MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

SEKCIA KYBERNETICKEJ BEZPEČNOSTI
ODBOR RIADENIA KYBERNETICKEJ
A INFORMAČNEJ BEZPEČNOSTI
VLÁDNA JEDNOTKA
CSIRT

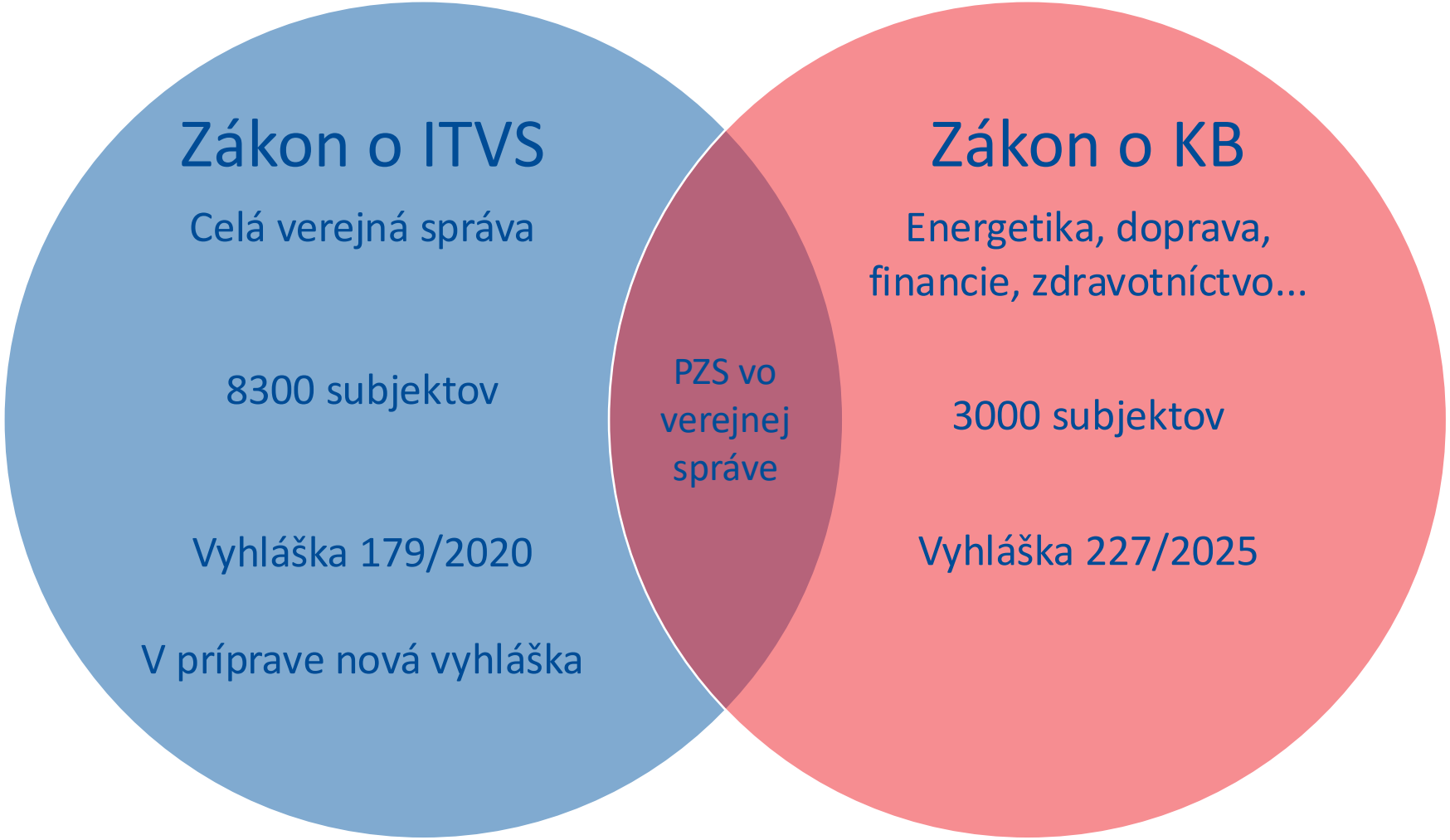
Aktivity MIRRI SR v oblasti KB pre verejnú správu

PROGRAM SLOVENSKO

PLÁN OBNOVY
Financované Európskou úniou
NextGenerationEU

Ing. Róbert Kováč
21.05.2026

Zákon č. 95/2019 Z.z. o ITVS - Zákon č. 69/2018 Z.z. o KB



Podpora verejnej správy

Centrálny portál kybernetickej bezpečnosti

Čo nájdete na portáli:

- Jednotný metodický rámec - štandardizované, aktuálne, bezplatné dokumenty pre verejnú správu
- Dôležité upozornenia a novinky v oblasti KIB
- Návody (návody pre obce, návody pre školy), usmernenia, manuály
- Kategorizáciu subjektov podľa vyhlášky 179/2020 Z.z.
- Checklisty na overenie súladu so zákonom o ITVS a vyhláškou
- Informácie o vzdelávaní – e-learning pre Vašich zamestnancov už tento mesiac?
- Kyber Asistent - AI chatbot

Pripravujeme:

- Checklisty k novej vyhláške
- Jednoduchú orientáciu v spleti povinností – Kyber Sprievodca
- Dokumenty na jednom mieste
- Návody pre jednotlivé kategórie subjektov

https://kyberportal.slovensko.sk

PLÁN OBNOVY

Financované Európskou úniou NextGenerationEU

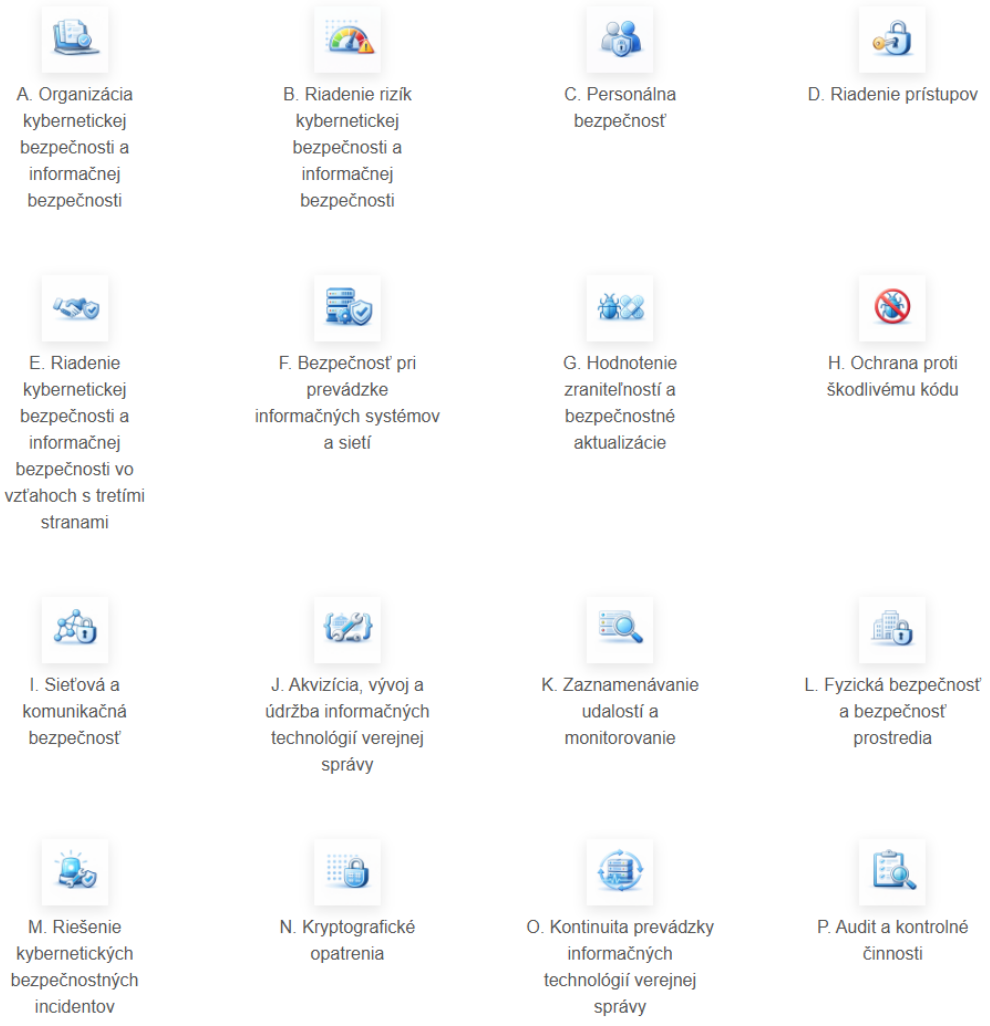
Jednotný metodický rámec

Čo je Jednotný metodický rámec

- Súhrn metodík, návodov, smerníc, či vzorov pre všetky subjekty verejnej správy na zabezpečenie kybernetickej a informačnej bezpečnosti v organizácii a súladu s právnymi predpismi v oblasti
- Viac ako 130 aktuálnych dokumentov
- Roztriedené podľa oblastí v rámci vyhlášky 179/2020 Z.z.
- Aktualizácia dokumentov pri novelizácii relevantných noriem
- Všetky dokumenty sú k dispozícii bezplatne verejnej správe
- Aktualizované k marcu 2026

Vybraná oblasť: Kontinuita prevádzky ITVS

- Smernica Riadenie kontinuity procesov
- Stratégia BCM
- Vzor Analýza dopadov (business impact analysis BIA)
- Vzor Plán testovania BCP, plán testovania DRP
- Vzor Plány kontinuity procesov (business continuity plans - BCP)
- Vzor Plány obnovy (disaster recovery plans - DRP)
- Evidencia záloh
- Smernica Riadenie zálohovania
- Stratégia pre zálohovanie
- Vzor Plán testovania obnovy zo záloh, plán záloh, záznam z vykonania zálohy
- Vzor testovanie obnovy dát zo zálohy



Vzdelávanie v kybernetickej a informačnej bezpečnosti

E-learning

- E-learningové vzdelávacie materiály vo forme profesionálneho video a animačného obsahu
- Bezplatne pre všetkých zamestnancov verejnej správy
- 6 rôznych modulov pre laikov, kvalifikovaných, riadiacich a špecializovaných riadiacich zamestnancov
- Testy a certifikáty
- Rozhovory s odborníkmi ako bonusový obsah
- Prvý modul k dispozícii na prelome mája a júna 2026

Online školenia

- Pri zmene legislatívy
- K metodikám
- K novým službám (spustenie e-learningu a podobne)

Workshopy a konferencie

- KyberTour 2026 – každé krajské mesto

Kybernetická aréna

- Školenia špecialistov na boj proti kybernetickým útokom

PLÁN OBNOVY

Financované Európskou úniou
NextGenerationEU

Služby vládnej jednotky CSIRT

Služba Achilles

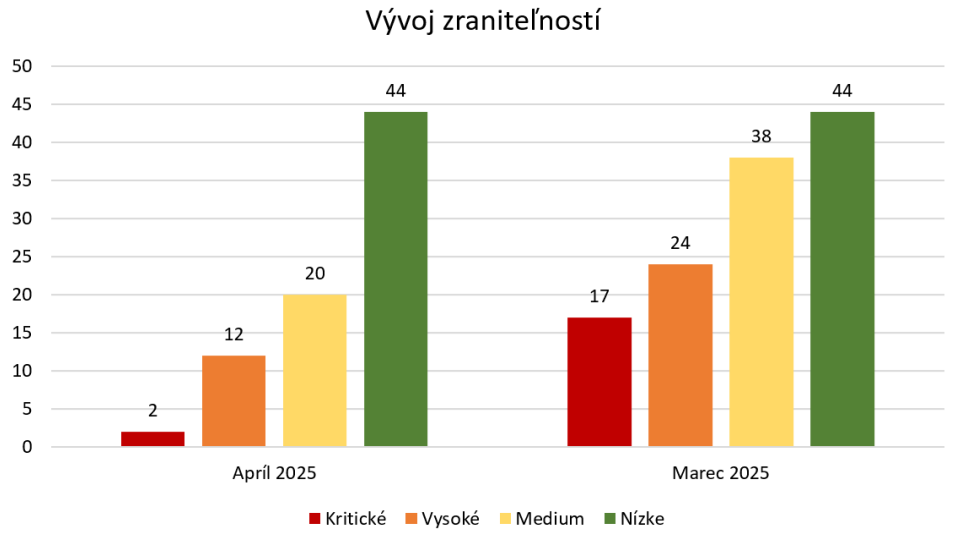
- Slúži na pravidelné a plošné neinvazívne hodnotenie zraniteľností služieb verejnej správy
- Služba podporuje ochranu pred útočníkmi prostredníctvom prevencie
- Zabezpečuje prehľad o stave infraštruktúry z externého prostredia
- Služba upozorňuje aj na úniky hesiel (služba Have i Been Pwned)
- Zaregistrujte sa na: **csirt.sk**

Výhody služby Achilles

- Mesačný report s identifikovanými zraniteľnosťami
- Aktuálne informácie o kampaniach aktérov hrozieb
- Odporúčania pre zabezpečenie infraštruktúry vyplývajúce z nálezov

Služba Domino

- pravidelné overovanie dostupnosti webových služieb



Služby vládnej jednotky CSIRT

Služba Ares

- Penetračné testovanie
- Testovanie webových aplikácií,
- Testovanie internej infraštruktúry (napr. interné siete, Active Directory),
- Testovanie externej infraštruktúry (verejne dostupné systémy),
- Bezpečnostné audity zariadení a konfigurácií.

Služba Afrodita

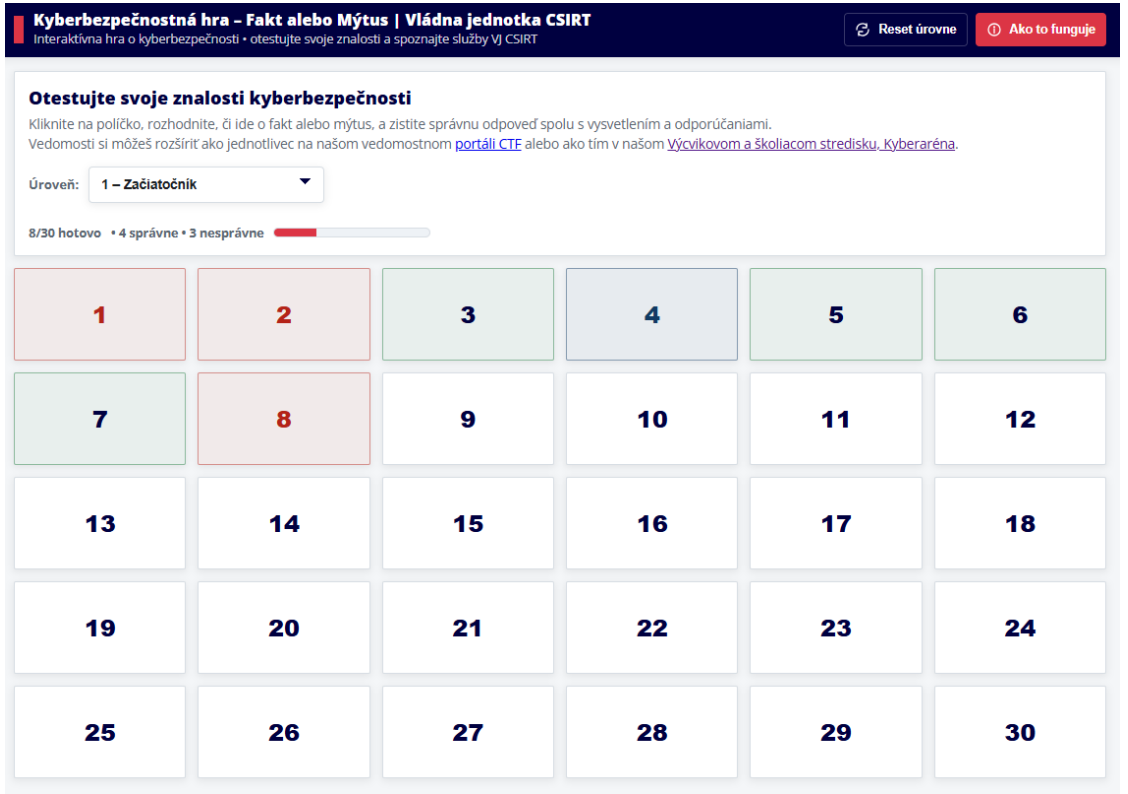
- Prístup pre zapojené subjekty k nástroju MISP s názvom „Afrodita“
- Platforma pre zdieľanie informácií o hrozbách škodlivého kódu
- Prístup k informáciám o indikátoroch kompromitácie z aktuálneho diania
- Možnosť ukladať si dané IoC vo Vašom vlastnom nástroji

Kybernetická aréna

- Školenie expertov na boj proti kybernetickým útokom
- Registrácia a CTF portál: **kyberarena.csirt.sk**

Kyberbezpečnostná hra

- Vyskúšajte ju tu: **csirt.sk/kyberbezpecnostna-hra.html**



CSIRT.SK

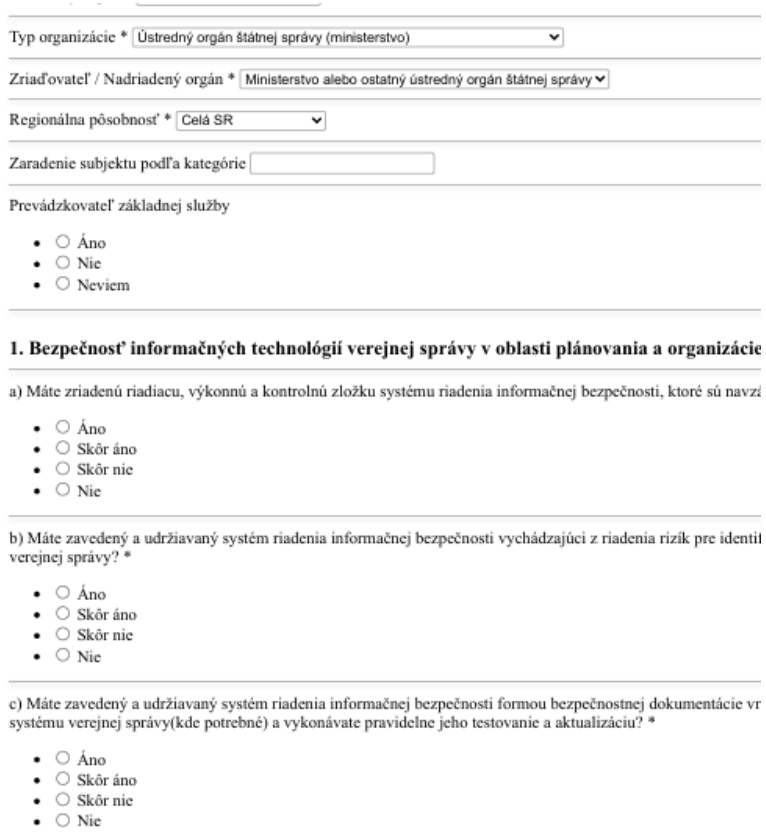
Správa o stave kybernetickej a informačnej bezpečnosti verejnej správy 2026

Účel

- Sledovať stav a vývoj úrovne bezpečnosti v čase
- Odhaliť hlavné nedostatky v rôznych segmentoch či doménach bezpečnosti
- Smerovať pomoc, aktivitu, osvetu tam, kde je to potrebné
- Tvoriť kvalitnejšiu legislatívu, politiky a koncepčné dokumenty
- Zvýšiť transparentnosť o stave a smerovaní KIB vo VS
- Vytvárať tlak na zvýšenie financovania kybernetickej bezpečnosti
- Ročná periodicita

Zber dát (anonymizovaný)

- Samohodnotiaci dotazník – zber dát online na CPKB a cez DKS
- Výstupy z kontrol ORKIB
- Hodnotenia zraniteľností a incidentov VJ CSIRT
- Výstupy NBÚ (správa o stave KB, samohodnotenia?, audity?)
- Iné zdroje (kritická infraštruktúra, vzdelávacie inštitúcie...)



Typ organizácie * Ústredný orgán štátnej správy (ministerstvo)

Zriaďovateľ / Nadriadený orgán * Ministerstvo alebo ostatný ústredný orgán štátnej správy

Regionálna pôsobnosť * Celá SR

Zaradenie subjektu podľa kategórie

Prevádzkovateľ základnej služby

- Áno
- Nie
- Neviem

1. Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

a) Máte zriadenú riadiacu, výkonnú a kontrolnú zložku systému riadenia informačnej bezpečnosti, ktoré sú navzá

- Áno
- Skôr áno
- Skôr nie
- Nie

b) Máte zavedený a udržiavaný systém riadenia informačnej bezpečnosti vychádzajúci z riadenia rizík pre identif verejnej správy? *

- Áno
- Skôr áno
- Skôr nie
- Nie

c) Máte zavedený a udržiavaný systém riadenia informačnej bezpečnosti formou bezpečnostnej dokumentácie vr systému verejnej správy(kde potrebné) a vykonávate pravidelne jeho testovanie a aktualizáciu? *

- Áno
- Skôr áno
- Skôr nie
- Nie

Projektová podpora

Čo sa nám podarilo - Plán obnovy a odolnosti SR

- Úspešne realizované reformy a investície
- Štandardizácia, vzdelávanie, Systém včasného varovania, kritická infraštruktúra

Čo plánujeme - Program Slovensko

- Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov
- Národné laboratórium umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab)

Čo plánujeme - NKIVS 2026-2030

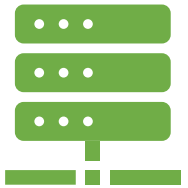
- Program Baseline bezpečnosti
- Program Zabezpečenie kontinuity prevádzky
- Program Operačná bezpečnosť

Čo plánujeme - Reformy a investície nadväzujúce na NKIVS

- Vnútroštátny plán digitálnej dekády
- Národný a regionálny partnerský plán 2028 - 2034
- Vízia Slovensko 2040

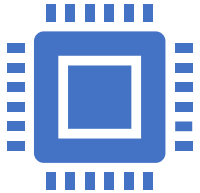
Baseline bezpečnosti

Metodiky, školenia, súlad s legislatívou



Operačná bezpečnosť

Dohľadové centrá, nástroje obrany



Kontinuita prevádzky

Technológie, DRP, infraštruktúra

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

www.mirri.gov.sk

Ing. Róbert Kováč
Odbor riadenia kybernetickej
a informačnej bezpečnosti