NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

МЕТОДИЧНІ МАТЕРІАЛИ ДО ПОСТАНОВИ №. 537 ВІД 9 ЛИПНЯ 2025 РОКУ ПРО ЗАБОРОНУ ПРОДУКТІВ, ДОДАТКІВ ТА ПОСЛУГ ГЛИБОКОГО ПОШУКУ

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

БРНО-9.№2025

МЕТОДИЧНИЙМАТЕРІАЛ:1.0

1 Мета посібника

Цільова аудиторія: вищі державні посадовці, менеджери з кібербезпеки, офіцери з безпеки, офіцери з IT-безпеки, офіцери з питань закупівель

Цей посібник містить практичні рекомендації та інформацію щодо впровадження продуктів, додатків, рішень, веб-сайтів та веб-сервісів DeepSeek у сфері закупівель[1].

2 Щодо Постанови Уряду № 537 від 9 липня 2025 року про заборону продуктів, додатків та послуг компанії DeepSeek

Урядова постанова вимагає від міністерств, відомств та інших державних органів не використовувати продукти, додатки, рішення, веб-сайти та веб-сервіси (включаючи інтерфейси прикладного програмування, API), що надаються компанією DeepSeek, для здійснення своїх повноважень та на об'єктах державної власності.

DeepSeek та пов'язані з нею продукти, додатки та послуги становлять загрозу безпеці міністерств, відомств та інших державних органів через:

- Низький рівень безпеки, що робить продукти DeepSeek вразливими до кібератак.
- Зберігання даних користувачів на серверах у Китайській Народній Республіці (КНР) та Російській Федерації (РФ), включаючи потенційно конфіденційні запити та файли, завантажені користувачами в продукти DeepSeek.
- Підпорядкування Компанії та її продуктів законодавству КНР, яке дозволяє урядові незаконно отримувати доступ до даних і примушувати до співпраці.
  доступ до даних і примушувати до співпраці, наприклад, шпигувати за користувачами DeepSeek.
- Передбачувана приналежність материнської компанії High-Flyer[(2)] доКомуністичної партії
  Китаю.

3 Визначення

- **Міністерство, Влада а Інші органи влади Державне адміністрація** - маються на увазі всі органи державного управління відповідно до § 1 та §
- 2 Закону Чеської національної ради № 2/1969 Зб. про створення міністерств та інших центральних органів державного управління Чеської Соціалістичної Республіки, зі змінами та доповненнями, та всі підпорядковані їм відомства.

[(1)]Повна назва 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]Повна назва компанії High-Flyer Quant Investment Management (Ningbo) L.P. (宁波幻方量化投资管理合伙企业).

- **Державне майно** - матеріальне (технічні засоби, спеціальне обладнання) та нематеріальне (програмне забезпечення, послуги) майно, яке використовується міністерством, бюро та іншими державними органами для здійснення покладених на них повноважень.

- **Продукти, додатки, рішення, веб-сайти та веб-сервіси DeepSeek** - сукупність продуктів, додатків і послуг, що належать DeepSeek або будь-якій з її попередніх, наступних, материнських, дочірніх або афілійованих компаній.[3](Корпоративна структура DeepSeek більш детально описана в Додатку 2)

    - Згадані продукти, додатки та послуги включають DeepSeek App, DeepSeek Chat, DeepSeek Platform, DeepSeek API та мовні моделі з доступом до Інтернету (список може бути неповним).

    - Ця заборона не поширюється на тестування безпеки, дослідження та аналіз продуктів DeepSeek, а також на великі мовні моделі DeepSeek з відкритим вихідним кодом, весь вихідний код яких доступний для перегляду та аналізу, якщо модель розгорнута локально без можливості зв'язку з серверами, що використовуються DeepSeek.

4 Рекомендації щодо виявлення та видалення продуктів, додатків і сервісів DeepSeek на службових пристроях

- **Спілкуйтеся зі співробітниками та іншими відповідними** особами - проінструктуйте співробітників (та інших осіб, які перебувають у трудових відносинах) повідомляти про те, чи встановлювали вони продукти, програми або веб-служби DeepSeek на робочих пристроях, чи отримували до них доступ або використовували їх.

- **Моніторинг мережевого трафіку та DNS-запитів** - за допомогою ключових слів і доменів можна відстежувати використання веб-сервісів і додатків DeepSeek у мережі організації (див. Додаток 1).

- **Журнали аудиту з систем реєстрації організації** - для визначення того, чи отримували користувачі доступ, завантажували або встановлювали продукти, додатки або веб-сервіси DeepSeek. Інструменти реєстрації подій повинні бути налаштовані на реєстрацію використання інтернет-сервісів, включаючи відвідані веб-сайти та завантажене програмне забезпечення, а також на ведення історії встановленого програмного забезпечення.

- **Керовані засоби безпеки** - програмне забезпечення або послуги, що використовуються для захисту інформаційно-комунікаційних систем, інформації та даних. Приклади інструментів безпеки:

    - **Антивірусне програмне забезпечення** - інструменти для безперервного захисту від шкідливого коду, які зазвичай використовуються для виявлення шкідливих файлів, але можуть бути налаштовані на виявлення певних типів файлів у більш широкому сенсі, включаючи додатки DeepSeek.

    - **Керування кінцевими точками** - програмне забезпечення, яке дозволяє керувати кінцевими точками. Може бути налаштоване на виявлення встановленого програмного забезпечення.

[3]Принцип розумних зусиль застосовується до виконання формулювання Резолюції 537 та пошуку і виявлення корпоративної структури DeepSeek та її продуктів, згідно з яким адресати зазначеної Резолюції зобов'язані докладати лише таких зусиль, які можуть бути розумно необхідними для виконання зазначених зобов'язань.

- **Управління мобільними пристроями** - рішення для управління мобільними пристроями, яке дозволяє реєструвати використання певних веб-сайтів і програмного забезпечення, де це можливо.

- **Застосування функцій кібербезпеки** - може використовуватися для виявлення використання певних продуктів або веб-сервісів. Функції кібербезпеки можуть виконуватися спеціалізованими командами або бути частиною звичайних IT-ролей, особливо в невеликих організаціях. До таких функцій належать

  - **Сканування Центру нагляду за безпекою (SOC**) - SOC захищає системи та пристрої і може використовуватися для перегляду журналів подій або запитів.
    запити на зміну системних налаштувань.

  - **Полювання на загрози** - як правило, проактивна діяльність, яка може бути використана для сканування мереж, кінцевих точок і наборів даних для виявлення використання веб-сервісів або додатків DeepSeek.

4.1 Видалення продуктів, програм і служб DeepSeek

Багато інструментів і рішень, що використовуються для виявлення використання продуктів, додатків і сервісів DeepSeek також можна використовувати для їх подальшого видалення:

- **Облікові записи адміністраторів кінцевих** точок - облікові записи з правами адміністратора кінцевих точок можуть використовувати вбудовані інструменти системи для видалення програмного забезпечення і додатків.

- **Інструменти безпеки** - програмне забезпечення або послуги для захисту технологій, інформації та даних. Приклади:

  - **Програмне забезпечення** для **керування кінцевими точками** - дозволяє керувати пристроями і може мати можливість віддалено видаляти програмне забезпечення та додатки.

  - **Програмне забезпечення** для **управління мобільними пристроями** - дозволяє адміністраторам видаляти програмне забезпечення та програми з керованих пристроїв.

5 Запобігання доступу та використанню

Щоб запобігти доступу, організації повинні розглянути наступні заходи:

- **Повідомлення персоналу** - повідомлення персоналу про те, що вони не можуть отримати доступ або використовувати продукти, програми та послуги DeepSeek відповідно до цієї політики.

- **Організаційні** заходи - внутрішня директива, політика, інструкція або інший захід для встановлення внутрішньої організаційної політики, яка визначає заборону на доступ до продуктів, додатків і послуг DeepSeek, а також будь-які винятки.

- **Фільтрація веб-контенту** - дозвіл на перегляд лише дозволених типів веб-контенту та сайтів із доброю репутацією, а також блокування доступу до певних доменів та IP-адрес DeepSeek.
- **Налаштування веб-браузера** - через проксі-сервери на шлюзах, які блокують доступ до певних категорій веб-сайтів DeepSeek, типів контенту та доменів.

Найбільш релевантними стратегіями для запобігання інсталяції є

- **Обмеження дозволів** - запобігання завантаженню, встановленню та використанню несанкціонованих програм шляхом контролю доступу, привілеїв та дозволів облікових записів, наприклад, на основі принципу найменших привілеїв, а також обмеження цих дозволів до тих, які необхідні для виконання роботи.
- **Контроль додатків** - забезпечення можливості встановлення та запуску лише затверджених додатків. Для мобільних пристроїв цей контроль забезпечує програмне забезпечення для управління мобільними додатками.

6 Додатки

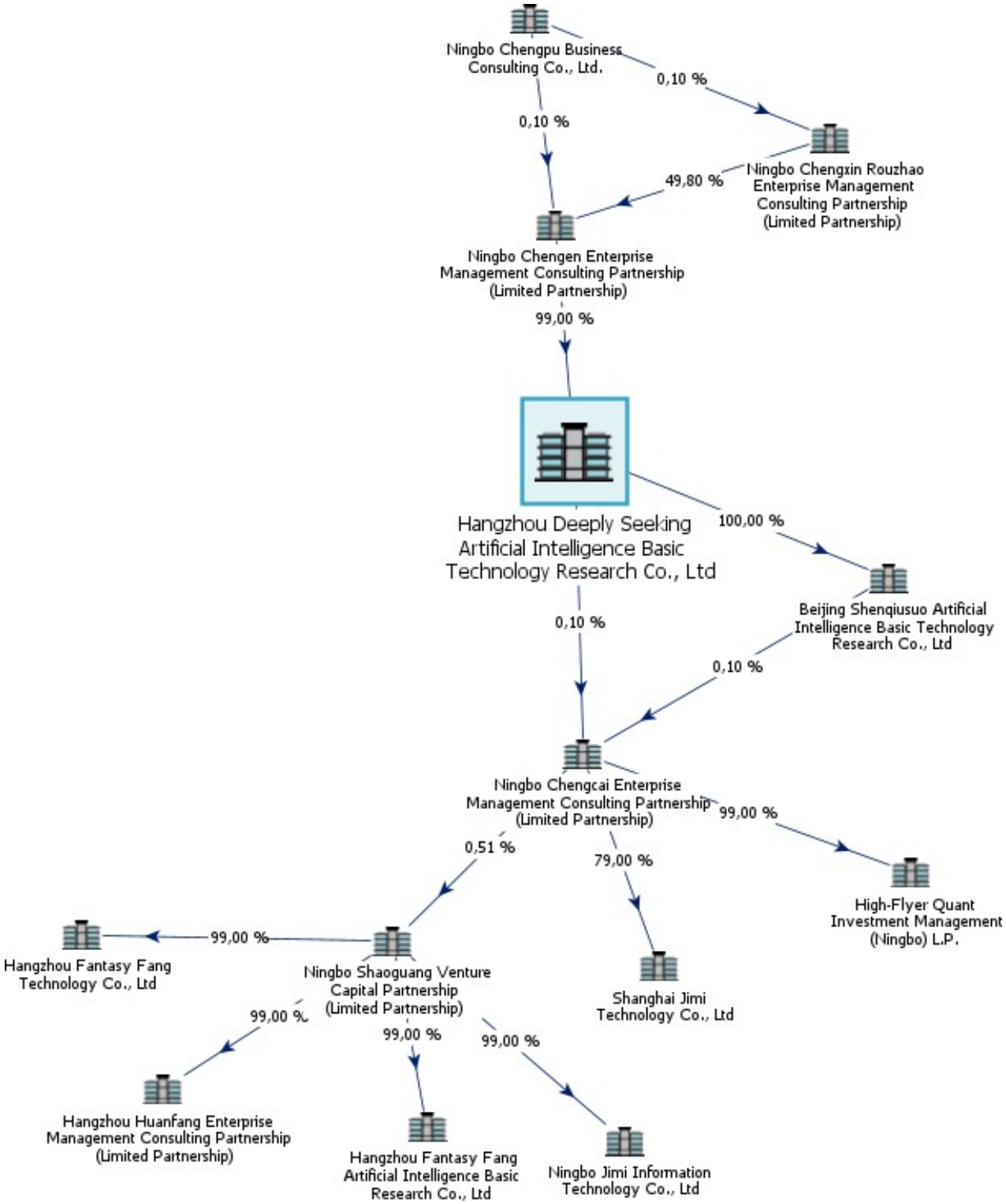
6.1 Додаток 1: Рекомендації щодо моніторингу мережевого трафіку

Додаток є окремим документом DeepSeek_indicators.csv

Крім конкретних доменів, можна також використовувати фільтр підстановочних символів:

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

6.2 Додаток 2: Структура компанії DeepSeek



Назва Компанія (EN)	Ім'я Компанія (CN)	Назва компанії (EN)	Назва компанії (CN)
Ханчжоу Глибокий пошук Штучний інтелект 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	Нінбо Ченпу Бізнес Консалтинг Лтд.	宁波程普商务咨询有限公司
Нінбо Партнерство з консалтингу управління підприємством Ченген (Товариство з обмеженою відповідальністю)	宁波程恩企业管理咨询合伙企业	Ханчжоуське фантастичне ікло Фундаментальні дослідження штучного інтелекту, Лтд.	杭州幻方人工智能基础研究有限公司
Пекінська компанія з дослідження базових технологій штучного інтелекту Shenqiusuo	北京深度求索人工智能基础技术研究有限公司	Товариство з обмеженою відповідальністю "Консалтингове партнерство з управління підприємством Ханчжоу Хуанфан	杭州幻方企业管理咨询合伙企业（有限合伙）
Нінбо Товариство з обмеженою відповідальністю "Ченкайське партнерство з консалтингу в галузі управління підприємством	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）
Нінбо Товариство з обмеженою відповідальністю "Ченсін Ружао" з управління підприємницьким консалтингом (Товариство з обмеженою відповідальністю)	宁波程信柔兆企业管理咨询合伙企业（有限合伙）	Шанхай 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	Нінбо Шаогуанське партнерство з венчурного капіталу (Товариство з обмеженою відповідальністю)	宁波少广创业投资合伙企业（有限合伙）
Нінбо Jimi Information Technology Co, Ltd.	宁波积幂信息科技有限公司	Wenfeng Liang	梁文锋

7 Умови використання інформації

Використання наданої інформації здійснюється відповідно до методології "Протоколу світлофора", доступної на веб-сайті НУКІБ. Інформація позначена прапорцем, який визначає умови використання інформації. Нижче наведені прапорці, які вказують на характер інформації та умови її використання:

Колір	Умови використання
TLP: ЧЕРВОНИЙ	Інформація не може бути надана іншій особі, окрім особи, якій вона була надана призначалася, за винятком випадків, коли інші особи, яким така інформація може бути розкрита, спеціально визначені. Якщо одержувач вважає важливим розкрити інформацію іншим особам, це може бути зроблено лише за згодою особи, яка її надала.
TLP: БУРШТИНОВИЙ+СУВОРИЙ	Інформація може бути передана тільки в межах організації одержувача і тільки особам, які відповідають принципам доступу до інформації.
TLP: ЯНТАР	Інформація може бути передана в межах організації-одержувача та її партнерам, і лише особам, які відповідають принципу службової необхідності.
TLP: ЗЕЛЕНИЙ	Інформація може бути передана в межах організації-одержувача та, за необхідності, з іншими партнерами бенефіціара, але не через загальнодоступні канали; бенефіціар повинен забезпечити конфіденційність повідомлення при його передачі.
БІЛИЙ **TLP: CLEAR**	Інформація може надалі надаватися та поширюватися без обмежень. Це положення не впливає на будь-які обмеження, що базуються на правах інтелектуальної власності автора та/або одержувача або третіх осіб.