



КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ
ТАРАСА ШЕВЧЕНКА

Навчально-науковий інститут неперервної освіти
ДЕРЖАВНОГО УНІВЕРСИТЕТУ «КИЇВСЬКИЙ
АВІАЦІЙНИЙ ІНСТИТУТ»



ЦИФРОВА БЕЗПЕКА ДЛЯ ЗАПОБІГАННЯ КОРУПЦІЇ НА РОБОЧОМУ МІСЦІ

2025



Орищук Василь Валерійович

науковий співробітник Київського національного університету імені Тараса Шевченка, доктор філософії у галузі публічного управління та адміністрування



Кожина Алла Василівна

в.о. завідувача кафедри публічного управління та адміністрування Навчально-наукового інституту неперервної освіти Державного університету «Київський авіаційний інститут», доктор наук з державного управління, професор





**Інтерактивна сесія: Що
для вас означає термін
"цифрова безпека"?**

Цифрова безпека



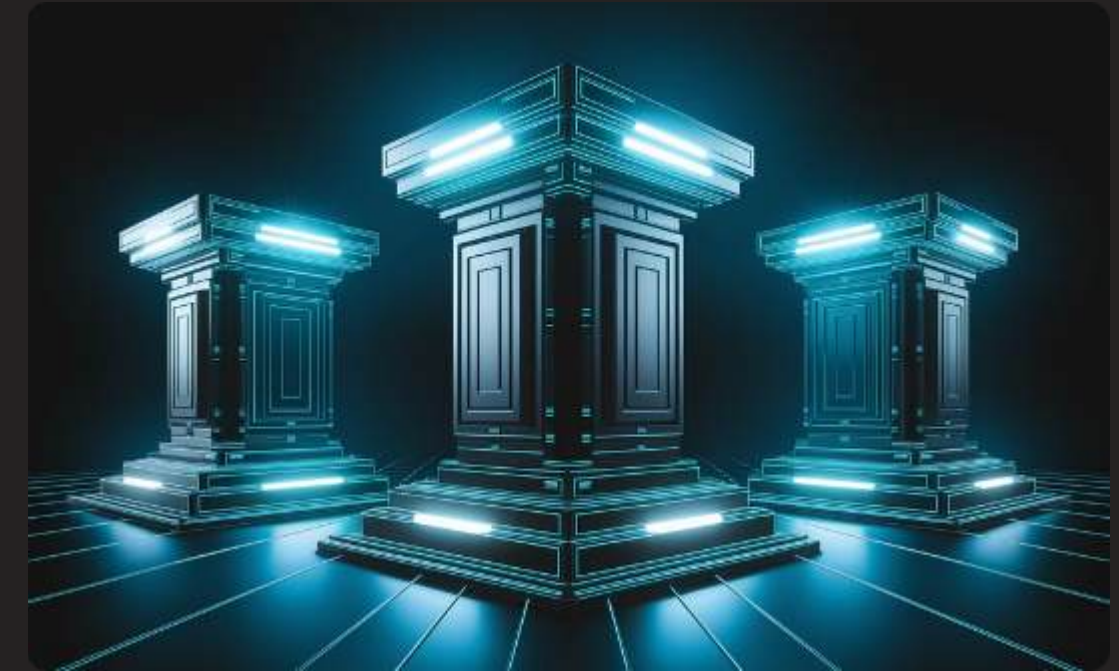
Захист цифрової особистості

Цифрова безпека охоплює різні способи захисту цифрової особистості, зокрема облікового запису комп'ютера в Інтернеті і файлів від вторгнення зовнішнього користувача



Інструменти захисту

Цифрова безпека включає інструменти, які використовуються для захисту своєї ідентичності, активів та технологій в цифровому світі



Основні принципи

Цифрова безпека – безперервний процес, що базується на трьох ключових принципах: конфіденційності, цілісності та доступності

Чому цифрова безпека є ключовим елементом антикорупційних стратегій?

Цифрова безпека відіграє важливу роль у боротьбі з корупцією, оскільки більшість корупційних схем та фінансових махінацій нині здійснюється через цифрові канали. Ось основні причини:

Захист конфіденційної інформації

- Корупційні дії часто пов'язані з несанкціонованим доступом до внутрішньої документації та баз даних.
- Надійний кіберзахист зменшує можливість витоку критичних даних, які можуть бути використані для маніпуляцій або шантажу.

1

2

Прозорість фінансових операцій

- Використання цифрових систем, таких як Prozorro (електронні держзакупівлі) або блокчейн, дозволяє відслідковувати фінансові потоки та унеможлиблює їх приховування.
- Чітка реєстрація всіх платежів і контрактів унеможлиблює корупційні «відкати».

Контроль доступу та аудиту

- Системи розмежування доступу (наприклад, ролеві моделі доступу) обмежують можливість змінювати чи видаляти критичні дані.
- Логування та моніторинг усіх дій у системі дозволяють виявляти підозрілу активність і запобігати зловживанням.

Захист інформаторів (whistleblowers)

- Захищені цифрові платформи для анонімних повідомлень про корупцію допомагають викривати зловживання без ризику для інформатора.

3

4

5

Автоматизація та мінімізація людського фактору

- Чим менше людей вручну обробляють документи чи ухвалюють рішення щодо фінансів, тим нижчі ризики корупції.
- Використання штучного інтелекту та аналітичних систем для перевірки заявок і контрактів зменшує вплив корупційного людського фактора.

Основні ризики цифрового середовища для корупційних схем

Незважаючи на можливості цифрової безпеки, є низка загроз, які можуть бути використані для приховування корупції або маніпуляцій:



Фішинг та соціальна інженерія

Співробітники можуть несвідомо передавати паролі або доступи до систем корупціонерам, які використовують фішингові атаки або підроблені запити від керівництва.



Маніпуляції з електронними системами

Підробка цифрових підписів або маніпуляції з базами даних можуть дозволити корупціонерам змінювати або приховувати незаконні фінансові операції.



Злом корпоративних систем

Недостатній рівень кіберзахисту може дозволити хакерам викрадати дані про тендери, контракти або бухгалтерські операції, що сприяє корупційним схемам.



Відсутність моніторингу

Відсутність належного логування всіх дій у цифрових системах дозволяє приховувати сліди корупційних дій



Зовнішній вплив та шантаж

Використання витоків персональних даних та цифрових загроз для шантажу посадових осіб



Анонімні цифрові активи

Використання криптовалют та анонімних електронних гаманців для приховування корупційних схем

Як дезінформація сприяє корупції?

Приховування фінансових махінацій

- Створення фальшивих звітів, підроблених тендерних документів та «офіційних» заяв для виправдання розкрадань бюджету.
- Використання медіа для публікації позитивних матеріалів про підозрілі проекти.

Маніпуляція громадською думкою перед виборами

- Використання дезінформації для впливу на рішення виборців щодо корумпованих кандидатів.
- Використання deepfake-технологій для створення компрометуючих відео або аудіозаписів.

1

2

3

4

Дискредитація антикорупційних органів та активістів

- Запуск фейкових кампаній проти журналістів-розслідувачів або посадовців, які викривають корупцію.
- Використання ботів і тролів у соцмережах для розповсюдження неправдивої інформації.

Фальсифікація даних у цифрових системах

- Використання підроблених електронних документів у держреєстрах або базах даних.
- Внесення змін у відкриті реєстри для приховування інформації про власників компаній або нерухомості.

Протидія дезінформації в антикорупційній діяльності

1

Розуміння ризиків

Дезінформація є серйозним корупційним ризиком, оскільки може маскувати зловживання, впливати на громадську думку та дискредитувати антикорупційні зусилля.

2

Технологічні рішення

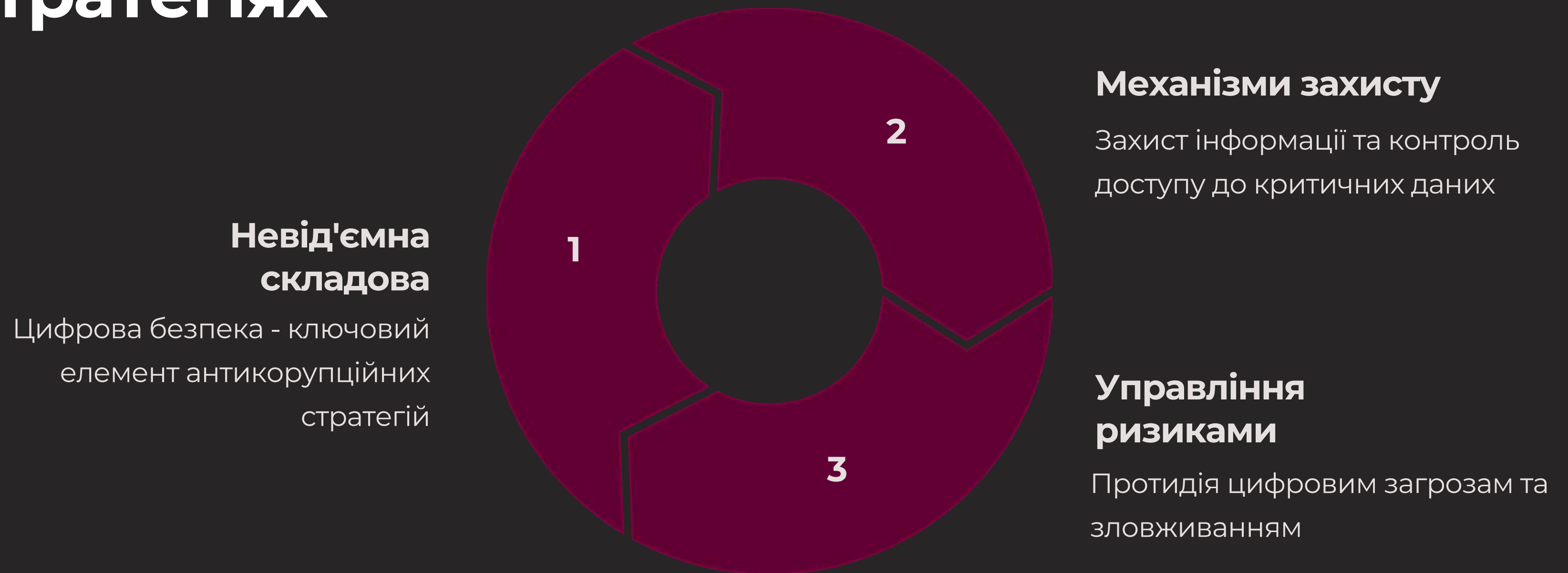
Використання цифрових технологій, фактчекінгу та алгоритмів моніторингу інформації допоможе мінімізувати вплив фейкових кампаній.

3

Освітні заходи

Підвищення медіаграмотності серед державних службовців і громадян – важливий елемент у боротьбі з дезінформацією.

Цифрова безпека в антикорупційних стратегіях



У сучасному світі цифрова безпека стала невід'ємною частиною ефективних антикорупційних стратегій. Надійний захист інформації, прозорість фінансових операцій і контроль доступу до критичних даних суттєво знижують корупційні ризики. При цьому важливо постійно враховувати нові загрози цифрового середовища.



Практична сесія:

- **Оцінка кібербезпеки та захисту даних з ШІ;**
- **Як виявляти дезінформацію, згенеровану ШІ?**

Висновки та рекомендації щодо запобігання корупції на робочому місці за допомогою цифрової безпеки

1

Впроваджуйте заходи безпеки

Захистіть інформацію та дані.

2

Навчайтеся

Підвищуйте обізнаність про цифрову безпеку.

3

Моніторте активність

Виявляйте та запобігайте корупційним діям.

1. З яким настроєм ви завершуєте сьогодні?
2. Що було для вас корисним?

