

PŘÍLOHA 14: ZKRATKY A POUŽÍVANÉ POJMY

Používané pojmy

Regulovaná služba je služba, o které tak rozhodl Úřad podle § 6 odst. 2 zákona.¹

Aktivum je cokoliv, co má hodnotu pro jednotlivce nebo organizaci.²

Akceptovatelné riziko je riziko, které je přijatelné pro povinnou osobu a není nutné jej zvládat pomocí dalších bezpečnostních opatření.

Analýza rizik zahrnuje ohodnocení kombinace hrozby a zranitelnosti ve vztahu k aktivům a výpočet finální hodnoty.

Bezpečnost informací je zajištění důvěrnosti, integrity a dostupnosti informací a dat.³

Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.⁴

Citlivé osobní údaje jsou speciální kategorií podle GDPR, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Do kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.⁵

Dostupnost je vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.⁶

Důvěrnost je vlastnost zajišťující, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.⁷

Garant aktiva je bezpečnostní role, která je odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.⁸ Garant aktiva spolupracuje s ostatními osobami zastávajícími bezpečnostní role, především dává relevantní vstupy do hodnocení aktiv a rizik.

¹ § 3 zákona o kybernetické bezpečnosti

² JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

³ § 2 odst. 2 písm. b) zákona o kybernetické bezpečnosti

⁴ § 13 odst. 1 zákona o kybernetické bezpečnosti

⁵ Citlivé osobní údaje | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/>

⁶ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary*. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

⁷ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary*. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

⁸ § 5 odst. 3 vyhlášky

Hodnocení rizik zahrnuje identifikaci rizik, analýzu rizik a vyhodnocení rizik.

Hrozba je jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby.

⁹

Určování rizik zahrnuje určování relevantních kombinací hrozeb a zranitelností s ohledem na aktiva.

Informační systém je funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.¹⁰

Integrita je jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samo-opravnými kódy, redundancí, žurnálováním atd.¹¹

Kritéria pro akceptovatelnost stanovují hranici, kdy mohou být rizika akceptována a kdy je nutné snižovat hodnotu rizika zaváděním bezpečnostních opatření.

Kybernetická bezpečnostní událost je událost, která může vyústit v kybernetický bezpečnostní incident.¹² Jde tedy o situaci, kdy může dojít k narušení kybernetické bezpečnosti a tím ke vzniku kybernetického bezpečnostního incidentu.

Kybernetický bezpečnostní incident je narušení bezpečnosti informací v kybernetickém prostoru,¹³ Jinými slovy dojde k situaci, kdy byla porušena kybernetická bezpečnost.

Metodika hodnocení rizik obsahuje postup k provedení hodnocení rizik včetně stanovení kritérií pro akceptovatelnost.

Need-to-know princip znamená, že informace by měla být dostupná pouze tomu, kdo ji potřebuje vědět v nezbytně nutném rozsahu.

Osobní údaje jsou jakékoli informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam.

⁹ § 2 odst. 2 písm. c) zákona o kybernetické bezpečnosti

¹⁰ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

¹¹ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

¹² § 2 odst. 2 písm. e) zákona o kybernetické bezpečnosti

¹³ § 2 odst. 2 písm. f) zákona o kybernetické bezpečnosti

Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.¹⁴

Plán zvládání rizik je přehledový dokument obsahující:

- popis bezpečnostních opatření pro zvládání rizik,
- cíle a přínosy bezpečnostních opatření pro zvládání rizik,
- určení osoby zajišťující zavedení bezpečnostních opatření pro zvládání rizik,
- předpokládané lidské, finanční a technické zdroje pro zavedení bezpečnostních opatření,
- požadovaný termín zavedení bezpečnostních opatření,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a
- konkrétní způsob realizace bezpečnostních opatření.¹⁵

Podpůrné aktivum je aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby.¹⁶

Povinná osoba je poskytovatel regulované služby (subjekt, který poskytuje službu, o které rozhodl Národní úřad pro kybernetickou a informační bezpečnost jako o regulované službě podle § 6 odst. 2 zákona o kybernetické bezpečnosti). Pro účely tohoto podpůrného materiálu se jedná pouze o poskytovatele regulované služby zařazené v režimu vyšších povinností.¹⁷

Primární aktivum je aktivum v podobě zpracovávané informace nebo poskytované služby.¹⁸

Prohlášení o aplikovatelnosti je přehledový dokument, který obsahuje přehled bezpečnostních opatření požadovaných vyhláškou, a to tak, že uvádí bezpečnostní opatření, která:

- nebyla aplikována, včetně odůvodnění a uvedení případných přijatých náhradních bezpečnostních opatření,
- byla aplikována, včetně způsobu jejich aplikace (plnění).¹⁹

Rizikem je možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a tím způsobí organizaci škodu.²⁰

Řízení aktiv je proces zahrnující vytvoření metodiky pro identifikaci a hodnocení aktiv, samotný proces identifikace a hodnocení aktiv, určení a evidenci vazeb mezi primárními a podpůrnými aktivy, stanovení přípustných způsobů používání aktiv, určení způsobu jejich likvidace a určení a evidování garantů aktiv.

¹⁴ Osobní údaje | GDPR.cz. *GDPR / Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/osobni-udaje/>

¹⁵ § 8 odst. 1 písm. g) vyhlášky

¹⁶ § 2 odst. 1 písm. e) zákona o kybernetické bezpečnosti

¹⁷ § 1 vyhlášky

¹⁸ § 2 odst. 1 písm. d) zákona o kybernetické bezpečnosti

¹⁹ § 8 odst. 1 písm. f) vyhlášky

²⁰ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

Řízení rizik je proces zahrnující hodnocení rizik, zavádění bezpečnostních opatření ke zvládnutí rizik a komunikaci rizik.²¹ Součástí řízení rizik je také vytvoření metodiky hodnocení rizik, vytvoření plánu zvládnutí rizik, prohlášení o aplikovatelnosti a zprávy o hodnocení rizik.

Sdílení informací o riziku zahrnuje informování zainteresovaných stran (stakeholderů), jako jsou např. garanti, výbor pro řízení kybernetické bezpečnosti a další.

Sledování a přezkoumávání rizik zahrnuje monitoring a provádění hodnocení rizik v pravidelných intervalech.

Systém řízení bezpečnosti informací (dále jen „ISMS“) je část systému řízení povinné osoby založená na přístupu k rizikům, zahrnující způsob ustanovení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.²² Často používaná zkratka ISMS vychází z anglického názvu Information Security Management System.

Technickým aktivem se rozumí technický nebo programový prostředek anebo vybavení.²³

TLP je metodika, která určuje, jakým způsobem je možné využívat poskytnuté informace. Více informací viz např. <https://www.first.org/tlp/>.

Výbor pro řízení kybernetické bezpečnosti je definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující organizovanou skupinu tvořenou osobami, které jsou pověřeny celkovým řízením a rozvojem systémů spadajících pod zákon o kybernetické bezpečnosti, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.²⁴

Významná změna každá změna ovlivňující bezpečnost informací, u níž povinná osoba, bez ohledu na již zavedená bezpečnostní opatření, může předpokládat ohrožení bezpečnosti informací. K určení významnosti změny subjekt využije pravidla, postupy a kritéria, které si sám stanoví a budou přiměřená danému konkrétnímu prostředí organizace. Běžně se za významnou změnu může považovat např. změna, která mění funkčnost, konfiguraci, integraci nebo architekturu systému, popřípadě jí může být i změna významného dodavatele nebo urgentní změna.²⁵

Výběr opatření zahrnuje volbu vhodných bezpečnostních opatření, kterými bude snižována hodnota příslušných rizik.

Vyhodnocení rizik zahrnuje porovnání hodnoty rizika s kritérii pro akceptovatelnost a rozhodnutí, zda bude riziko akceptováno nebo bude snižováno zaváděním bezpečnostních opatření.

²¹ § 2 písm. f) vyhlášky

²² § 2 písm. g) vyhlášky

²³ § 2 odst. 2 písm. f) zákona o kybernetické bezpečnosti

²⁴ JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti = Cyber Security Glossary. 6. doplněné a upravené elektronické vydání. Praha, 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>

²⁵ Důvodová zpráva k vyhlášce č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností [online]. Praha: Sbírka zákonů, 2025. Dostupné z: <https://www.zakonyprolidi.cz/media2/file/2508/File77594.pdf>

Zavádění opatření zahrnuje proces implementace bezpečnostních opatření.

Zpráva o hodnocení rizik je dokumentovaným shrnutím závěrů hodnocení rizik.

Zranitelnost je slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito hrozbou.²⁶

Zvládání rizik zahrnuje výběr opatření, vytvoření Plánu zvládání rizik a zavádění opatření.

²⁶ § 2 odst. 2 písm. h) zákona o kybernetické bezpečnosti

Používané zkratky

ACL	Access Control List (Seznam řízení přístupu)
AD	Active Directory (Adresářová služba)
ADSL	Asymmetric Digital Subscriber Line
APT	Advanced Persistent Threat (Pokročilá přetrvávající hrozba)
BIA	Analýza dopadů (Business Impact Analysis)
BYOD	Bring your own device
CCTV	Closed-circuit television (kamerový systém)
CD	Kompaktní disk (Compact Disc)
CERT	Computer Emergency Response Team
CIA	Důvěrnost, Integrita, Dostupnost (Confidentiality, Integrity, Availability)
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
DB	Databáze
DLP	Data Loss Prevention
DMS	Document Management System
DMZ	Demilitarizovaná zóna
DOS / DDOS	Denial of Service / Distributed Denial of Service (kybernetický útok)
DPO	Pověřenec pro ochranu osobních údajů (Data Protection Officer)
DVD	Digitální víceúčelový disk (Digital Versatile Disc)
EDGE	Enhanced Data rates for GSM Evolution
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EOL / EOS	End of Life / End of Service
EPS	Elektrická požární signalizace
EU	Evropská unie
EZS	Elektronický zabezpečovací systém
FW	Firewall

GDPR	General Data Protection Regulation
GPO	Group Policy Object
GPRS	General Packet Radio Service
HA	Vysoká dostupnost (High Availability)
HDD	Pevný disk (Hard Disk Drive)
HMI	Human-Machine-Interface
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
ID	Identifikace (Identification)
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
IS	Informační a komunikační systém
ISMS	Systém řízení bezpečnosti informací (Information Security Management System)
ISZS	Informační systém základní služby
IT	Informační technologie
KB	Kybernetická bezpečnost
KBI	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečnostní událost
KII	Kritická informační infrastruktura
LAN	Lokální síť (Local Area Network)
LTE	Vysokorychlostní technologie Long Term Evolution
MDM	Mobile device management
MFA	Multi-factor Authentication (Vícefázové ověření)
Ministerstvo	Ministerstvo certifikací
MITM	Man-in-the-Middle (kybernetický útok)
MS	Microsoft
MT	Mobilní telefon

NATO	Severoatlantická aliance (North Atlantic Treaty Organization)
NB	Notebook
NDA	Non-Disclosure Agreement (Dohoda o mlčenlivosti)
NGFW	Next Generation Firewall
NIA	Národní identitní autorita
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
OSINT	Open Source Intelligence
PC	Osobní počítač (Personal Computer)
PDCA	Plan, Do, Check a Act
PIM / PAM	Privileged Identity Management / Privileged Access Management
PKI	Public Key Infrastructure
PoA	Prohlášení o aplikovatelnosti
PZTS	Poplachový zabezpečovací a tísňový systém
RAID	Diskové pole (Redundant Array of Inexpensive Disks)
RDP	Remote Desktop Protocol (Protokol vzdálené plochy)
RPO	Recovery point objective
RTO	Recovery time objective
RTP	Risk treatment plan
SIEM	Security Information and Event Management
SLA	Smlouva o úrovni poskytovaných služeb (Service Level Agreement)
SOAR	Security Orchestration, Automation and Response
SPOC	Jednotné kontaktní místo (Single Point of Contact)
SSD	Datové médium (Solid State Drive)
SSL	Secure Sockets Layer
SW	Software
TLP	Traffic Light Protocol
ÚOOÚ	Úřad pro ochranu osobních údajů

URL	Uniform Resource Locator
USB	Universal Serial Bus
VIS	Významný informační systém
VLAN	Virtuální LAN
VPN	Virtual Private Network (Virtuální privátní síť)
Výbor KB	Výbor pro řízení kybernetické bezpečnosti
Vyhláška	Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
VZ	Veřejná zakázka
Wi-Fi	Bezdrátové připojení (Wireless Fidelity)
XSS	Cross-site scripting
Zákon	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
5G	Sítě 5. generace