SLOVENSKÁ AKREDITAČNÁ AGENTÚRA
PRE VYSOKÉ ŠKOLSTVO

VNÚTORNÝ PREDPIS č. 3/2024

METODIKA ANALÝZY RIZÍK INFORMAČNEJ BEZPEČNOSTI SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

V Bratislave 20. júna 2024

METODIKA ANALÝZY RIZÍK INFORMAČNEJ BEZPEČNOSTI SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

Výkonná rada Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „výkonná rada“) schválila dňa 20. júna 2024 podľa § 7 ods. 10 písm. d) zákona č. 269/2018 Z. z. o zabezpečovaní kvality vysokoškolského vzdelávania a o zmene a doplnení zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) túto *Metodiku analýzy rizík informačnej bezpečnosti Slovenskej akreditačnej agentúry pre vysoké školstvo*.

Článok 1
Úvodné ustanovenia

1. Cieľom tohto vnútorného predpisu je popis procesu a metodiky analýzy rizík informačnej bezpečnosti, jej cieľov a priorít. Procesom analýzy rizík sa dosahuje identifikácia hroziacich rizík, pravdepodobnosti dopadov jednotlivých hrozieb na aktíva Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „SAAVŠ“ alebo „agentúra“) a určenie adekvátnych bezpečnostných opatrení, ako tieto riziká odstrániť alebo znížiť na akceptovateľnú úroveň.

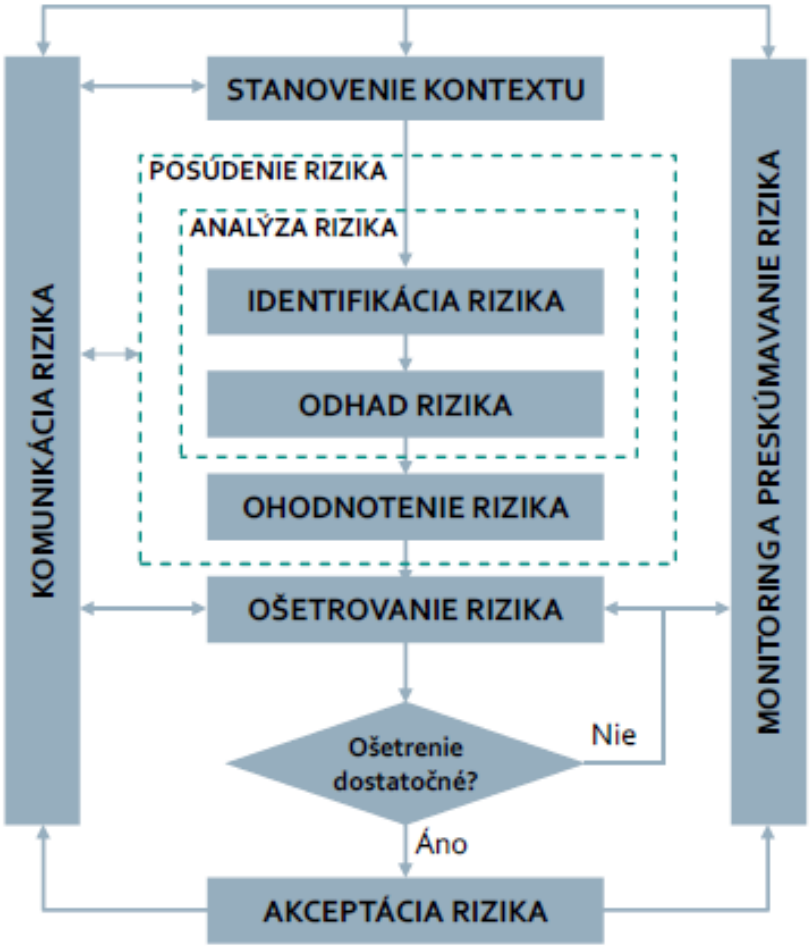
Článok 2
Rozsah, ciele a priority analýzy rizík

1. Do rozsahu analýzy rizík informačnej bezpečnosti (ďalej len „analýza rizík“) patria aktíva v správe SAAVŠ. Pod *aktívom* sa rozumie každá informácia, systém, aplikácia alebo hardvér v majetku SAAVŠ, ktorý sa používa pri prevádzkových činnostiach a podieľa sa na prevádzke základnej služby v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“), alebo súvisí s informačnými technológiami verejnej správy podľa Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „ZoITVS“).
2. Cieľom analýzy rizík je:
   - identifikovať možné hrozby pôsobiace na aktíva SAAVŠ,
   - identifikovať potenciálne zraniteľnosti, ktoré tieto hrozby môžu zneužiť,
   - vyhodnotiť riziká podľa metodiky popísanej v článku č. 6,
   - navrhnúť bezpečnostné opatrenia na zníženie identifikovaných rizík.

Článok 3
Analýza rizík

1. Celkový proces riadenia rizika pozostáva z cyklických a na seba nadväzujúcich procesov:
   1) stanovenie kontextu rizík,
   2) posúdenie rizík,
   3) ošetrovanie rizík,
   4) komunikácia o rizikách,
   5) monitorovanie a preskúmanie rizika.
2. Samotné posudzovanie rizík uvedené v bode č. 2 ods. 1 je komplexný proces, ktorý pozostáva z:
   1) identifikácie rizík,
   2) analýzy rizík,
   3) ohodnotenia rizík.

Schéma procesu riadenia rizík informačnej bezpečnosti
podľa normy ISO/IEC 27005



3. Analýza rizík sa opiera o **kvalitatívnu metódu**, t. j. na definovanie rizikových faktorov sú použité **nečíselné (slovné) hodnoty**. Hodnota pravdepodobnosti a dopadu je určená na základe individuálnych odborných znalostí. Takéto vyjadrenie jednotlivých udalostí využíva odhad, ktorý vyjadruje mieru osobného presvedčenia o výskyte posudzovaného javu (hrozby, škodlivej udalosti).
4. Metodika vychádza z odporúčaní uverejnených Národným bezpečnostným úradom v Metodike analýzy rizík kybernetickej bezpečnosti v 1.0 z 13. decembra 2021 a účinnej od 1. januára 2022.
5. Stanovenie kontextu pozostáva najmä z nasledujúcich činností:
   - identifikácia aktív SAAVŠ,
   - identifikácia zraniteľností,
   - identifikácia potenciálnych hrozieb,
   - odhad dopadov,
   - odhad pravdepodobností,
   - identifikácia existujúcich opatrení.

Článok 4
Identifikácia hrozieb a zraniteľností

1. Hrozba má vo všeobecnosti potenciál poškodenia aktív; môže byť úmyselná (Ú), alebo náhodná (N), príp. spôsobená vplyvom prostredia pre udalosti, ktoré vznikajú nezávisle od

ľudskej činnosti, t. j. prostredia (P).

2. Na efektívne riadenie rizík je nevyhnutné identifikovať všetky hrozby spôsobilé narušiť informačnú a kybernetickú bezpečnosť. Zoznam uvažovaných hrozieb je uvedený v tabuľke nižšie, spolu s informáciou, či má vplyv na dôvernosť (confidentiality – C), integritu (integrity – I) alebo dostupnosť (availability – A) dát.
3. Zoznam hrozieb uvažovaných a použitých v analýze rizík je uvedený v prílohe č. 1 tejto smernice.
4. Okrem externých, verejných katalógov hrozieb môžu byť relevantné najmä nasledujúce dodatočné zdroje informácií:
   - **výkonní zamestnanci** – osobne, mailom, telefonicky, príp. prostredníctvom rôznych formulárov alebo service-deskových systémov;
   - **odborní zamestnanci** – riziká zistené náhodne, alebo ako výsledok analýz v procese štandardnej prevádzky informačných systémov, ktoré môžu identifikovať najmä zamestnanci IT oddelenia;
   - **testovacie procesy** – testovanie softvéru, penetračné testy a iné typy posudzovania a analýzy zraniteľností;
   - **výsledky analýz rizík a bezpečnostných testov** vykonávaných v rámci plánu testovania, alebo náhodne;
   - **projektový manažment** – projektoví manažéri a projektové tímy – najmä identifikované riziká IT projektov;
   - **odporúčania auditu** – riziká a hrozby identifikované v rámci programu interného auditu, alebo zistenia nesúladu konštatované certifikovaným audítorom kybernetickej bezpečnosti;
   - **monitoring** – výstupy automatizovaných monitorovacích systémov prevádzky, resp. bezpečnosti;
   - **incidenty** – záverečné správy o incidentoch, t. j. výstupy poučenia z uskutočneného incidentu;
   - **tretie strany** – notifikácia od externej osoby, resp. organizácie, ktorá je akýmkoľvek spôsobom informovaná o riziku (napr. výrobcovia HW a SW, dodávatelia služieb, konzultačné spoločnosti, klienti, webové fóra, blogy, mailinglisty atď.).
5. Pre SAAVŠ je v samotnej analýze rizík použitá len podmnožina týchto hrozieb, keďže nie všetky sa dajú reálne aplikovať na všetky aktíva.
6. Existencia jednej alebo viacerých hrozieb však sama osebe nekompromituje bezpečnosť daného aktíva. Aby bola narušená bezpečnosť, musí dôjsť k naplneniu hrozby, a to cez zraniteľnosť. Na potreby tejto analýzy rizík sa uvažuje o zraniteľnostiach, ktoré sú prevzaté najmä z medzinárodného štandardu ISO/IEC 27005:2022.
7. Zoznam zraniteľností uvažovaných a použitých v analýze rizík je uvedený v prílohe č. 1 tejto smernice.
8. Hrozba je konštatovaním potenciálnej možnosti. Reálna možnosť, že sa jednotlivá hrozba uplatní, je definovaná ako **dopad** hrozby a **riziko**.

Článok 5
Odhad dopadov a pravdepodobnosti pri naplnení rizika

1. Klasifikácia dopadov na aktíva SAAVŠ v dôsledku straty dôvernosti, integrity a dostupnosti dát je uvedená v nasledujúcej tabuľke. Úroveň závažnosti dopadov je vyjadrená podľa nasledovných významov do piatich kategórií:

Dopad	Vysvetlenie
Zanedbateľný	dopad akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov;

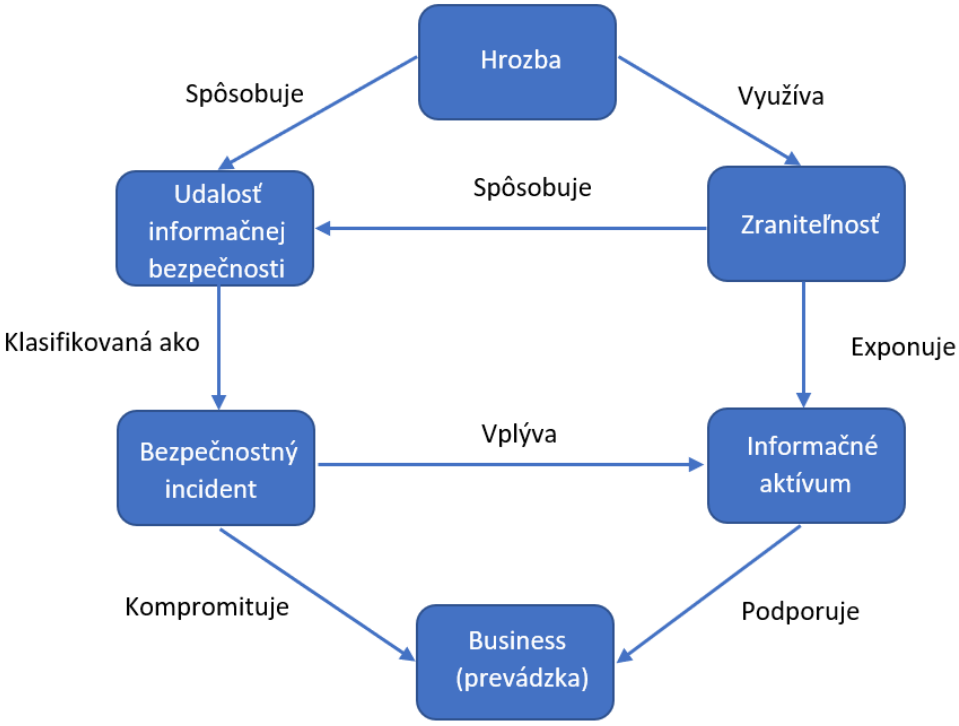
Minimálny	dopad neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi;
Stredný	dopad neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje mimoriadne personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu);
Závažný	prerušenie výkonu určitej konkrétnej 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;
Katastrofický	zásadné ohrozenie výkonu a funkčnosti primárnych procesov, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej agentúry.

2. Určenie pravdepodobnosti naplnenia hrozby je nutnou požiadavkou na vyhodnotenie rizika danej hrozby. Pri určovaní pravdepodobnosti sa vychádza z predpokladaného naplnenia danej hrozby v časovom horizonte dvoch rokov. V analýze rizík je táto pravdepodobnosť vyjadrená nasledujúcim rozsahom:

Pravdepodobnosť	Vysvetlenie
Vysoká	je takmer isté, že v dohľadnom čase nastane naplnenie danej hrozby;
Stredná	je pravdepodobné, že v dohľadnom čase nastane naplnenie danej hrozby;
Nízka	je možné, že v dohľadnom čase nastane naplnenie danej hrozby;
Veľmi nízka	je nepravdepodobné, že by v dohľadnom čase malo nastať naplnenie danej hrozby.

Článok 6
Identifikácia rizík a určenie úrovne rizika

1. **Riziko** je funkcia pravdepodobnosti, že hrozba (potenciálna príčina nechceného) využije známu alebo neznámu zraniteľnosť, pričom jej následkom nastane udalosť, typicky prinášajúca nežiaduci dopad na aktíva. Norma ISO/IEC 27000 definuje riziko relatívne jednoducho ako „účinok neistoty na ciele“.
2. Vzťahy logických objektov z pohľadu rizika vzniku incidentu prehľadne zobrazuje graf z medzinárodnej normy ISO/IEC 27035-1:2016 Informačné technológie – Bezpečnostné metódy – Manažment incidentov v inf. bezp.– Časť 1: Princípy manažmentu incidentov:



3. Výsledné riziko sa určuje ako kombinácia pravdepodobnosti naplnenia scenára rizika a závažnosti „najhoršieho“ dopadu. Pri určovaní výsledného rizika sa vychádza z nasledujúcej tabuľky.
4. Matica určenia úrovne výsledného rizika kvalitatívnou metódou:

		Dopad				
		Zanedbateľný	Minimálny	Stredný	Závažný	Katastrofický
Pravdepodobnosť	Vysoká	C	B	B	A	A
	Stredná	C	C	B	B	A
	Nízka	D	C	C	B	B
	Veľmi nízka	D	D	C	C	C

5. Klasifikácia závažnosti rizika pri použití kvalitatívnej metódy vyplýva priamo z matice pre určenie úrovne výsledného rizika. Ohodnotenie závažnosti rizík je vyjadrené stupňom podľa nasledovných významov:

Úroveň závažnosti	Skratka	Slovný opis
Mimoriadne vysoká	A	riziko bezprostredne ohrozuje poskytovanie základnej služby, bezpečnosť agentúry, resp. kritického procesu, alebo systému (typicky prekročenie stanoveného limitu tolerancie rizika, katastrofálna finančná strata alebo škoda na majetku, dopady na zdravie a život, dopad na životné prostredie atď.);

Vysoká	**B**	riziko potenciálne ohrozuje poskytovanie základnej služby, bezpečnosť agentúry, resp. kritického procesu alebo systému;
Nízka	**C**	riziko neohrozuje poskytovanie základnej služby, ohrozuje výkon niektorých podporných procesov. Kritické procesy alebo systémy však nie sú rizikom ohrozené;
Zanedbateľná	**D**	riziko neohrozuje poskytovanie základnej služby, výkon procesov a prevádzka systémov nie sú rizikom ohrozené.

Článok 7
Prístupy k ošetrovaniu rizika

1. Pri prijímaní opatrení na sa zohľadňujú nasledovné štyri typy prístupu k riziku:
   - **Zníženie rizika**
     Zníženie rizika je najčastejšou metódou ošetrenia rizika. Uplatnený je výber vhodných opatrení tak, aby riziko bolo znížené až na úroveň zvyškového rizika (úroveň D – zanedbateľné riziko), ktoré môže byť následne prehodnotené ako akceptovateľné. Zníženie rizika je možné dosiahnuť pomocou vhodných opatrení na zníženie následkov rizika alebo na zníženie pravdepodobnosti realizácie rizika.
   - **Vyhnutie sa riziku**
     Keď je identifikované riziko považované za príliš vysoké alebo náklady na implementáciu ošetrenia rizika presahujú prínosy, je možné aj úplné vyhnutie sa riziku, a to nevykonaním plánovanej alebo existujúcej aktivity alebo súboru aktivít, resp. zmenou podmienok, podľa ktorých bude činnosť vykonávaná.
   - **Presun rizika**
     Presun rizika je metóda ošetrenia rizika, pri ktorej bude určitá časť následkov rizika zdieľaná s externými subjektmi. Typickým presunom rizika je poistenie, alebo výber zmluvného partnera, ktorého úlohou bude monitorovať proces a prijať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda.
   - **Zachovanie rizika**
     Ak úroveň rizika spĺňa kritériá na akceptáciu rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované v pôvodne ohodnotenej úrovni.

Článok 8
Návrh bezpečnostných opatrení

1. Riziká sú ošetrované v poradí od najvyšších (najkritickejších) po najnižšie. Bezpečnostné opatrenia musia byť preto prijímané v závislosti na stanovenej úrovni rizika podľa tabuľky nižšie:

Úroveň závažnosti	Skratka	Opatrenia
Mimoriadne vysoká	**A**	Rozšírené a dodatočné bezpečnostné opatrenia sú bezpodmienečne nutné a je nutné prijať ich bezodkladne. Výkon kľúčových procesov a ďalšia prevádzka systému je podmienená prijatím opatrení.

Vysoká	**B**	Rozšírené a dodatočné bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dohľadnej dobe, ktorú určí vlastník rizika. Výkon kľúčových procesov ani prevádzka systému sa nepovažujú za akútne ohrozené.
Nízka	**C**	Vlastník aktíva musí stanoviť, či je nutné prijať rozšírené bezpečnostné opatrenia, alebo či v minulosti prijaté opatrenia sú ešte potrebné. Riziko je možné akceptovať ako prijateľné len v prípade, že boli prijaté rozšírené bezpečnostné opatrenia.
Zanedbateľná	**D**	Nie je nutné prijať dodatočné ani rozšírené bezpečnostné opatrenia. Riziko je možné akceptovať ako prijateľné.

2. Návrh bezpečnostných opatrení vychádza z nasledovných princípov:
   - pri návrhu opatrení sa vychádza z hodnoty a charakteru výsledného rizika určeného podľa metodiky,
   - pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho ošetrenia pomocou navrhovaných bezpečnostných opatrení,
   - opatrenia sú navrhované v kontexte identifikovaných hrozieb,
   - cieľom je navrhnúť systém bezpečnostných opatrení takým spôsobom, aby po ich implementácii boli všetky riziká znížené na úroveň zodpovedajúcu akceptovateľným rizikám.
3. Typy opatrení v kontexte životného cyklu informačného aktíva:
   - **existujúce opatrenia** – opatrenia inherentne zabudované už v čase návrhu, resp. implementácie systému;
   - **rozšírené opatrenia** – aplikované na implementovaný systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému;
   - **dodatočné opatrenia** – odporúča ich typicky audítor v správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu kybernetickej bezpečnosti.
4. Z hľadiska realizácie opatrení na zníženie rizika je potrebné opatrenia rozdeliť na:
   - **Operatívne** – t. j. opatrenia, ktorých implementácia je z časového a finančného hľadiska nenáročná, ale účinok ktorých prináša bezprostredný efekt na zníženie rizika. Cieľom operatívnych opatrení je uplatnenie takých zmien procesov a technológií, ktoré budú viesť k urýchlenému zníženiu identifikovaného rizika s čo najnižšími nákladmi a najvyšším účinkom.
   - **Systémové** – t. j. organizačné a rozsiahlejšie technické opatrenia s dlhodobým účinkom na znižovanie rizika. Cieľom systémových opatrení je zvoliť optimálnu hranicu medzi účinnosťou bezpečnostných mechanizmov a požiadavkami, ktoré sú kladené na prevádzku aktív. Výsledkom systémových opatrení musí byť proaktívny prístup k riadeniu rizika, ktoré umožní:
     - identifikovať riziko v počiatočnom štádiu pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
     - monitorovať riziko počas pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
     - eliminovať dopad hrozby na funkčnosť IS,
     - zdokumentovať priebeh rizika.

Článok 9
Akceptácia zvyškového rizika

1. Zvyškové je také riziko, ktorého hodnota po komplexnom ošetrení rizík implementáciou pôvodných, dodatočných a rozšírených opatrení je taká nízka, že je pre organizáciu prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.
2. Výsledné riziko môže byť v rámci analýzy rizík označené ako akceptovateľné len za

predpokladu splnenia nasledovných podmienok:
- pravdepodobnosť realizácie rizika je príliš nízka,
- straty spôsobené realizáciou rizika sú nepatrné,
- realizácia rizika výrazne nenaruší stanovenú/očakávanú úroveň bezpečnosti,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie sú nákladnejšie ako prípadné straty,
- opatrenia minimalizujúce pravdepodobnosť jeho realizácie výrazne prevyšujú štandardnú úroveň bezpečnosti v prostredí nasadenia,
- pri presune rizika na iný subjekt.

3. Referenčná hodnota zvyškového rizika je stanovená ako úroveň **D – zanedbateľná úroveň** závažnosti rizika.
4. Akceptácia zvyškového rizika je proces, v ktorom štatutárny orgán agentúry alebo štatutárnym orgánom agentúry poverený organizačný útvar formálne odsúhlasí zvyškové riziko.
5. Návrh na akceptáciu rizika sa predkladá vo formáte, ktorý obsahuje všetky informácie potrebné na rozhodnutie o akceptácii, a to najmä:
   - momentálny stav ošetrenia rizika,
   - opis rizika,
   - pravdepodobnosť,
   - dopad,
   - použitá metóda na ošetrenie rizika,
   - postup ošetrenia rizika (čo sa spravilo doteraz a aký je ďalší postup).
6. Všetky akceptované riziká musia byť prehodnocované minimálne raz ročne, a to až do doby, pokiaľ riziko neprestane byť relevantné alebo sa nepristúpi k inému spôsobu ošetrenia identifikovaného a trvajúceho rizika.

Článok 10
Záverečné ustanovenia

1. Táto metodika analýzy rizík informačnej bezpečnosti SAAVŠ nadobúda platnosť a účinnosť dňom jej schválenia výkonnou radou dňa 20. júna 2024.

V Bratislave 20. júna 2024

p**rof. Ing. Robert Redhammer, PhD.**
predseda výkonnej rady

Prílohy:
Príloha č. 1: Analýza_rizík_informačnej_bezpečnosti.xlsx – CHRÁNENÝ OBSAH