

CISO Campus

це важливий етап у розвитку факультету
кібербезпеки CDTO Campus



CDTO Campus

це перший в світі повноцінний освітній проєкт
розвитку цифрових лідерів та їх команд для
державного сектору

Місія:

Забезпечити державу кваліфікованими фахівцями

Що пропонує CDTO Campus?

Унікальний контент
цифровізації
України



Лектори
практики



Безоплатне навчання
за підтримки донорів



Рекомендації для
працевлаштування



Нетворкінг з
топ-менеджерами
цифровізації



Навчання через
мобільний додаток



Результати CDTO Campus

1361

випускників

9000+

заявок

30+

програм

100+

лекторів

272

випускників кастомних
програм

2000+

слухачів
відкритих сесії

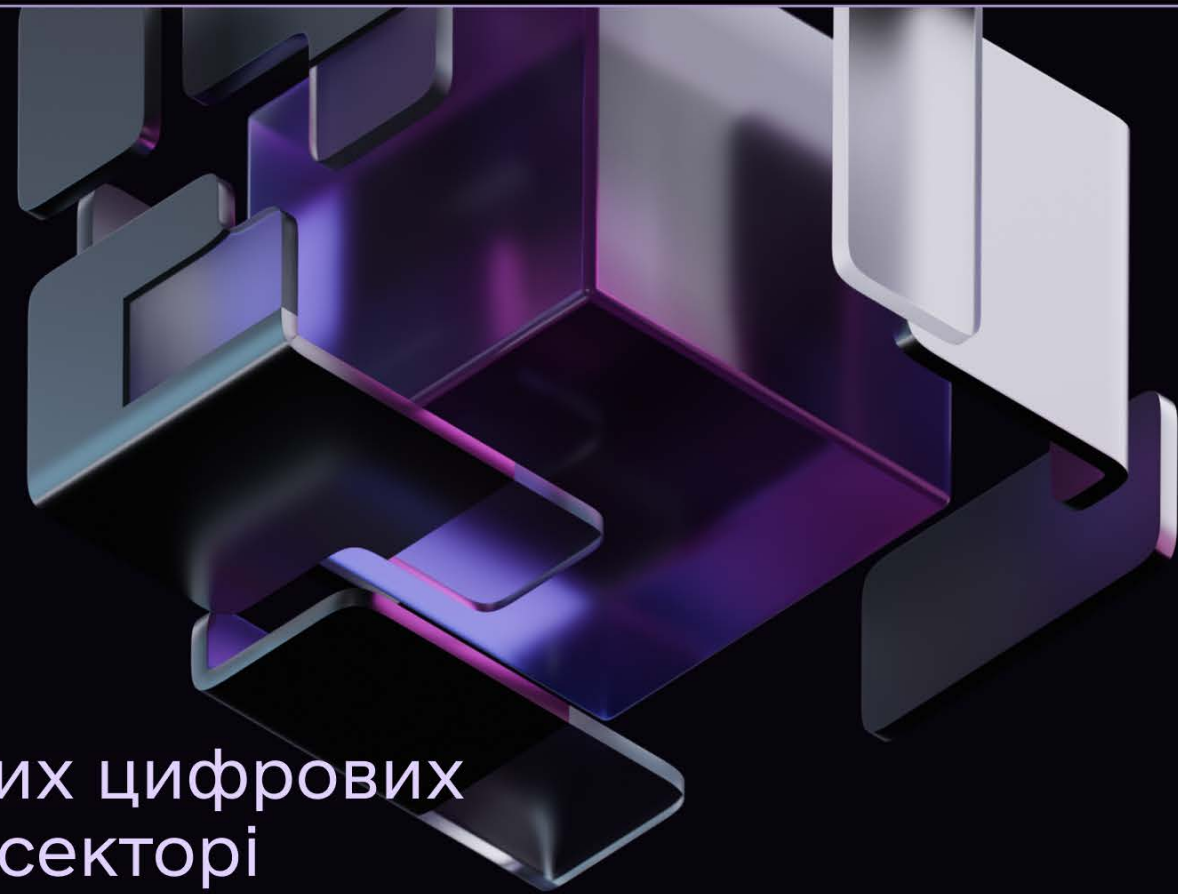
1382

годин лекцій

Факультети

GovTech

Впровадження сучасних цифрових рішень у державному секторі



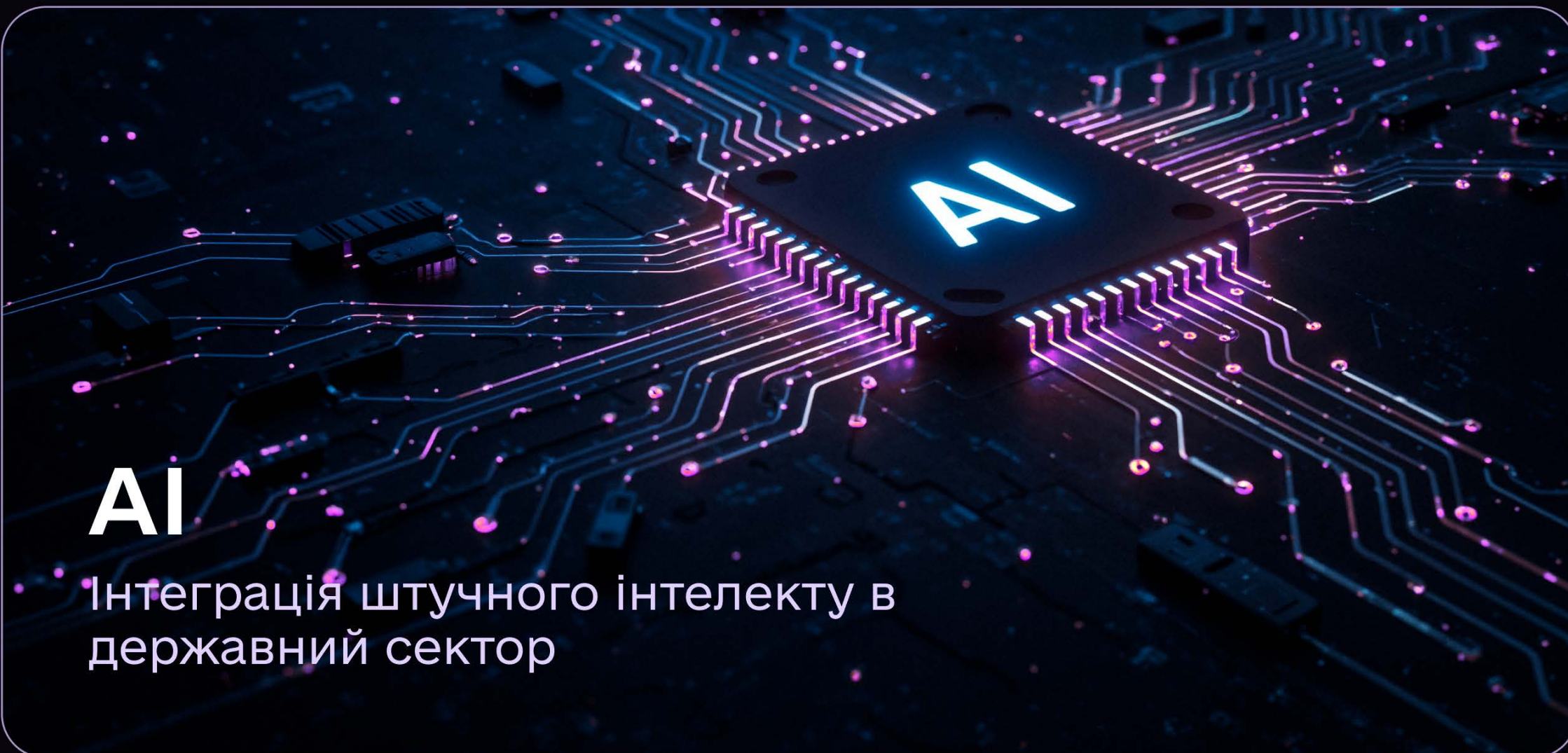
Cybersecurity

Управління цифровими ризиками та кіберзахист



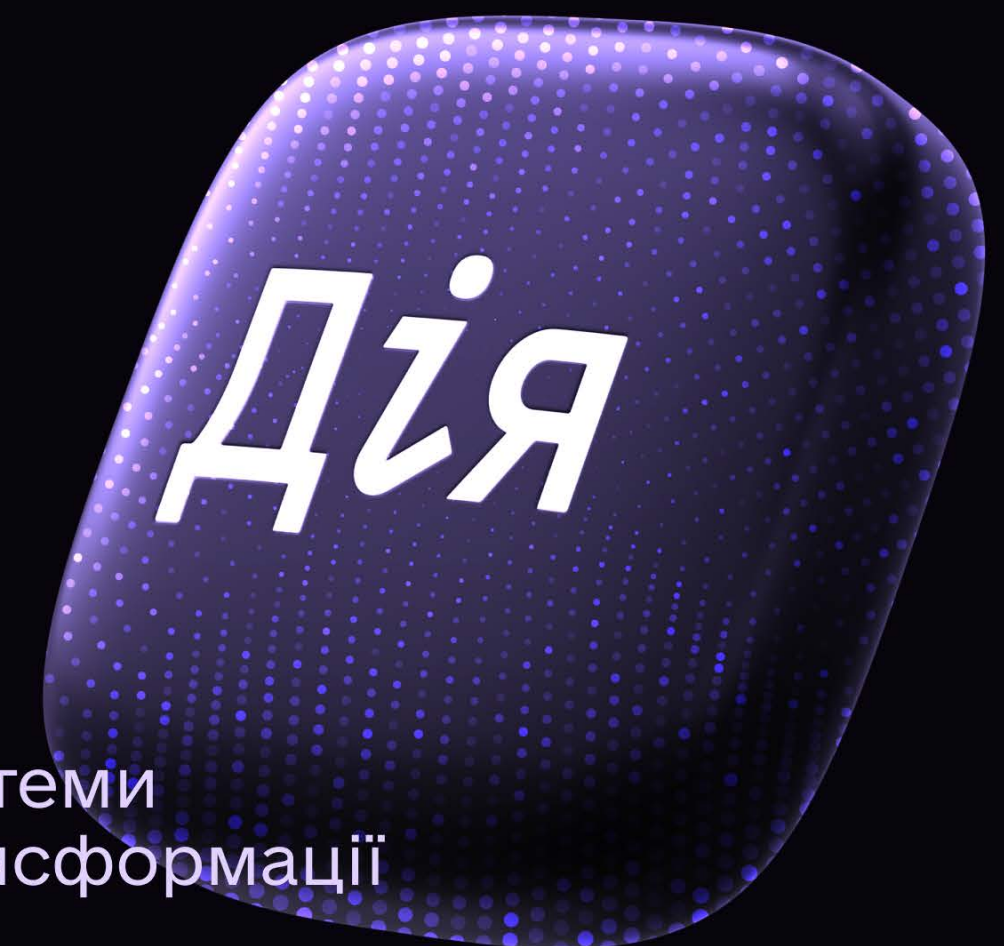
AI

Інтеграція штучного інтелекту в державний сектор



Diia

Підтримка розвитку екосистеми Міністерства цифрової трансформації



Програми CDTO Campus

Кастомні програми

Лідерські програми

Партнерські програми

В межах Талліннського
механізму

Програми факультету кібербезпеки CDTO Campus

Кастомні програми

Лідерська програма з кібербезпеки для управлінців

4 ітерацій

77 учасників

Основи кібербезпеки для нетехнічних працівників

4 ітерацій

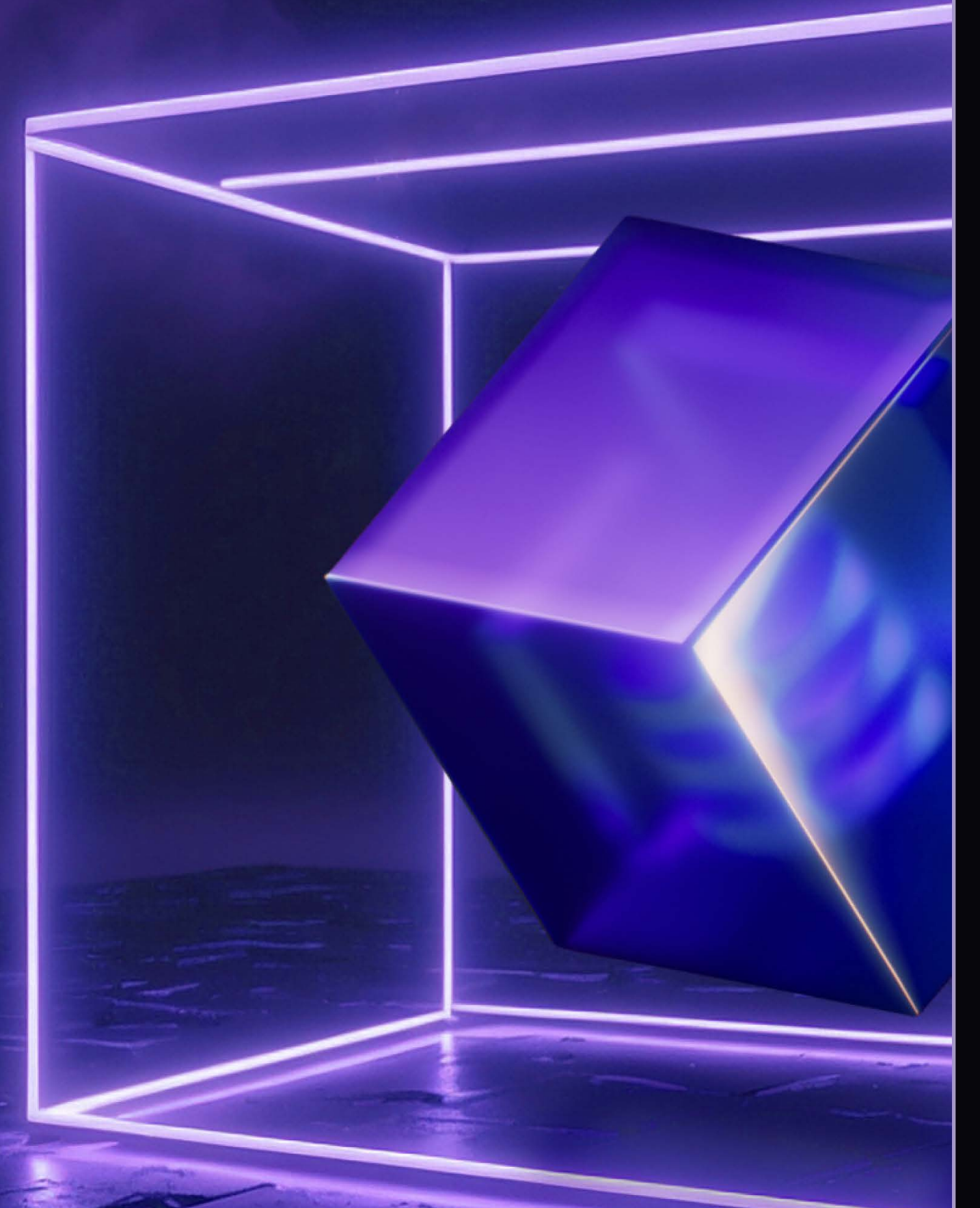
95 учасників

Тренінг для тренерів “Як навчити виявленню кіберзагроз та заходам протидії

2 ітерації

22 учасника

Програми були реалізовані за підтримки Проекту "Кібербезпека критично важливої інфраструктури України" під патронатом Міністерства цифрової трансформації



Програми факультету кібербезпеки CDTO Campus

Партнерські програми

Mandiant: Розвідка кіберзагроз і побудова стійкості до них



Monarch: Інформаційна безпека, Мережева безпека та реагування на інциденти, Впровадження профілів безпеки та управління ризиками



Women in Cyber: Навички у сфері кіберзахисту

Cisco: Основи кібербезпеки для нетехнічних спеціалістів у державному секторі



CrackenAGI: Кібербезпека в контексті цифровізації



Талліннський механізм

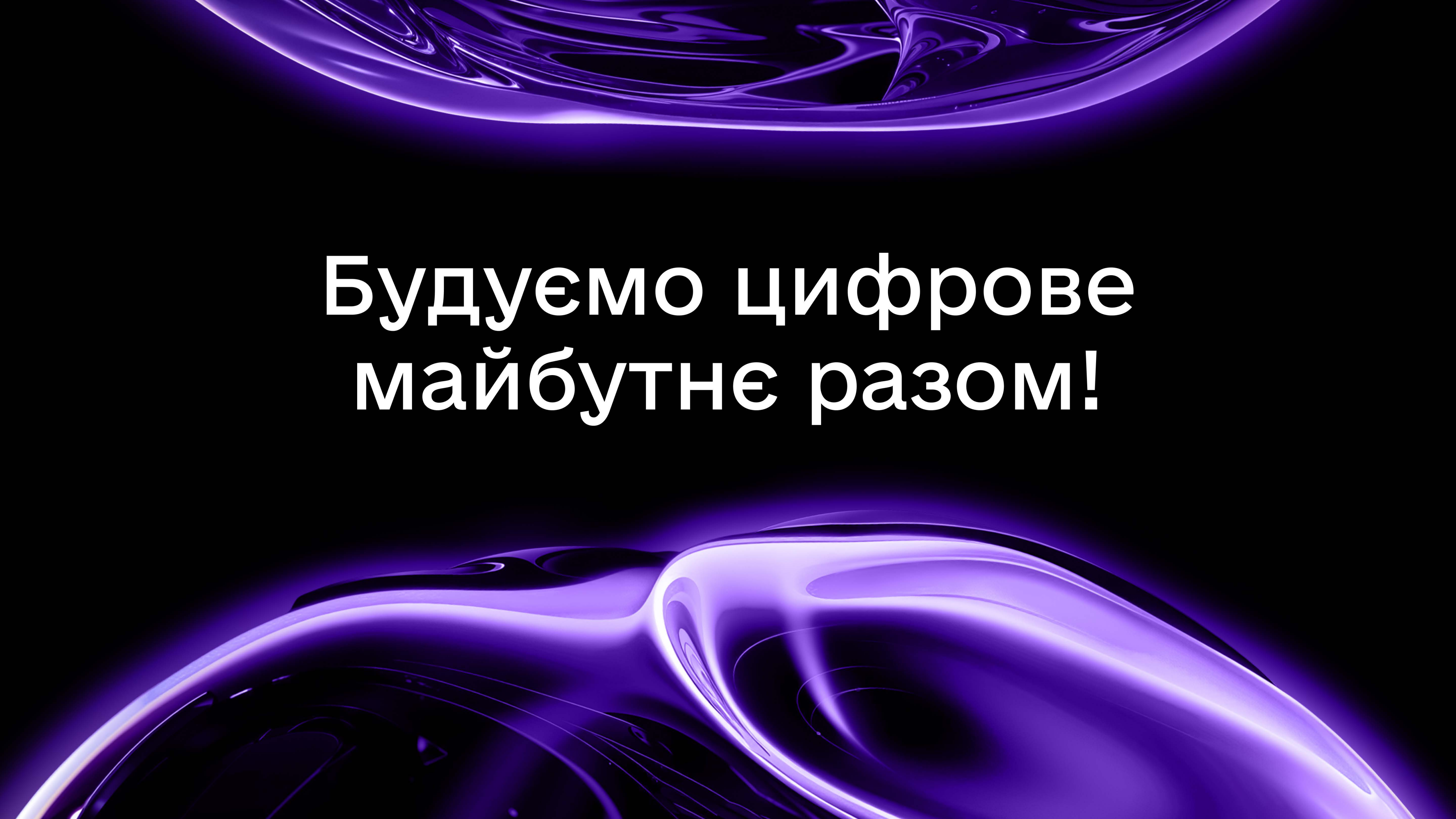


Міжнародна ініціатива, спрямована на підтримку кібербезпеки України, посилення кіберзахисту та кіберстійкості, а також розвиток цивільного кібернетичного потенціалу шляхом системної координації міжнародної допомоги

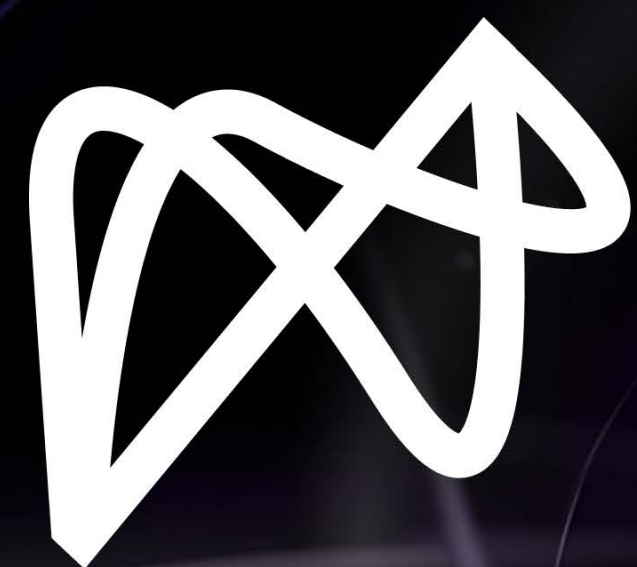
У межах Таллінського механізму CDTO Campus реалізує програми, спрямовані на підвищення кібербезпекових спроможностей органів державної влади України

2025

У партнерстві з міжнародними партнерами було реалізовано 8 програм у рамках Таллінського механізму



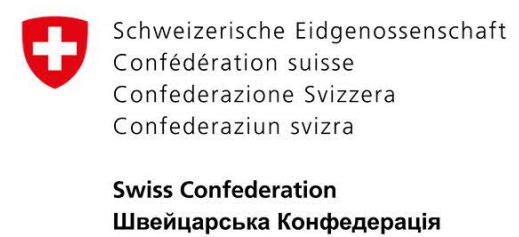
Будуємо цифрове
майбутнє разом!



CDTO Campus



Implemented by:



Ministry
of Digital Transformation
of Ukraine

CISO Campus

is a national educational project for
training cybersecurity leaders and
specialists (CISOs)

The background of the slide is a deep purple color with a fine, grainy texture. In the top right and bottom left corners, there are abstract, flowing shapes that resemble liquid or smoke, rendered in a lighter shade of purple with highlights and shadows, giving them a three-dimensional appearance.

CISO Campus

is an initiative launched by SSSCIP and the Ministry of Digital Transformation, implemented by the East Europe Foundation within CDTO Campus, and developed with the support of international donors and partners based at the CDTO Campus Cybersecurity Faculty

Project Summary

Goal

To establish an educational and practical platform for CISOs, managers, and cybersecurity professionals, aligned to current challenges and legislation

Focus

Training new CISOs (in line with Ukrainian cybersecurity law)

Upskilling CISOs

Team training

Crisis management

Compliance and regulations

Formats

- Short- and long-term programs
- Workshops, seminars, briefings, summits, informal exchanges

Why Now



Growing number
and complexity
of cyberattacks



New legislative
mandates to appoint
CISOs



Shortage of qualified
leaders and no unified
CISO school in Ukraine



Need to build a national
culture of cyber
resilience and crisis
management

Key Advantages of CISO Campus

CISO Campus — a collaborative initiative of the Ministry of Digital Transformation and SSSCIP, within CDTO Campus, serves as a single state-approved entry point for building cyber and information security competencies across all government institutions, including the national security and defense sector.

Not a competition of programs, but a comprehensive, unified approach — with verified training modules, flexible scaling for each agency's needs, and the ability to rapidly respond to emerging skill demands.

SSSCIP uniquely understands who and why needs training, providing a full learning lifecycle: needs and education gaps assessment, reskilling and upskilling, onboarding and tracking to ongoing development and career support.

CISO Campus also builds a coordinated professional community of cybersecurity experts who share a common foundation of knowledge and best practices, strengthening Ukraine's overall cyber resilience.

Target Audience and Outcomes

Primary audience

Chief Information Security Officers (CISOs) or equivalent positions in

1. Government agencies and local self-government bodies
2. State-owned enterprises, institutions, and organizations
3. Critical infrastructure operators

Secondary audience

Heads of cybersecurity departments

Specialists included in the CISO talent reserve pool

Experts responsible for key cybersecurity areas

- Issuance of Certificates upon successful completion of training
- Mentorship Program for early-career CISOs

Modular Trainings

Leveraging structures such as the

ENISA European Cybersecurity Skills Framework (ECSF)

WEF Strategic Cybersecurity Talent Framework (CTF)

Modular and practically-oriented programs to cover essential and advanced topics, e.g

- Cybersecurity Fundamentals for Civil Servants
- Cyber Hygiene and Awareness
- Cybersecurity Legislation and Regulations
- Cybersecurity Risk Management
- Architecture and Technologies
- Cybersecurity for Industrial Control Systems
- Cyber Incident Response
- Cloud Technologies Security

Practical Workshops and Simulations utilizing cyber ranges

Continuous Monitoring of changes in cyber threats, technologies, and legislation

Evaluate Effectiveness and Regular Updates of educational materials and programs

Delivery Format and Scale

01

Hybrid Learning Format:
Combining in-person (classroom)
and online instruction

02

Establishing a unified
educational platform (LMS) for
learning, sharing best practices
and continuous engagement

03

Central hub in Kyiv,
considering two regional
centers in 2026-2027

04

Experienced cybersecurity instructors
drawn from academic environment,
government sector, and leading private
companies

05

Active partnership with
cybersecurity companies

06

Collaborate with government institutions,
international partners, and private
companies to synchronize educational
Initiatives and share best practices

Financial Sustainability

Initial Stages (Creation, Development, Operation)

Primarily supported by securing International Technical Assistance (ITA) from partner countries and international organizations committed to strengthening Ukraine's cyber capabilities

Future Sustainability

Potential integration of other sources to ensure the long-term sustainability and scalability of the project