NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

METODICKÝ MATERIÁL K USNESENÍ Č. 537 Z 9. ČERVENCE 2025 O ZÁKAZU PRODUKTŮ, APLIKACÍ A SLUŽEB DEEPSEEK

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 9. ČERVENCE 2025

VERZE DOKUMENTU: 1.0

1 Účel metodického materiálu

Cílové publikum: vedoucí představitelé úřadů, manažeři kybernetické bezpečnosti, bezpečnostní pracovníci, IT bezpečnostní pracovníci, pracovníci zadávání zakázek

Tento metodický materiál poskytuje praktické pokyny a informace k implementaci zákazu produktů, aplikací, řešení, webových stránek a webových služeb společnosti DeepSeek[1].

2 O usnesení vlády č. 537 Z 9. července 2025 o zákazu produktů, aplikací a služeb DeepSeek

Nařízení vlády vyžaduje, aby ministerstva, úřady a další orgány státní správy nevyužívaly produkty, aplikace, řešení, webové stránky a webové služby (včetně aplikačního programového rozhraní, API) poskytované společností DeepSeek pro výkon svých pravomocí a na zařízeních v majetku státu.

DeepSeek a s ním spjaté produkty, aplikace a služby představují bezpečnostní riziko pro ministerstva, úřady a další orgány státní správy z důvodu:

- Nízkého zabezpečení, které produkty DeepSeek činí zranitelné vůči kybernetickým útokům.
- Ukládání uživatelských dat na serverech v Čínské lidové republice (ČLR) a Ruské federaci (RF) – včetně potenciálně citlivých dotazů a souborů nahraných do produktů společnosti DeepSeek uživateli.
- Podřízení společnosti a produktů legislativě ČLR, která státu umožňuje invazivní přístup k datům a vynucení spolupráce např. ke špionáži proti uživatelům DeepSeek.
- Pravděpodobného napojení mateřské společnosti High-Flyer[2] na Komunistickou stranu Číny.

3 Definice

- **Ministerstva, úřady a další orgány státní správy** – těmito se rozumí všechny orgány státní správy dle § 1 a §
- 2 zákona České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, ve znění pozdějších předpisů, a veškeré jim podřízené úřady.

[1] Celým názvem Hangzhou Deeply Seeking Artificial Intelligence Basic Technology Research Co., Ltd (杭州 深度求索人工智能基础技术研究有限公司).

[2] Celým názvem High-Flyer Quant Investment Management (Ningbo) L.P. (宁波幻方量化投资管理合伙企业).

- **Majetek státu** – hmotná (hardware, konkrétní zařízení) i nehmotná (software, služby) věc, která je ministerstvem, úřadem a dalšími orgány státní správy užívána k výkonu svěřených pravomocí.
- **Produkty, aplikace, řešení, webové stránky a webové služby společnosti DeepSeek** – množina produktů, aplikací a služeb patřících společnosti DeepSeek či kterékoli její předchůdkyni, nástupnické, mateřské, dceřiné nebo přidružené společnosti.[3] (struktura společnosti DeepSeek je blíže popsaná v Příloze 2)
    - Mezi zmíněné produkty, aplikace a služby patří např. DeepSeek App, DeepSeek Chat, DeepSeek Platform, DeepSeek API a jazykové modely s přístupem k internetu (výčet nemusí být kompletní).
    - Tento zákaz nezahrnuje bezpečnostní testování, výzkum a analýzu produktů DeepSeek a také open-source velké jazykové modely DeepSeek, jejichž celý zdrojový kód je k dispozici k nahlédnutí a analýze, v případě, že je model nasazen lokálně bez možnosti komunikovat na servery využívané společností DeepSeek.

4 Doporučení pro identifikaci a odstranění produktů, aplikací a služeb DeepSeek na služebních zařízeních

- **Komunikace se zaměstnanci a dalšími relevantními osobami**– instruujte zaměstnance (a další osoby v pracovněprávním vztahu), aby nahlásili, zda na služebních zařízeních nainstalovali nebo používali produkty, aplikace nebo webové služby DeepSeek, nebo k nim přistupovali.
- **Monitoring síťového provozu a DNS dotazů** – pomocí klíčových slov a domén lze zachytit využívání webových služeb a aplikací DeepSeek v rámci sítě organizace. (viz Příloha 1)
- **Auditování logů z logovacích systémů organizace** – k identifikaci, zda uživatelé přistoupili k produktům, aplikacím či webovým službám DeepSeek, nebo je stáhli či nainstalovali. Nástroje sloužící pro zaznamenávání událostí by měly být nakonfigurovány tak, aby zaznamenávaly používání internetových služeb, včetně navštívených webových stránek a staženého softwaru, a uchovávaly historii instalovaného softwaru.
- **Správa bezpečnostních nástrojů** – software nebo služby sloužící k ochraně informačních a komunikačních systémů, informací a dat. Příklady bezpečnostních nástrojů:
    - **Antivirový software** – nástroje pro nepřetržitou ochranu před škodlivým kódem se běžně používají k identifikaci škodlivých souborů, ale lze je nakonfigurovat tak, aby obecněji identifikovaly specifické typy souborů, včetně aplikací DeepSeek.
    - **Správa koncových zařízení (Endpoint Management)** – software umožňující správu koncových zařízení. Lze jej nastavit pro identifikaci nainstalovaného softwaru.

[3] Pro plnění znění usnesení č. 537 a vyhledávání a zjišťování korporátní struktury společnosti DeepSeek a jejích produktů platí princip přiměřeného úsilí, dle něhož jsou adresáti zmíněného usnesení povinni při plnění zmíněných povinností vynaložit pouze takové úsilí, které po nich lze rozumně požadovat.

    - **Správa mobilních zařízení (Mobile Device Management)** – řešení pro správu mobilních zařízení umožňující případně i zaznamenávání používání specifických webových stránek a softwaru.

- **Aplikace funkcí kybernetické bezpečnosti** – lze využít k detekci používání konkrétních produktů nebo webových služeb. Kyberbezpečnostní funkce mohou vykonávat specializované týmy nebo být součástí běžných IT rolí, zejména v menších organizacích. Tyto funkce zahrnují:
    - **Kontrolu v rámci bezpečnostního dohledového centra (SOC)** – SOC chrání systémy a zařízení a může být využit ke kontrole logů událostí nebo žádostí o změnu nastavení systému.
    - **Threat Hunting** – obvykle proaktivní činnost, která může být použita k prohledání sítí, koncových bodů a datových sad za účelem identifikace použití webových služeb nebo aplikací DeepSeek.

4.1 Odstranění produktů, aplikací a služeb DeepSeek

Mnohé z nástrojů a řešení používaných pro identifikaci použití produktů, aplikací a služeb DeepSeek lze využít i pro jejich následné odstranění:

- **Endpoint administrátorské účty** – účty s endpoint administrátorskými oprávněními mohou využívat vestavěné nástroje systému k odinstalaci softwaru a aplikací.
- **Bezpečnostní nástroje** – software nebo služby pro ochranu technologií, informací a dat. Příklady:
    - **Software pro správu koncových zařízení (Endpoint Management)** – umožňuje správu zařízení, a mohou disponovat možností vzdáleného odinstalování softwaru a aplikací.
    - **Software pro správu mobilních zařízení (Mobile Device Management)** – umožňuje administrátorům odinstalovat software a aplikace ze spravovaných zařízení.

5 Zamezení přístupu a používání

Aby se zabránilo přístupu, měly by subjekty zvážit:

- **Informování zaměstnanců** – upozornění personálu, že nesmí přistupovat k produktům, aplikacím a službám DeepSeek ani je používat, v souladu s tímto nařízením.
- **Organizační opatření** – interní směrnice, politika, pokyn či jiné opatření k nastavení vnitřní politiky organizace, které definuje zákaz přístupu k produktům, aplikacím a službám DeepSeek a případné výjimky.

- **Filtrování webového obsahu** – povolení pouze schválených typů webového obsahu a webů s dobrou reputací a blokování přístupu ke konkrétním doménám a IP adresám DeepSeeku.
- **Konfigurace webových prohlížečů** – prostřednictvím proxy serverů na bránách, které blokují přístup ke specifickým kategoriím webových stránek DeepSeek, typům obsahu a doménám.

Nejrelevantnější strategie pro zamezení instalace jsou:

- **Omezení oprávnění** – zabránění stažení, instalaci a využívání neschválených aplikací pomocí řízení přístupu, práv a oprávnění účtů např. na základě principu least privilege a omezení těchto oprávnění na nezbytně nutné k výkonu náplně práce.
- **Řízení aplikací (Application Control)** – zajištění, že lze instalovat a spouštět pouze schválené aplikace. U mobilních zařízení toto řízení poskytuje software pro správu mobilních aplikací (Mobile Application Management).

6 Přílohy

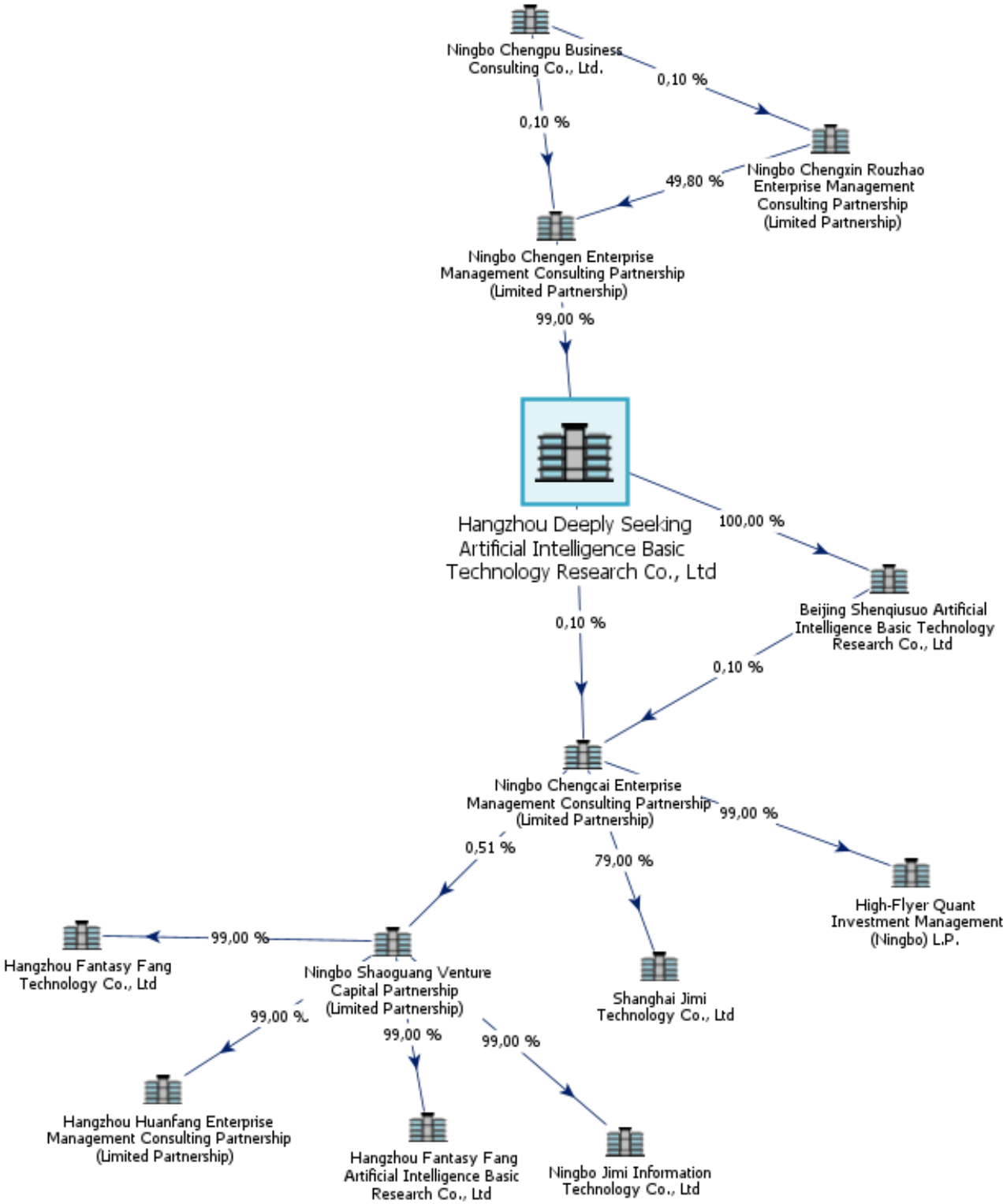
6.1 Příloha 1: doporučení pro monitoring síťového provozu

Příloha je samostatný dokument DeepSeek_indikátory.csv

Nad rámec konkrétních domén lze také využít wildcard filtr:

- *.deepseek.ai
- *.deepseek.com
- *.deepseek.cn

6.2 Příloha 2: struktura společnosti DeepSeek



Název společnosti (EN)	Název společnosti (CN)	Název společnosti (EN)	Název společnosti (CN)
Hangzhou Deeply Seeking Artificial Intelligence Basic Technology Research Co., Ltd	杭州深度求索人工智能基础技术研究有限公司	Ningbo Chengpu Business Consulting Co., Ltd.	宁波程普商务咨询有限公司
Ningbo Chengen Enterprise Management Consulting Partnership (Limited Partnership)	宁波程恩企业管理咨询合伙企业	Hangzhou Fantasy Fang Artificial Intelligence Basic Research Co., Ltd	杭州幻方人工智能基础研究有限公司
Beijing Shenqiusuo Artificial Intelligence Basic Technology Research Co., Ltd	北京深度求索人工智能基础技术研究有限公司	Hangzhou Huanfang Enterprise Management Consulting Partnership (Limited Partnership)	杭州幻方企业管理咨询合伙企业（有限合伙）
Ningbo Chengcai Enterprise Management Consulting Partnership (Limited Partnership)	宁波程采企业管理咨询合伙企业（有限合伙）	High-Flyer Quant Investment Management (Ningbo) L.P.	宁波幻方量化投资管理合伙企业（有限合伙）
Ningbo Chengxin Rouzhao Enterprise Management Consulting Partnership (Limited Partnership)	宁波程信柔兆企业管理咨询合伙企业（有限合伙）	Shanghai Jimi Technology Co., Ltd	上海积幂科技有限公司
Hangzhou Fantasy Fang Technology Co., Ltd	杭州幻方科技有限公司	Ningbo Shaoguang Venture Capital Partnership (Limited Partnership)	宁波少广创业投资合伙企业（有限合伙）
Ningbo Jimi Information Technology Co., Ltd	宁波积幂信息科技有限公司	Wenfeng Liang	梁文锋

7 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol dostupnou na webových stránkách NÚKIB. Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují zásady need-to-know.
TLP: AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují zásady need-to-know.
TLP: GREEN	Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.