelů a odborníků je nezbytné další prohlubování dosavadních znalostí a dovedností.

STRUKTURA

Koncepce je strukturována do dvou kapitol.

1) OBECNÉ VZDĚLÁVÁNÍ

Základní osvěta určená především široké veřejnosti a institucím, které se vzděláváním a výchovou veřejnosti zabývají.

- a) Děti předškolního věku a žáci 1. stupně ZŠ
- b) Žáci 2. stupně ZŠ
- c) Žáci SŠ
- d) Pedagogičtí pracovníci
- e) Preventisté
- f) Sociální pracovníci a pomáhající profesionálové
- g) Odborná a zájmová sdružení
- h) Rodiče
- i) Senioři
- j) Široká veřejnost

2) SPECIFICKÉ VZDĚLÁVÁNÍ

Různě pokročilá školení určená pro uživatele se znalostmi kybernetické bezpečnosti.

- a) Správci KII a VIS
- b) Vysoké školy /akademická sféra
- c) Veřejná správa
- d) Policie ČR
- e) Armáda ČR
- f) Státní zástupci /soudci
- g) Soukromý sektor
- h) Pracoviště typu CERT a CSIRT (operátoři, analytici, specialisté)
- i) Administrátoři a bezpečnostní správci systémů a sítí

U každé cílové skupiny jsou posléze rozpracovány následující body:

- zdůvodnění cílové skupiny;
- určení vzdělávacích subjektů;
- doporučení vzdělávacích nástrojů;
- *specifická role NBÚ / NCKB a případných dalších přizvaných subjektů.*