PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

# Previazané s balíkom KPB6 – Publikačné výstupy

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

**Plánované príspevky na konferenciu na témy súvisiace s témou projektu**

Autorské kolektívy:

1. Milan Kubina, Martin Mičiak, Barbora Blahová
   (názov príspevku a konkrétna konferencia budú určené neskôr)
2. Milan Kubina, Dominika Toman, Dominika Findriková
   (názov príspevku a konkrétna konferencia budú určené neskôr)

Nasledujúce kapitoly obsahujú **podklady týkajúce sa témy kybernetickej bezpečnosti**. Tieto budú predmetom pripravovaných príspevkov.



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

# Úvod do problematiky

V súčasnej dobe, keď objem dát, vrátane tých v digitálnej forme, rastie exponenciálne, sa informácie stávajú kľúčovým výrobným faktorom, ktorého hodnota neustále narastá. V tejto súvislosti je nevyhnutné venovať zvýšenú pozornosť otázkam ich ochrany. Organizácie sa čoraz častejšie stávajú terčom útokov v digitálnom priestore. Zatiaľ čo na fyzickej úrovni (zabezpečenie zariadení a sietí) sú tieto organizácie často zabezpečené dostatočne alebo nadpriemerne, najslabším článkom v ochrane dát bývajú práve ľudia.

Pre úspešné fungovanie v digitálnej ére je pre organizáciu nevyhnutné zvyšovať povedomie o kybernetickej bezpečnosti medzi zamestnancami. Zvyšovanie povedomia by však malo viesť k zmene správania zamestnancov v digitálnom priestore. Na takúto zmenu je potrebné kontinuálne vzdelávanie zamestnancov v oblasti kybernetickej bezpečnosti a sociálneho inžinierstva. Proces vzdelávania by mal byť prispôsobený potrebám a očakávaniam organizácie (veľkosť, hierarchia, kultúra). Okrem výberu vhodných metód a spôsobov vzdelávania je potrebné nájsť aj vhodný spôsob motivovania zamestnancov ku vzdelávaniu v oblasti kybernetickej bezpečnosti. Cieľom vzdelávania je zabezpečenie kontinuálneho zlepšovania zručností a znalostí v danej oblasti. Častokrát však zamestnanci vnímajú vzdelávanie ako povinnosť, na ktorú pri výkone svojej práce nemajú čas.

Do budúcnosti by sa organizácie mali zamerať na integráciu moderných vzdelávacích prístupov a technologických inovácií, ktoré umožnia interaktívnejšie a efektívnejšie školenia. Simulácie kybernetických útokov či individualizované učebné plány môžu výrazne zvýšiť úroveň pripravenosti zamestnancov. Týmto spôsobom môžu organizácie nielen zvýšiť svoju bezpečnosť, ale aj posilniť svoju konkurencieschopnosť v čoraz digitalizovanejšom svete.

# Teoretické východiská

**Ľudské zdroje** sú považované za **najcennejší kapitál** pomáhajúci organizácii zvyšovať výkonnosť a konkurencieschopnosť. [1], [2] Podľa Armstronga (2007) je riadenie ľudských zdrojov definované ako **strategický a logicky premyslený prístup** k riadeniu toho najcennejšieho, čo v organizácii je – ľudí, ktorí v nej pracujú, a ktorí individuálne aj kolektívne prispievajú k dosiahnutiu cieľov organizácie. [2]

Na pojem **ľudské zdroje** nadväzuje aj **koncept ľudského potenciálu**, ktorý poukazuje na hĺbku a rozmanitosť schopností, ktoré zamestnanci prinášajú do pracovného prostredia. „Ľudský potenciál *predstavuje* sumárnu potenciu *(duševnú, inovačnú atď.), ako systém všetkých fyzických i psychických* možností, predpokladov a talentu, *ktorými sa ľudia vyznačujú a ktoré nechávajú prejaviť sa a zužitkovať, s markantným podielom a determináciou najmä* budúceho napredovania, *rozvoja, rastu.“* [3]

V teoretických prístupoch sa často objavuje aj koncept **ľudského kapitálu**. Tento pojem však nie je v rozpore s chápaním ľudského potenciálu, ale skôr ho dopĺňa. Rozlíšenie medzi nimi spočíva v tom, že **ľudský kapitál predstavuje aktuálne dostupné vedomosti, schopnosti a zručnosti jednotlivca**, zatiaľ čo **ľudský potenciál označuje kapacitu týchto zdrojov na ďalší rozvoj a uplatnenie v budúcnosti**. Ľudský kapitál tak možno považovať za **zásobu potenciálu**, ktorá má strategický význam pre dlhodobý rast a konkurencieschopnosť organizácie. [4] **Ľudský kapitál** predstavujú **jednotlivci,** ktorí sú **nositeľmi znalostí,** skúseností a nápadov prispievajúcich k **zvyšovaniu výkonnosti** a **konkurencieschopnosti** organizácie, ale aj celej spoločnosti. [5]

Pochopenie tejto komplexnosti vedie **k potrebe systematického a strategického rozvoja,** ktorý zabezpečí nielen využitie, ale aj dlhodobé budovanie tohto potenciálu. **Strategický rozvoj ľudského potenciálu** je proces definovania a plánovania **dlhodobých cieľov** a opatrení na podporu a **rozvoj ľudského potenciálu.** Zameriava sa na efektívne



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

**využívanie aktuálnych schopností** a kompetencií zamestnancov a manažérov, pričom kladie dôraz na ich **neustály rast,** zdokonaľovanie zručností a rozvoj talentu, ako aj na **posilnenie motivácie** do budúcnosti. [6] Rozvoj **podstatným spôsobom mení jednotlivca a pomáha mu rásť.** [7]

Jedným z kľúčových nástrojov, ako tento strategický rozvoj realizovať, je práve **vzdelávanie a profesionálny rast pracovníkov. „Vzdelávanie** a rozvoj zamestnancov a manažérov predstavuje **sústavný systematický proces** cieľavedomého a vyváženého skvalitňovania ľudského potenciálu organizácie.“ [8] Podľa Gibba (2008) je **vzdelávanie** špecifickým typom formálneho učenia poskytovaného na pracovnom mieste alebo **príprava na zamýšľanú prácu alebo rolu.** Je to **proces,** pri ktorom ľudia **získavajú a rozvíjajú špecifické zručnosti** pre kompetentný výkon. **Vzdelávacie aktivity** majú začiatok a koniec. Sú teda **časovo ohraničené.** [9] Z uvedeného vyplýva, že rozvoj ľudského potenciálu nie je náhodný proces, ale premyslený nástroj na dosahovanie strategických cieľov organizácie.

### *Zákony, normy a smernice v oblasti vzdelávania a kybernetickej bezpečnosti*

**Zákon č. 568/2009 Z. z. o celoživotnom vzdelávaní** upravuje systém celoživotného vzdelávania, pričom ďalšie vzdelávanie nadväzuje na dosiahnutý stupeň školskej kvalifikácie a zároveň **stanovuje podmienky pre akreditáciu vzdelávacích programov** v oblasti ďalšieho vzdelávania. Zákon vytvára **komplexný legislatívny rámec** pre **kontinuálne vzdelávanie** na Slovensku, ktorý zahŕňa ako formálne, tak neformálne formy **vzdelávania dospelých.** Definuje systém akreditácie vzdelávacích programov, čím **zabezpečuje kvalitu** a uznávanie získaných kvalifikácií. Zákon ustanovuje **mechanizmy pre certifikáciu** a **hodnotiace procesy,** vrátane osvedčení o čiastočných a úplných kvalifikáciách. Zákon taktiež upravuje postavenie a **kompetencie vzdelávacích inštitúcií** a poskytovateľov vzdelávania, čím vytvára **stabilný základ** pre **rozvoj sektora celoživotného vzdelávania.** [10]

**Smernica Európskeho parlamentu a Rady 2005/36/ES** zo 7. septembra 2005 o uznávaní odborných kvalifikácií predstavuje kľúčový legislatívny nástroj Európskej únie zameraný na **podporu voľného pohybu pracovníkov a služieb** v rámci jednotného trhu. Smernica ustanovuje **harmonizované postupy** pre **uznávanie odborných kvalifikácií** získaných v jednom členskom štáte v ostatných členských štátoch EÚ. Tento nástroj významne podporuje mobilitu kvalifikovaných pracovníkov a prispieva k **efektívnemu využívaniu ľudských zdrojov** v rámci európskeho pracovného trhu. [11]

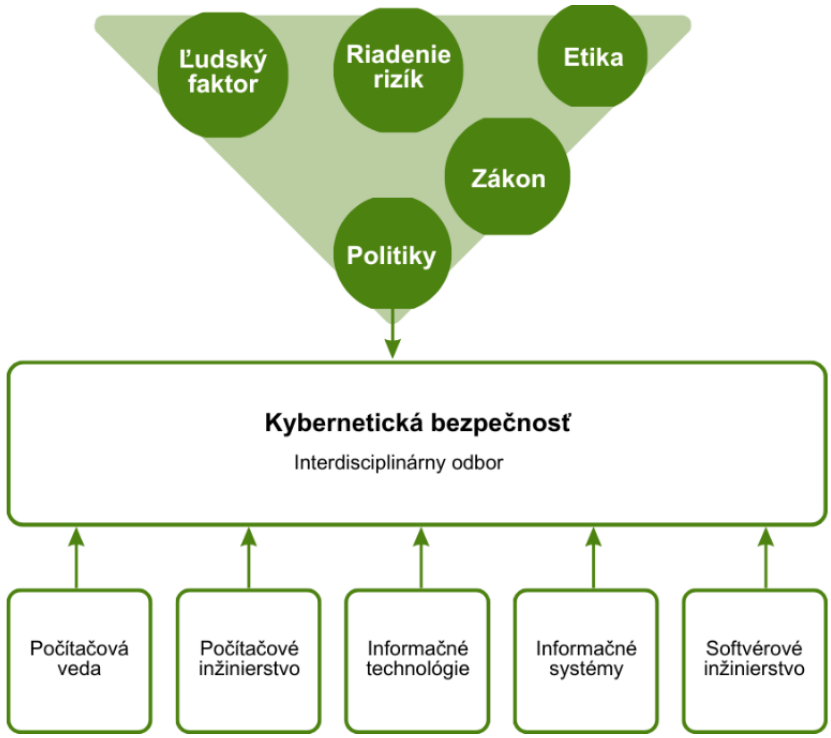
**Norma ISO 30414:2018** poskytuje **komplexný rámec** pre meranie a podávanie správ o ľudskom kapitáli organizácie. Ustanovuje súbor **58 metrík** rozdelených do **11 oblastí,** vrátane etiky, nákladov, diverzity, efektívnosti a produktivity, inovácie, organizačnej kultúry, organizačného zdravia a bezpečnosti, pripravenosti na pohotovostné situácie, náboru, udržania, zručností a spôsobilostí. Norma umožňuje organizáciám **porovnávať** svoju **výkonnosť** s inými subjektmi a podporuje **transparentnosť** v oblasti riadenia ľudských zdrojov. ISO 30414 taktiež pomáha organizáciám **identifikovať oblasti** pre **zlepšenie a optimalizáciu** investícií do **ľudského kapitálu,** čím prispieva k **dlhodobej udržateľnosti** a **konkurencieschopnosti.** [12]

**Vláda Slovenskej republiky** schválila **7. januára 2021** prostredníctvom uznesenia **č. 5/2021** *Národnú stratégiu kybernetickej bezpečnosti* na obdobie **2021-2025.** Tento kľúčový **strategický dokument** predstavuje **komplexnú koncepciu** pre **riadenie informačnej a kybernetickej bezpečnosti** na národnej úrovni. Stratégia je vypracovaná v súlade so strategickými dokumentami medzinárodných organizácií, konkrétne NATO, Európskej únie, OECD a Organizácie spojených národov. Strategický dokument obsahuje **šesť základných** oblastí: definovanie kľúčových princípov, identifikáciu a analýzu hrozieb, stanovenie **strategických cieľov,** určenie hlavných zahraničnopolitických partnerov, mechanizmy implementácie a merateľnosti, ako aj spôsoby financovania jednotlivých aktivít. [13]

Národná rada Slovenskej republiky prijala **30. januára 2018 zákon o kybernetickej bezpečnosti č. 69/2018,** ktorý nadobudol účinnosť 1. apríla 2018, pričom jeho úplné znenie je účinné od **25. mája 2018.** Tento legislatívny rámec pozostáva z **33 paragrafov** spolu s prechodnými a záverečnými ustanoveniami. Hlavným **účelom zákona** je vytvorenie legislatívnych podmienok potrebných na ochranu **kybernetického priestoru** štátu pred potenciálnymi bezpečnostnými hrozbami. Zákon **č. 69/2018 Z. z.** o kybernetickej bezpečnosti prešiel **zásadnou novelizáciou** prostredníctvom zákona **č. 366/2024 Z. z.,** ktorý bol schválený Národnou radou Slovenskej republiky a **nadobudol účinnosť 1. januára 2025.** Táto novela predstavuje prenesenie **európskej smernice NIS2** do slovenského právneho poriadku. [14]

**Smernica NIS2** predstavuje **európsky legislatívny nástroj zameraný** na posilnenie a zabezpečenie kybernetického priestoru v rámci Európskej únie. Všetky členské štáty EÚ majú **povinnosť implementovať túto smernicu** do svojho národného právneho systému. Smernica zavádza **inovatívne opatrenia** na **zlepšenie úrovne kybernetickej bezpečnosti.** Na Slovensku bola príslušná novela zákona schválená Národnou radou Slovenskej republiky a nadobudla **účinnosť 1. januára 2025.** [15]

**Kybernetická bezpečnosť (KB)** je prax **ochrany** počítačov, serverov, mobilných zariadení, elektronických systémov, sietí a údajov **pred škodlivými útokmi.** Je tiež známa ako bezpečnosť informačných technológií alebo **elektronická informačná bezpečnosť.** Tento pojem sa používa v rôznych kontextoch, od podnikania až po mobilné výpočty, a možno ho rozdeliť do niekoľkých bežných kategórií. [16] Termín kybernetická bezpečnosť sa používa na označenie opatrení, ktoré štátne inštitúcie prijímajú na ochranu verejnosti a seba samých pred hrozbami v **kybernetickej sfére**, známej aj ako **kyberpriestor**. Zároveň sa však používa aj na **individuálnejšej úrovni** – keď sa hovorí o **ochrane počítačov** pred vírusmi a iným škodlivým softvérom, či už ide o osobné zariadenie alebo počítač používaný v pracovnom prostredí. [17] V modernom chápaní je KB definovaná ako **interdisciplinárny odbor,** ktorý zahŕňa aspekty práva, politiky, ľudského faktoru, etiky a riadenia rizík.




**Obrázok 1 Štruktúra odboru kybernetickej bezpečnosti**
*Zdroj: [18]*



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

**Kybernetický priestor,** tzv. kyberpriestor je globálny, dynamický, otvorený systém, ktorý tvoria elektronické komunikačné siete, informačné systémy a ich programové vybavenie. Údaje, ktoré sú v tomto priestore, sa **spracovávajú elektronicky.** Systémy riadiacich, výrobných, bezpečnostných, resp. iných systémov a zariadení, činnosti, ktoré v jednotlivých častiach tohto systému prebiehajú, vzťahy a interakcie medzi časťami a prvkami sú subsystémami tohto systému. [19], [20]

Úlohou kybernetickej bezpečnosti je **chrániť kybernetické** (elektronické) **systémy pred kybernetickými hrozbami.** Vo vzťahu ku kybernetickej bezpečnosti je potrebné spomenúť aj **pojmy** [19]:

- **informačná bezpečnosť –** súhrn prostriedkov a postupov na zabezpečenie **dôvernosti, integrity** a **dostupnosti** informácií, ale aj na zabezpečenie ochrany proti neautorizovanej manipulácii alebo poškodeniu informácií v informačnom systéme. [21]
- **ochrana kritickej infraštruktúry** – zaoberá sa ochranou proti rozvrátení, obmedzení, deštrukcii a zlomyseľným operáciám voči infraštruktúre bezpečnosti.

Prepojenie **systému riadenia informačnej bezpečnosti** (ISMS) a **vzdelávania zamestnancov** v oblasti kybernetickej bezpečnosti je **kľúčové,** pretože efektívne ISMS závisí od **systematických a pravidelne sa opakujúcich vzdelávacích aktivít.** Vzdelávanie v kybernetickej bezpečnosti plní preventívnu funkciu voči ľudským chybám, ktoré predstavujú jeden z najzávažnejších rizikových faktorov pre informačnú bezpečnosť organizácie. Vytvorenie **komplexného vzdelávacieho programu,** ktorý zahŕňa pravidelný **tréning, osvetu** o kybernetických hrozbách a **testovanie pripravenosti zamestnancov,** podporuje bezproblémové zavedenie a fungovanie ISMS. Podľa normy ISO/IEC 27001:2022 príloha A, pod A.7.2.2 (Osveta, vzdelávanie a školenie) sa **odporúčajú pravidelné školenia** a osveta v oblasti kybernetickej bezpečnosti, aby sa zamestnanci stali **vedomí rizík** a bezpečnostných politík organizácie, čím sa **znižuje pravdepodobnosť bezpečnostných incidentov.**

**Systém riadenia informačnej bezpečnosti** možno charakterizovať ako **komplexný dokumentovaný systém,** ktorý definuje základné požiadavky na informačnú bezpečnosť naprieč všetkými organizačnými úrovňami. **Norma ISO/IEC 27001** poskytuje metodický rámec pre plánovanie, implementáciu, kontrolu a kontinuálne zlepšovanie tohto systému prostredníctvom cyklického prístupu. Systém zahŕňa požiadavky na komplexnú analýzu, systematické riadenie a dôkladné vyhodnocovanie rizík, pričom definuje potrebné bezpečnostné opatrenia na minimalizáciu potenciálnych negatívnych dopadov na organizáciu. [22]

## Súčasný stav problematiky

Správanie jednotlivcov, ich postoje k bezpečnosti a schopnosť správne reagovať na **rizikové situácie** predstavujú kľúčové determinanty odolnosti organizácií voči kybernetickým hrozbám. Tento aspekt naberá na význame najmä v kontexte rastúceho počtu incidentov, ktoré priamo vyplývajú z ľudských chýb. Ako ukazuje vývoj na Slovensku, incidenty spôsobené **nevedomosťou, nepozornosťou či podcenením rizík** zostávajú dominantné naprieč rôznymi sektormi. Jedným z najvýraznejších prejavov tejto zraniteľnosti je nárast phishingových útokov (kybernetický útok, pri ktorom sa útočníci snažia získať citlivé informácie pomocou podvodných e-mailov, či SMS správ). V roku 2023 predstavoval **až 48 %** všetkých útokov práve **phishing.** Dominantnou vstupnou bránou bola **ľudská chyba** pri interakcii s e-mailovými alebo webovými podvodmi. [23] DDoS (Distributed Denial of Service) útoky (zahltenie webovej stránky, servera alebo siete), ktoré medziročne narástli **o 45 %,** taktiež poukazujú na fakt, že bezpečnostné povedomie a pripravenosť zamestnancov sú rozhodujúcimi faktormi v schopnosti organizácií čeliť eskalujúcim hrozbám. [24] Napriek



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

existencii relevantných štátnych stratégií sa ukazuje, že prax v jednotlivých organizáciách zaostáva za odporúčaniami. Hoci strategické dokumenty Slovenskej republiky, ako Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, zdôrazňujú **potrebu rozvoja bezpečnostnej kultúry a edukácie,** implementácia týchto princípov v praxi je nerovnomerná. Správy NBÚ (Národný bezpečnostný úrad) opakovane poukazujú na **nízku mieru bezpečnostného povedomia** v sektore verejnej správy, **absenciu aktívneho školenia zamestnancov** a nedostatky v zdieľaní dobrej praxe medzi organizáciami. [25],[26] V praxi existujú výrazné rozdiely medzi jednotlivými sektormi. Sektory ako bankovníctvo dosahujú vysoký stupeň pripravenosti. V iných oblastiach, najmä v oblasti zdravotníctva a energetiky, sa zistenia pravidelne dotýkajú aj základného nepochopenia bezpečnostných princípov a ignorovania legislatívnych povinností. Na prekonanie týchto výziev je **nevyhnutné implementovať systematický prístup** k podpore kybernetickej bezpečnosti prostredníctvom **rozvoja ľudského kapitálu.**

Dôležitosť ľudského faktora potvrdzujú aj **zahraničné výskumy. Verzion** poukazuje na to, že **väčšina únikov dát** je spôsobených **ľudským zavinením.** [27] Podľa správy FBI, došlo medzi júnom 2017 a júlom 2019 **k stratám vo výške 26 miliárd** dolárov v dôsledku **útokov cez e-maily,** ktoré obsahovali pokyny na schválenie platieb útočníkom a tvárili sa, že pochádzajú od vedúcich pracovníkov. Počas pandémie COVID-19 sa **finančné straty zvýšili na 43 miliárd dolárov,** pravdepodobne v dôsledku práce na diaľku, keďže komunikácia prebiehala prevažne elektronicky. [28] Phishingové útoky, ktoré sú najčastejším, najpreskúmanejším a najúspešnejším typom útokov, ktoré spôsobujú bezpečnostné incident. [29], [30] Pracovná skupina proti phishingu (APWG), ktorá zhromažďuje najviac phishingových e-mailov na svete, uvádza, že phishing sa od roku 2019 rozrastá. V roku 2019 bolo zaznamenaných **800 000 phishingových stránok,** v roku 2020 to bolo **1,8 milióna,** v roku 2021 už **2,8 milióna** a v roku 2022 **viac ako 4,7 milióna.** [31] V porovnaní s rokom 2022 kybernetické incidenty **vzrástli o 27 %.** Phishing tvoril **48 %** všetkých kybernetických útokov v roku 2023. Pričom celkový počet nahlásených kybernetických incidentov v roku 2023 bol **7 432.** Organizácie v SR kvôli kybernetickým útokom stratili priemerne **120 000 € na jednu organizáciu.** [26]**,** [25] Situácia na Slovensku však poukazuje na **vážny nedostatok** v oblasti vzdelávania. Na Slovensku **až 69 %** organizácií **neposkytlo** svojim zamestnancom **školenie** na zvyšovanie povedomia o kybernetickej bezpečnosti, či vzdelávacie aktivity v tejto oblasti. Napriek tomuto nedostatku **41 %** organizácií v Česku a Nemecku v uplynulom roku podniklo kroky na zvýšenie povedomia a školenie svojich zamestnancov v kybernetickej bezpečnosti. Tento rozdiel poukazuje na **rozmanité prístupy k vzdelávaniu** o kybernetických hrozbách v rámci **Európskej únie** a zdôrazňuje **potrebu systematického zlepšovania bezpečnostného povedomia** v organizáciách. [32] Z uvedeného vyplýva, že **absencia systematického vzdelávania** zamestnancov v oblasti kybernetickej bezpečnosti predstavuje **vážny problém,** ktorý môže ohroziť nielen jednotlivé organizácie, ale aj **spoločenskú infraštruktúru ako celok.**

Útočníci totiž čoraz častejšie využívajú **behaviorálne a psychologické slabiny ľudí**, aby obchádzali technické bariéry a získali prístup k dôverným údajom či systémom. Tento spôsob útoku, známy ako **sociálne inžinierstvo**, sa opiera o manipulatívne techniky ako presviedčanie, vzbudenie dôvery alebo paniky, čím zneužíva ľudské správanie a psychológiu. V oblasti kybernetickej bezpečnosti už nestačí chrániť iba technickú infraštruktúru. Útočníci využívajú **behaviorálne a psychologické slabiny**, aby obišli technické opatrenia a získali prístup k dôverným údajom či systémom. Tento prístup je známy ako **sociálne inžinierstvo**, ktoré sa spolieha na manipuláciu, presviedčanie, vzbudenie dôvery alebo paniky.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

## Hlavné oblasti výskumu, predpokladaný postup a možnosti využitia navrhnutého riešenia

Zvyšujúci sa počet kybernetických incidentov spôsobených ľudskou chybou potvrdzuje, že technické riešenia samy osebe **nie sú dostatočné na ochranu organizácií** pred útokmi. **Vzdelávanie zamestnancov** sa tak stáva kľúčovým prvkom odolnosti voči hrozbám. Dizertačná práca by sa preto mala zameriavať na **výskum efektívnosti vzdelávacích programov** v oblasti kybernetickej bezpečnosti a ich potenciál prispieť k **budovaniu bezpečnostného povedomia a správania.**

### *Predmet skúmania*

Predmetom skúmania dizertačnej práce budú **vzdelávacie programy** a aktivity zamerané na kybernetickú bezpečnosť, **ich forma, obsah,** a predovšetkým ich **efektívnosť** v kontexte prevencie kybernetických incidentov. Cieľom je posúdiť, do akej miery tieto programy **vedú k zlepšeniu správania zamestnancov** a k zníženiu rizík vyplývajúcich z ľudského faktora.

### *Objekt skúmania*

Objekt výskumu budú **zamestnanci organizácií,** prípadne aj vrátane vzdelávacích inštitúcií, pričom pozornosť bude sústredená najmä na **sektory s vysokou mierou rizika** a nižšou úrovňou pripravenosti, prevažne však malé a stredné organizácie.

### *Metódy výskumu*

Medzi aplikované metódy budú patriť **kvantitatívne metódy,** a to najmä použitie dotazníkov pred a po vzdelávacích aktivitách, s cieľom porovnať úroveň povedomia, vnímanie rizík a schopnosť reagovať na simulované incidenty. Ďalej to budú **kvalitatívne metódy,** prevažne hĺbkové rozhovory s bezpečnostnými expertmi, HR manažérmi a účastníkmi školení a vyhodnotenie prípadových štúdií z organizácií, ktoré implementovali rôzne formy školení. Súčasťou práce bude aj **analýza sekundárnych dát** a využitie existujúcich štatistík (napr. NBÚ, ENISA), trhových správ, ako aj odporúčaní rámcov ako NIST, ktoré poskytujú štandardizovaný pohľad na bezpečnostné vzdelávanie. Budú využité prvky **analýzy a metaanalýzy, dekompozície, syntézy, komparácie či štrukturalizácie, historickej metódy, kreatívnej metódy, pozorovania, dedukcie, indukcie, generalizácie, modelovania a štatistického vyhodnocovania.**



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

# Zoznam použitej literatúry

[1] A. Baron a M. Armstrong, *Human Capital Management: Achieving Added Value Through People*. Kogan Page Publishers, 2007.

[2] M. Orenič, "Aplikácia Nových Trendov Riadenia Ľudských Zdrojov V Organizácii", *Mladá Veda*, roč. 11, č. 1, s. 136–155, mar. 2023.

[3] Dominika Toman, "RIADENIE A ROZVOJ ĽUDSKÉHO POTENCIÁLU". 2022.

[4] M. Mičiak, "Návrh modelu posudzovania efektívnosti ľudského kapitálu pre zvyšovanie výkonnosti a konkurencieschopnosti podniku na trhu", Dizertačná práca, Žilinská univerzita v Žiline, Žilina, 2020. [Online]. Available at: https://opac.crzp.sk/?fn=detailBiblioFormChildC55R0&sid=81B8C7E3C61A011F163F361BFB16&seo=CRZP-detail-kniha

[5] A. Kucharcikova, M. Durisova, a N. Staffenova, "Implementation of the human capital management concept: an empirical study of small trading company", *Humanit. Soc. Sci. Commun.*, roč. 11, č. 1, s. 1–14, nov. 2024, doi: 10.1057/s41599-024-03946-x.

[6] Dominika Toman, "STRATEGICKÝ ROZVOJ ĽUDSKÉHO POTENCIÁLU". 2022.

[7] "Bridging Canadian Adult Second Language Education and Essential Skills Policies: Approach With Caution - Tara L. Gibb, 2008". Cit: 12. február 2025. [Online]. Available at: https://journals.sagepub.com/doi/abs/10.1177/0741713608318893

[8] Dominika Toman, "VZDELÁVANIE A ROZVOJ ZAMESTNANCOV". 2024.

[9] S. Bujnová, "Návrh vnitropodnikového vzdělávání zaměstnanců, zaznamenávání a sdílení tacitních a explicitních znalostí".

[10] S.-E. s r o s.r.o AION CS, "568/2009 Z. z. Zákon o celoživotnom vzdelávaní | Aktuálne znenie", epi.sk. Cit: 28. máj 2025. [Online]. Available at: https://www.epi.sk/zz/2009-568

[11] "Smernica - 2005/36 - EN - EUR-Lex". Cit: 28. máj 2025. [Online]. Available at: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32005L0036

[12] "ISO 30414:2018 Human Capital Reporting - HRSI". Cit: 28. máj 2025. [Online]. Available at: https://www.business.hrci.org/certifications/iHumanCapitalReporting

[13] "Národná stratégia a akčný plán kybernetickej bezpečnosti". Cit: 04. február 2025. [Online]. Available at: https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti/

[14] "69/2018 Z.z. - Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov". Cit: 04. február 2025. [Online]. Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

[15] "Pripravte sa na NIS2 a novelu kyberzákona | ESET". Cit: 04. február 2025. [Online]. Available at: https://www.eset.com/sk/nis2/

[16] "WHAT IS CYBERSECURITY AND WHAT CYBERSECURITY SKILLS ARE EMPLOYERS SEEKING?", *Issues Inf. Syst.*, 2019, doi: 10.48009/2_iis_2019_62-72.

[17] M. Bay, "In search of an encompassing definition for the post-Snowden era", 2016.

[18] Sedlák et al., *Kybernetická (ne)bezpečnosť*, Prvé. Brno: Akademické nakladatelství CERM, s. r. o., 2021.

[19] Dušan Levický, *Úvod do kybernetickej bezpečnosti*, Prvé., 100 roč. Košice: elfa, 2019.

[20] I. Makatura, "Čo je to kybernetická bezpečnosť? | Preventista.sk". Cit: 31. január 2025. [Online]. Available at: https://preventista.sk/info/co-je-to-kyberneticka-bezpecnost/



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

[21] D. Findriková a M. Kubina, “Cybersecurity risks in transportation”, *Transp. Res. Procedia*, roč. 87, s. 135–140, jan. 2025, doi: 10.1016/j.trpro.2025.04.116.

[22] “ISO/IEC 27001:2022”, ISO. Cit: 06. marec 2025. [Online]. Available at: https://www.iso.org/standard/27001

[23] AliPort, “Manažované služby kybernetickej bezpečnosti - ALISON Slovakia”. Cit: 29. marec 2025. [Online]. Available at: https://aliport.sk/statistiky-kybernetickej-bezpecnosti

[24] TASR, “Kybernetické útoky na Slovensku prudko stúpajú: Priemerný počet útokov na firmu sa strojnásobil”, Živé.sk. Cit: 29. marec 2025. [Online]. Available at: https://zive.aktuality.sk/clanok/k8T7Qo6/kyberneticke-utoky-na-slovensku-prudko-stupaju-priemerny-pocet-utokov-na-firmu-sa-strojnasobil/

[25] “Výročná správa NBÚ”. Cit: 12. február 2025. [Online]. Available at: https://www.nbu.gov.sk/data/att/2855.pdf

[26] “Výročná správa NBÚ 2022”. Národný bezpečnostný úrad, 2022.

[27] T. Steen, “Developing a behavioural cybersecurity strategy: A five-step approach for organisations”, *Comput. Stand. Interfaces*, roč. 92, s. 103939, mar. 2025, doi: 10.1016/j.csi.2024.103939.

[28] T. Longtchi, R. Rodriguez, L. Shawaf, A. Atyabi, a S. Xu, “Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey | IEEE Journals & Magazine | IEEE Xplore”. Cit: 29. marec 2025. [Online]. Available at: https://ieeexplore.ieee.org/abstract/document/10493072?casa_token=vxChRtXbMQQAAAAA:jSfrfnuU24ornCzXo4Jal8zSnz9JX_kLZQ001X36w2K132rCTp9jr25r_c_UPREH6KpF3QkLEIpn8A

[29] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, a S. Shukla, “Applications of deep learning for phishing detection: a systematic literature review”, *Knowl. Inf. Syst.*, roč. 64, č. 6, s. 1457–1500, jún. 2022, doi: 10.1007/s10115-022-01672-x.

[30] F. Salahdine a N. Kaabouch, “Social Engineering Attacks: A Survey”, *Future Internet*, roč. 11, č. 4, Art. č. 4, apr. 2019, doi: 10.3390/fi11040089.

[31] “APWG | Phishing Activity Trends Reports”. Cit: 06. január 2025. [Online]. Available at: https://apwg.org/trendsreports/

[32] “Firms cybersecurity training in EU”, Statista. Cit: 29. marec 2025. [Online]. Available at: https://www.statista.com/statistics/1498051/firms-cybersecurity-training-in-eu/



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY