

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôverynosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Fyzické hrozby	TP01	1.1	Oheň	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) požiarom		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP06	1.2	Prach, korózia, mrazy	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) prachom, mrazom, koróziou		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP04	1.3	Veľká nehoda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu vplyvu okolitých blízkych udalostí (napríklad únik radiácie, požiar vedľajšej budovy, chemické znečistenie, výbuch v blízkosti, dopravná nehoda, letecká nehoda) vrátane ďalších dôsledkov vyplývajúcich z udalosti - cestné uzávery, zákaz vychádzania a podobne		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP02	1.4	Voda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) záplavou, vytopením, typicky vodoinštalačnou haváriou.		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP05	1.5	Výbuch	Áno	Áno	Áno	Premyselná havária, bombový útok, teroristické útoky, vojna, použitie zbraní		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP03	1.6	Znečistenie, škodlivé žiarenie	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) znečistením alebo škodlivým elektromagnetickým žiarením		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby		1.7	Zničenie zariadenia, alebo médií	Áno	Áno	Áno	Zničenie zariadení, alebo médií napr. vodou, požiarom, vandalizmus, zlyhanie úložného zariadenia, atď.		Áno	Áno	ISO/IEC 27005:2011
Hospodárske a ekonomické hrozby		2.1	Chybný rozpočet	Áno	Áno		Nedostatky finančného rozpočtu			Áno	
Hospodárske a ekonomické hrozby		2.2	Energetická závislosť	Áno		Áno	Nediverzifikovaná závislosť na jednom dodávateľovi energie, resp. zdrojov na jej výrobu		Áno	Áno	
Hospodárske a ekonomické hrozby		2.3	Narušenie hospodárstva štátu		Áno		Narušenie alebo obmedzenie menového, devízového a finančného hospodárstva		Áno	Áno	
Hospodárske a ekonomické hrozby		2.4	Ekonomické ovplyvňovanie tretej strany		Áno		Politické riziko tretej strany vzhľadom na analýzu vlastnickej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany	Áno		Áno	ZoKB 20/5c
Informačné operácie		3.1	Šírenie propagandy		Áno		Úmyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.2	Vytvorenie dezinformácií		Áno		Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.3	Zdieľanie dezinformácií		Áno		Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Kompromitácia funkcií alebo služieb	TC01	4.1	Chyba pri používaní	Áno			Nechcená modifikácia údajov v databázach, zmazanie súborov, potrebných pre chod softvéru, chyba operátora, ktorý modifikuje údaje, vysoké pracovné zaťaženie, stres alebo negatívne zmeny pracovných podmienok, zadanie úlohy nad rámec schopností zamestnanca, slabé znalosti a zručnosti, atď.		Áno	Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.2	Chyby prenosu (vrátane nesprávneho smerovania správ)		Áno		Reorganizácia prenosových kanálov elektronických, alebo materializovaných údajov; zmena pracovného jazyka, zmeny v doručovaní pošty, úprava alebo presmerovanie správ, atď.	Áno	Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC03	4.3	Falšovanie práv alebo povolení		Áno		Neoprávnené pozmeňovanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa			Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb	TC04	4.4	Odmietnutie konania		Áno		Odmietnutie vykonania pracovnej aktivity, odopretie pracovnej zodpovednosti v procese, štrajk, atď.		Áno		ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.5	Odmietnutie služby	Áno	Áno		Narušenie procesov, infraštruktúry alebo iných prvkov za účelom znefunkčnenia služby (typicky DoS, DDoS)		Áno		ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb		4.6	Zhoršovanie stavu pamäťových médií	Áno		Áno	Starnutie archivovaných dokumentov, postupné prepisovanie obsahu v čase, dobrovoľné vymazanie častí dokumentu, zničenie médií napr. pri požiaroch, záplave atď.		Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC02	4.7	Zneužitie práv alebo povolení	Áno	Áno		Neoprávnené získanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa	Áno			ISO/IEC 27005:2022
Ľudské konanie		5.1	Popretie	Áno	Áno		Popretie pôvodu informácie (neoprávnené popretie pravdivej informácie). Tiež stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje zlomyseľnú manipuláciu alebo sfaľšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfaľšovanie identifikácie nepovolených aktivít, vymazanie denníkov alebo zápis nesprávnych údajov do protokolových súborov.			Áno	ISO/IEC 27005:2011
Ľudské konanie	ST26	5.2	Detekcia polohy		Áno		Zistenie údajov o geografickej polohe	Áno			ISO/IEC 27005:2022

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôvernosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Ľudské konanie	TH14	5.3	Infiltrácia webovej komunikácie		Áno		Poškodenie, alebo neoprávnená zmena obsahu, typicky webovej stránky, alebo aplikácie, ktoré môže zmeniť informačný obsah, alebo aj vizuálny vzhľad webovej stránky, alebo aplikácie (tzv. defacement). Hrozba prieniku do cieľového systému prostredníctvom webových aplikácií.	Áno		Áno	ISO/IEC 27005:2022
Ľudské konanie	TH08	5.4	Krádež digitálnej identity alebo prihlasovacích údajov		Áno		Krádež identity a jej zneužitie na podvodné konanie alebo neoprávnený prístup.	Áno			ISO/IEC 27005:2022
Ľudské konanie	TH06	5.5	Krádež médií alebo dokumentov		Áno		Krádež dokumentov, krádež súborov, strata súborov počas sťahovania, krádež emailu z mailboxu, rozmnožovanie dokumentov počas prenosu, nájdenie stratených dokumentov, atď.	Áno			ISO/IEC 27005:2022
Ľudské konanie	TH07	5.6	Krádež zariadenia		Áno		Krádež notebooku, alebo mobilu, strata zariadenia, nájdenie strateného zariadenia, strata úložného zariadenia, atď.	Áno	Áno		ISO/IEC 27005:2022
Ľudské konanie	TH12	5.7	Manipulácia s hardvérom		Áno		Neoprávnená manipulácia s hardvérom, pridanie nekompatibilnej časti zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, sledovanie hardvérovým keyloggerom, odstránenie komponentov zariadenia, pripojenie zariadení (napr. USB diskov) pre štart OS alebo získanie dát, použitie USB kľúčov alebo diskov, ktoré nie sú vhodné pre danú klasifikáciu informácií, použitie alebo prenos citlivých zariadení pre osobné použitie, ukladanie súkromných súborov, osobné použitie atď.	Áno		Áno	ISO/IEC 27005:2022
Ľudské konanie	TH13	5.8	Manipulácia so softvérom	Áno	Áno		Neoprávnená manipulácia so softvérom, nepovolené, neschválené aktualizácie, konfigurácie, výmena komponentov, nelegálne spájanie údajov, nepovolené získanie vyšších oprávnení, mazanie stôp po použití, zneužitie softvérových funkcií, atď.	Áno		Áno	ISO/IEC 27005:2022
Ľudské konanie	TH18	5.9	Neoprávnené používanie zariadení		Áno		Neoprávnený alebo neautorizovaný prístup do systému alebo k zariadeniu, znižovanie zabezpečenia zariadení a služieb	Áno			ISO/IEC 27005:2022
Ľudské konanie	TH16	5.10	Neoprávnené spracúvanie osobných údajov	Áno	Áno		Neoprávnené poskytnutie, sprístupnenie alebo zverejnenie osobných údajov o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo získaných v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie	Áno			ISO/IEC 27005:2022
Ľudské konanie	TH17	5.11	Neoprávnený vstup do priestorov		Áno		Neoprávnený fyzický vstup do priestorov	Áno			ISO/IEC 27005:2022
Ľudské konanie	TH19	5.12	Nesprávne používanie zariadení	Áno	Áno		Porušenie politík alebo návodov na bezpečné používanie zariadenia			Áno	ISO/IEC 27005:2022
Ľudské konanie	TH24	5.13	Nezákonné spracovanie údajov		Áno		Neoprávnená manipulácia s informáciami			Áno	ISO/IEC 27005:2022
Ľudské konanie	TH25	5.14	Odosielanie alebo distribúcia malvéru	Áno	Áno	Áno	Infiltrácia škodlivým kódom, výmaz spúšťačích súborov alebo zdrojového kódu, atď.	Áno	Áno	Áno	ISO/IEC 27005:2022
Ľudské konanie	TH05	5.15	Odpočúvanie		Áno		Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky, GPS sledovanie zariadenia, vzdialená detekcia elektromagnetického signálu, (vrátane analýzy dátovej prevádzky) atď.	Áno			ISO/IEC 27005:2022
Ľudské konanie	ST21	5.16	Podvodné kopírovanie softvéru		Áno		Neoprávnená manipulácia so softvérom vedúca k nepovolenému neschválenému kopírovaniu kódu, prípadne až ku odcudzeniu kódu.			Áno	ISO/IEC 27005:2022
Ľudské konanie		5.17	Poškodenie reputácie				Poškodenie reputácie úmyselným konaním (klebety, ohováranie, dezinformácie, dehonestácia predstaviteľov organizácie, poškodzovanie dobrého mena atď.)	Áno		Áno	ISO/IEC 27005:2011
Ľudské konanie	ST23	5.18	Poškodenie údajov		Áno		Zmena, alebo zničenie údajov, zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia autora, odosielanie viacerých konfliktných dokumentov, manipulácia alebo zmena s informáciou, ktorá znamená narušenie jej integrity.			Áno	ISO/IEC 27005:2022
Ľudské konanie	TH20	5.19	Poškodenie zariadení alebo médií	Áno	Áno		Úmyselné poškodenie zariadení, alebo médií, narušenie integrity zariadenia alebo média.			Áno	ISO/IEC 27005:2022
Ľudské konanie	ST22	5.20	Používanie falošného alebo skopírovaného softvéru	Áno	Áno		Použitie nelegálneho, falošného alebo nelicencovaného softvéru. Tento je typicky upravený tak, aby obsahoval malvér ohrozujúci počítačový systém	Áno	Áno	Áno	ISO/IEC 27005:2022
Ľudské konanie		5.21	Používanie sieťových zariadení neoprávneným spôsobom		Áno		Skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď.	Áno		Áno	ISO/IEC 27005:2011
Ľudské konanie		5.22	Prístup neoprávneného používateľa k sieti		Áno		Skenovanie sieťových adries a portov, hľadanie zraniteľností pri počúvaní, analýze, reportovaní alebo sprostredkovaní porty a služby	Áno			ISO/IEC 27005:2011
Ľudské konanie	TH02	5.23	Sociálne inžinierstvo		Áno		Zneužitie práv, ovplyvňovanie (phishing, sociálne inžinierstvo, podplácanie, a pod.), nátlak (výhrážne emaily, psychologické obťažovanie) atď.	Áno			ISO/IEC 27005:2022

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôverynosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Ludské konanie	TH01	5.24	Teroristický útok, sabotáž		Áno		Úmyselná manipulácia alebo poškodenie fyzických objektov, zariadení a/alebo procesov alebo obmedzenie funkcií z dôvodu sabotáže, alebo teroristického útoku, za účelom spôsobenia škody		Áno		ISO/IEC 27005:2022
Ludské konanie	TH15	5.25	Útok man-in-the-middle		Áno		Typ hrozby počas ktorej útočník prenikne do komunikácie medzi dvoma účastníkmi a bez ich vedomia začne komunikáciu neoprávnenne modifikovať	Áno		Áno	ISO/IEC 27005:2022
Ludské konanie	TH11	5.26	Vstup údajov z nedôveryhodných zdrojov	Áno	Áno		Údaje získané z nedôveryhodných zdrojov, kompromitácia údajov, atď. (Např. prezenčná listina bez súhlasov, používanie mailinglistu s neoprávnené získanými, alebo chybnými adresami)			Áno	ISO/IEC 27005:2022
Ludské konanie	TH04	5.27	Vzdialené špehovanie		Áno		Špehovanie sieťovej prevádzky, získavanie dát posielaných cez rádiové frekvenčné siete, maskovanie identity, sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu, výmena pôvodných komponentov, atď.	Áno			ISO/IEC 27005:2022
Ludské konanie	TH03	5.28	Zachytenie žiarenia zariadenia		Áno		Sledovanie GPS signálu zariadenia, vzdialená detekcia elektromagnetického vyžarovania zariadenia, vrátane analýzy dátovej prevádzky atď.	Áno			ISO/IEC 27005:2022
Ludské konanie	TH09	5.29	Zber recyklovaných alebo vyradených médií		Áno		Nedostatočné zmluvy o vyradení a údržbe zariadení, resp. nedostatočné, alebo chybné opodredujú vyradenia a údržby môžu viesť k neoprávnenému prístupu k informáciám	Áno			ISO/IEC 27005:2022
Ludské konanie	TH10	5.30	Zverejňovanie informácií	Áno	Áno		Neoprávnené zverejnenie informácií v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup	Áno			ISO/IEC 27005:2022
Medzinárodné vzťahy		6.1	Neplnenie záväzkov EÚ		Áno		Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s EÚ, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách			Áno	ZoKB 20/5a
Medzinárodné vzťahy		6.2	Neplnenie záväzkov NATO		Áno		Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s NATO, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách			Áno	ZoKB 20/5a
Medzinárodné vzťahy		6.3	Neplnenie záväzkov OSN		Áno		Neplnenie alebo obmedzené plnenie záväzkov zo zmlúv s OSN, ktorými je Slovenská republika viazaná, alebo obmedzovanie členstva v medzinárodných organizáciách			Áno	ZoKB 20/5a
Obrana štátu		7.1	Asymetrické útoky		Áno		Asymetrická (rozvratná, sabotážna a spravodajská) aktivita voči Slovenskej republike	Áno	Áno	Áno	
Obrana štátu		7.2	Obmedzenie mobilizácie		Áno		Obmedzenie, alebo znemožnenie procesu mobilizácie		Áno	Áno	
Obrana štátu		7.3	Obmedzenie prípravy obrany štátu		Áno		Znemožnenie alebo obmedzenie prípravy obrany štátu v podobe ľudského, materiálneho a organizačného charakteru		Áno	Áno	
Obrana štátu		7.4	Obmedzenie vojenských operácií		Áno		Obmedzenie alebo znemožnenie vykonávania vojenských operácií		Áno	Áno	
Organizačné hrozby		8.1	Chybné plánovanie a nedostatky v adaptácii	Áno	Áno		Zanedbanie bezpečnostných požiadaviek pri plánovaní, nákupe a implementácii zariadení, služieb a procesov			Áno	
Organizačné hrozby	TO01	8.2	Nedostatok personálu	Áno		Áno	Preloženie, ukončenie kontraktu alebo zrušenie, prevzatie firmy alebo jej časti, prevzatie zamestnanca, zmena zariadenia, ukončenie procesu po organizačnej zmene, doručenie pošty zrušené štrajkom, pracovný úraz, choroba z povolania, iné zranenie alebo choroba, smrť, neurologická, psychologická alebo psychiatrická diagnóza, atď. atď.		Áno		ISO/IEC 27005:2022
Organizačné hrozby	TO02	8.3	Nedostatok zdrojov	Áno		Áno	Nedostatok alebo nesprávne riadenie finančných, technických alebo personálnych zdrojov		Áno		ISO/IEC 27005:2022
Organizačné hrozby		8.4	Porušenie interných riadiacich aktov	Áno	Áno		Nesúlad s platnými porušeniami internými riadiacimi aktami vyúsťujúce do potenciálneho incidentu			Áno	
Organizačné hrozby	TO04	8.5	Porušenie zákonov alebo nariadení	Áno	Áno		Nesúlad s platnou reguláciou, porušenie zákona vyúsťujúce do trestno-právnej, správno-právnej alebo inej právnej konzekvencie			Áno	ISO/IEC 27005:2022
Organizačné hrozby	TO03	8.6	Zlyhanie poskytovateľov služieb	Áno		Áno	Prerušenie outsourcovaných služieb, např. dodávky plynu, elektrickej energie, telekomunikačných služieb, vody, ventilácie atď.		Áno		ISO/IEC 27005:2022
Poruchy infraštruktúry	TI06	9.1	Elektromagnetická radiácia	Áno	Áno	Áno	Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením, radiáciou			Áno	ISO/IEC 27005:2022
Poruchy infraštruktúry	TI08	9.2	Elektromagnetické impulzy	Áno	Áno	Áno	Poškodenie údajov (typicky na nosičoch) elektromagnetickými impulzmi, resp. kolísaním napájania			Áno	ISO/IEC 27005:2022
Poruchy infraštruktúry	TI02	9.3	Porucha chladiaceho alebo ventilačného systému	Áno	Áno		Porucha klimatizácie alebo prívodu vody ktoré môže spôsobiť výpadky systémov a následne zníženie úrovne dostupnosti údajov		Áno		ISO/IEC 27005:2022
Poruchy infraštruktúry	TI01	9.4	Porucha napájacieho systému	Áno	Áno		Narušenie alebo poškodenie energetickej infraštruktúry		Áno		ISO/IEC 27005:2022

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôverynosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Poruchy infraštruktúry	TI05	9.5	Porucha telekomunikačného zariadenia	Áno	Áno		Zlyhanie telekomunikačných komponentov, prerušenie kabeľáže, slabý telekomunikačný signál, nedostatočný signál Wi-Fi, atď.		Áno		ISO/IEC 27005:2022
Poruchy infraštruktúry	TI04	9.6	Porucha telekomunikačnej siete	Áno	Áno	Áno	Poškodenie telekomunikačného spojenia, zničenie kabeľáže, výpadok komponentov optického spojenia, nedostupné WiFi pripojenie, atď.		Áno		ISO/IEC 27005:2022
Poruchy infraštruktúry	TI03	9.7	Strata napájania	Áno	Áno	Áno	Obmedzená alebo zastavená dodávka energií resp. zdrojov na jej výrobu		Áno		ISO/IEC 27005:2022
Poruchy infraštruktúry	TI07	9.8	Tepelné žiarenie	Áno	Áno	Áno	Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou			Áno	ISO/IEC 27005:2022
Prírodné hrozby	TN01	10.1	Klimatický jav			Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu klimatického javu - tornádo, záplava, zosuv pôdy, lavína, lesný požiar		Áno	Áno	ISO/IEC 27005:2022
Prírodné hrozby	TN04	10.2	Meteorologický jav			Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) mrázom, vysokou teplotou, vetrom, vlhkosťou, bleskom			Áno	ISO/IEC 27005:2022
Prírodné hrozby	TN06	10.3	Pandémia/epidemický jav			Áno	Rozsiahla epidémia, nemoc, ktorá ktorá sa rozširuje na geograficky rozsiahlom území a spôsobuje typicky nedostupnosť personálu		Áno		ISO/IEC 27005:2022
Prírodné hrozby		10.4	Poškodenie zvieratám	Áno		Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) zvieratami		Áno	Áno	ISO/IEC 27005:2011
Prírodné hrozby	TN05	10.5	Povodeň			Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) povodňou		Áno	Áno	ISO/IEC 27005:2022
Prírodné hrozby	TN02	10.6	Seizmický jav			Áno	Poškodenie (typicky priestorov, nosičov údajov, alebo IT zariadení) zemetrasením, alebo inými seizmickými udalosťami		Áno	Áno	ISO/IEC 27005:2022
Prírodné hrozby	TN03	10.7	Sopečný fenomén			Áno	Poškodenie (typicky priestorov, nosičov údajov, alebo IT zariadení) vulkanickými udalosťami		Áno	Áno	ISO/IEC 27005:2022
Štátna nezávislosť a rozhodovanie		11.1	Obmedzenie rozvoja		Áno		Obmedzenie alebo znemožnenie politického, ekonomického, sociálneho a vojenského rozvoja Slovenskej republiky			Áno	
Štátna nezávislosť a rozhodovanie		11.2	Špionáž		Áno		Zhromažďovanie, vyhodnocovanie a spracovanie informácií neoprávneným spôsobom, v neprospech štátneho zriadenia	Áno			ISO/IEC 27005:2011
Štátna nezávislosť a rozhodovanie		11.3	Negatívne spravodajské informácie		Áno		Hrozby vyplývajúce z informácií špecifických pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky	Áno			ZoKB 20/5e
Štátna nezávislosť a rozhodovanie		11.4	Strata slobody rozhodovania		Áno		Strata slobody rozhodovania a konania na strategickom, operačnom a taktickom stupni štátu zo strany predstaviteľov verejnej moci			Áno	
Štátna nezávislosť a rozhodovanie		11.5	Znemožnenie presadzovania záujmov		Áno		Znemožnenie presadzovania záujmov (národno-štátnych, organizačných) na medzinárodnej úrovni			Áno	
Štátna nezávislosť a rozhodovanie		11.6	Ovplyvňovanie a zasahovanie do činnosti tretej strany cudzím štátom		Áno		Možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“)			Áno	ZoKB 20/5b
Súkromie		12.1	Detekovateľnosť	Áno	Áno		(1) Potenciál, že útočník dokáže z uložených údajov dostatočne rozlíšiť, či predmet záujmu, resp. položka množiny jestvuje alebo nie. (napr. schopnosť rozpoznania súborov obsahujúcich osobné údaje od iných typov údajov)	Áno			LINDDUN: a privacy threat analysis framework
Súkromie		12.2	Identifikovateľnosť	Áno	Áno		(3) Potenciál, že útočník dokáže priamo identifikovať dotknuté osoby asociované na predmety záujmu (napr. v súbore osobných údajov rozpoznať osobné údaje konkrétnej dotknutej osoby. napr. konkrétneho odosielateľa správy medzi mnohými správami elektronickej pošty). Identifikovateľnosť je špeciálny typ spojitosti, kde sú zahrnuté aj atribúty dotknutých osôb.	Áno			LINDDUN: a privacy threat analysis framework
Súkromie		12.3	Nepopierateľnosť	Áno	Áno		Potenciál, že útočník dokáže z podstaty procesu zhromaždiť dôkazy proti nároku odporujúcej strany a dokázať, že používateľ vie, že niečo urobil, alebo že niečo povedal. Opakom je Plausible deniability (tzv. prijateľné popretie) . (T.j. neoprávnené zverejňovanie pravdivých informácií, resp. pôvodu informácie - napr. dotknutá osoba nechce, aby bolo jasné, komu dala hlas vo voľbách do DR, avšak útočník túto informáciu zverejní)	Áno			LINDDUN: a privacy threat analysis framework
Súkromie		12.4	Nesúlad s právnym základom	Áno	Áno		Nesúlad spracovania s politikami a právnym základom (napr. poskytnutým súhlasom) je hrozba, ktorá znamená, že napriek deklarácii súladu spracovania s politikami, neexistuje záruka, že systém skutočne vyhovuje prijatým pravidlám. Tým následne môže nastať porušenie práv dotknutej osoby.			Áno	LINDDUN: a privacy threat analysis framework

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôvernosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Súkromie		12.5	Neznalosť klasifikácie	Áno	Áno		Neznalosť klasifikácie je hrozba, ktorá indikuje, že používateľ si neuvedomuje citlivosť, resp. klasifikačný stupeň informácie spracovanej v systéme a následne napr. zverejňuje informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie. (napr. nechcené prezradenie informácií)	Áno		Áno	LINDDUN: a privacy threat analysis framework
Súkromie		12.6	Neznalosť obsahu	Áno	Áno		Neznalosť obsahu je hrozba, ktorá indikuje, že používateľ si neuvedomuje obsah informácie spracovanej v systéme a následne napr. zverejňuje nadbytočné informácie, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie. (napr. nechcené prezradenie informácií)	Áno			LINDDUN: a privacy threat analysis framework
Súkromie		12.7	Neoprávnené sprístupnenie	Áno	Áno		Neoprávnené sprístupnenie osobných údajov v rozpore bezpečnostnými opatreniami prijatými na základe klasifikácie informácií, osobám, ktoré k nim nemajú mať prístup. (Neoprávnené prečítanie, kopírovanie, fotografovanie, použité odpočúvacích zariadení na stretnutiach, atď.)	Áno			LINDDUN: a privacy threat analysis framework
Súkromie		12.8	Spojiteľnosť, linkovateľnosť	Áno	Áno		(2) Spojiteľnosť (linkovateľnosť) je hrozba, že útočník dokáže aj nepriamo rozpoznať podstatu entity, alebo vzájomné vzťahy entít. (napr. odosielateľa podľa domény, aktivity, alebo podľa predmetu správy)	Áno			LINDDUN: a privacy threat analysis framework
Technické poruchy		13.1	Porucha softvéru	Áno	Áno		Chyby počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď.		Áno	Áno	ISO/IEC 27005:2011
Technické poruchy	TT01	13.2	Porucha zariadenia alebo systému	Áno			Náhle a neplánované zlyhanie alebo porucha IT zariadenia, alebo akéhokoľvek HW komponentu, ktoré môže spôsobiť zníženie úrovne dostupnosti údajov		Áno		ISO/IEC 27005:2022
Technické poruchy		13.3	Strata napájania alebo kolísanie výkonu	Áno	Áno	Áno	Strata zdroja napájania alebo kolísanie výkonu napájania zariadení		Áno		ISO/IEC 27005:2011
Technické poruchy	TT02	13.4	Zahltie informáčného systému	Áno	Áno		Plná úložná jednotka, výpadok el.energie, preťaženie systému, prehriatie, výnimočné teploty, atď.		Áno		ISO/IEC 27005:2022
Technické poruchy	TT03	13.5	Zníženie úrovne údržby, chyba údržby informačného systému	Áno	Áno		Neplánované zníženie úrovne údržby systémom, chyba údržby informačného systému, alebo IT zariadení		Áno		ISO/IEC 27005:2022
Štátna nezávislosť a rozhodovanie		11.7	Negatívne informácie z analýzy právnych predpisov cudzieho štátu		Áno		Politické riziko tretej strany vzhľadom na analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií	Áno		Áno	ZoKB 20/5d
Územná celistvosť a nedotknuteľnosť hraníc		14.1	Strata kontroly nad územím		Áno		Strata kontroly na časťou, alebo celým územím Slovenskej republiky			Áno	
Územná celistvosť a nedotknuteľnosť hraníc		14.2	Strata obyvateľstva		Áno		Strata obyvateľstva v dôsledku vojenských aktivít alebo iných aktivít porušujúcich medzinárodné právo			Áno	
Územná celistvosť a nedotknuteľnosť hraníc		14.3	Strata zdrojov		Áno		Strata kritických prírodných, potravinových, hospodárskych, infraštruktúrnych, energetických a dopravných zdrojov a spôsobilostí Slovenskej republiky		Áno	Áno	
Verejný poriadok		15.1	Destabilizácia		Áno		Destabilizácia a narušenie chodu orgánov verejnej moci		Áno	Áno	
Verejný poriadok		15.2	Poškodenie zdravia obyvateľstva		Áno		Poškodenie zdravia a/alebo úmrtie významnej časti obyvateľov v dôsledku narušenia verejného poriadku			Áno	
Verejný poriadok		15.3	Preťaženie dopravy		Áno		Preťaženie kapacity prevádzky - preťaženie pošty, preťaženie procesov overovania, prekročenie veľkosti databázy, vkladanie dát mimo normálny rozsah hodnôt, zneužitie šírky pásma, neoprávnené sťahovanie, strata internetovej konektivity, atď.		Áno		
Verejný poriadok		15.4	Verejné nepokoje		Áno		Verejné nepokoje a protesty, vedúce k narušeniu verejného poriadku na území okresu, kraja, štátu			Áno	
Verejný poriadok		15.5	Významné spoločenské udalosti v okolí		Áno		Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu významných udalostí v okolí, vyvolaných ľudskou činnosťou (športové udalosti, festivaly atď.)		Áno	Áno	