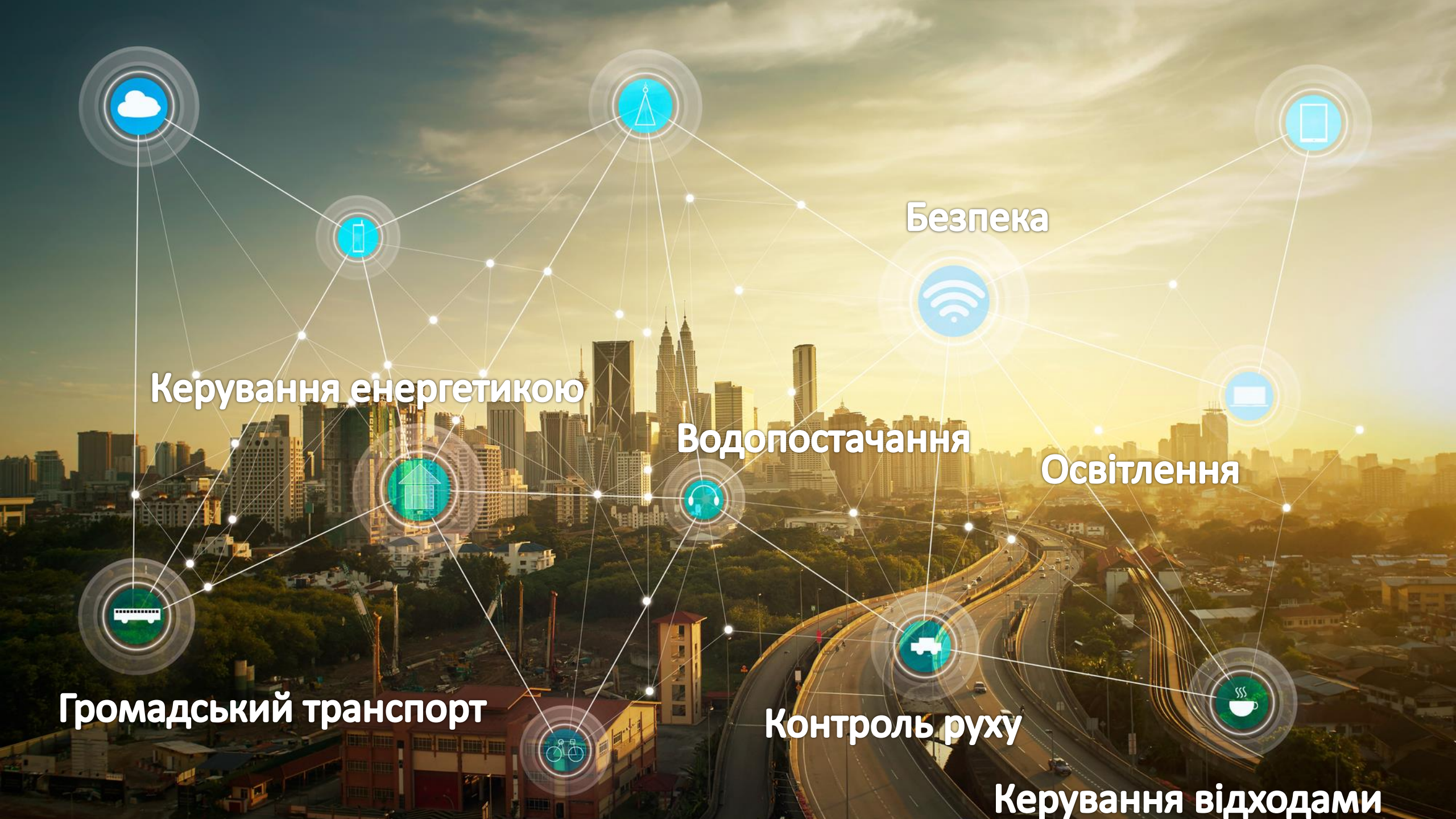
Виклики кібербезпеки для розумних міст

Віктор Жора, Директор


Безпека
Керування енергетикою
Водопостачання
Освітлення
Громадський транспорт
Контроль руху
Керування відходами

Виклики кібербезпеки

- Недостатнє тестування
- Відсутність або недостатність технологій безпеки
- Недостатність шифрування
- Відсутність команд реагування
- Масштаб і складність поверхні атаки
- Встановлення оновлень
- Застарілі системи
- Особливості бюджетування
- Відсутність сценаріїв реагування на атаки
- Ризики DoS/DDoS

*За даними ioactive.com

Кіберзагрози (1/2)

Освітлення вулиць

- Компрометація системи освітлення, перехоплення керування

Енергопостачання

- Вимкнення електроживлення

Громадський транспорт

- Перехоплення керування, зміна розкладу

Керування трафіком

- Отримання контролю над світлофорами

Системи керування містом

- Отримання контролю, ураження шкідливим ПЗ

Розумні сенсори

- Спотворення сигналів

Кіберзагрози (2/2)

Камери спостереження

- Втручання в роботу

Соціальні мережі

- Провокування безладу

Публічні дані

- Використання для планування атак

Мобільні застосування

- Злам і спотворення даних

Сервіси геолокації

- GPS-спуфінг, маніпуляції

«Хмарні» сервіси

- DDoS-атаки

Атаки на розумні міста (1/2)

- **Атака на обленерго** (BlackEnergy, 23.12.2015, 30 підстанцій, 230 тисяч мешканців без світла)
- **Атака на Київенерго** (Industroyer, 17.12.2016, підстанція Північна, більше години)

Атаки на розумні міста (2/2)

- **03.2016** – атака на станцію очищення води, 2,5M користувачів
- **04.11.2016** – Швеція, атака на аеропорти
- **25.11.2016** – Сан-Франциско, муніципальна залізниця, ураження ransomware
- **07.04.2017** – Даллас, 156 сирен небезпеки о 23:40
- **11.10.2017** – Швеція, DDoS-атака на систему спостереження за рухом поїздів
- **22.03.2018** – Атланта, інформаційні системи міста, ураження ransomware

За даними ioactive.com

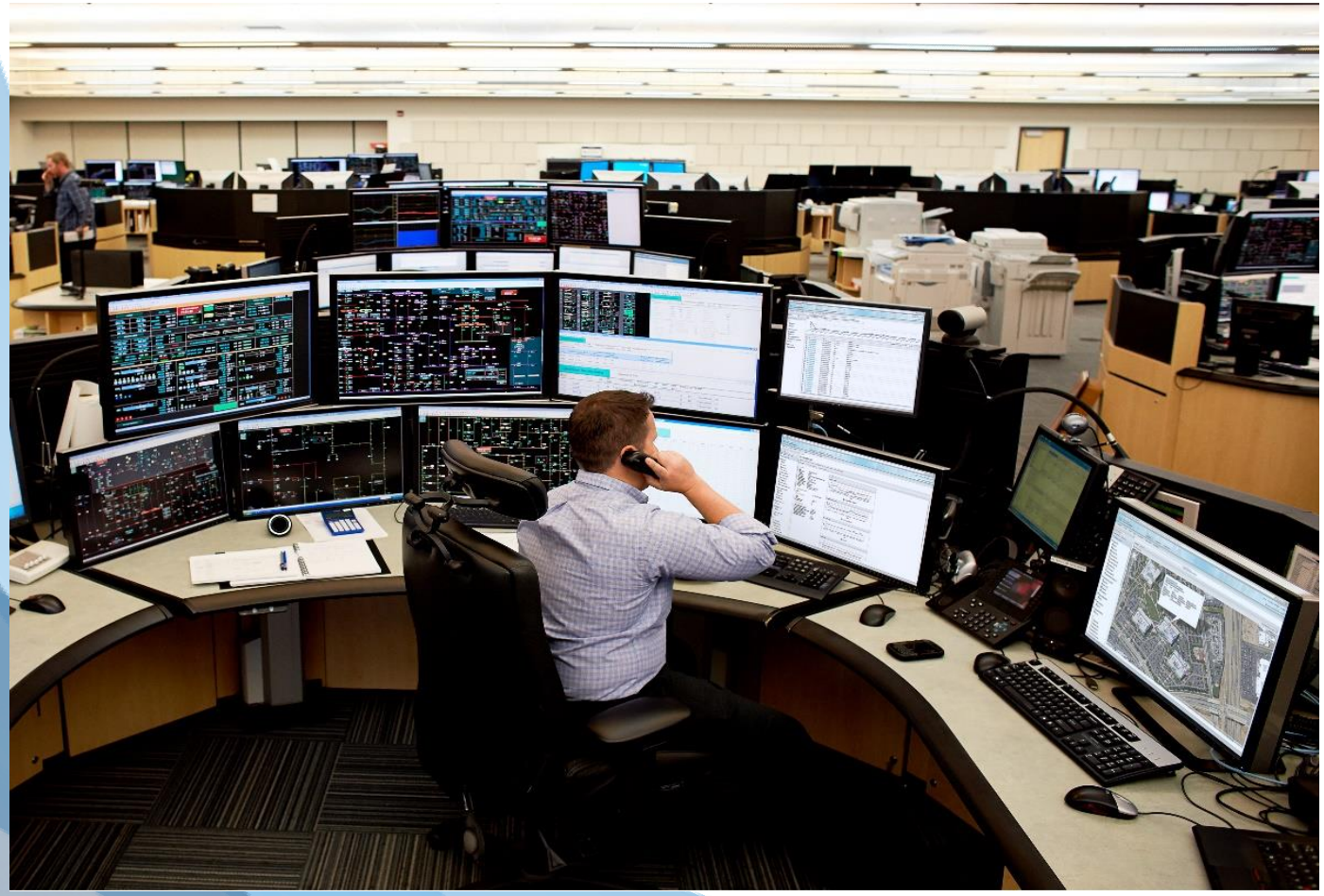

Системи спостере-ження
Обмін знаннями
Безпечне розумне місто
Відео-аналітика
Команд-ний центр
Центр обробки даних

*За даними EY

Технології захисту для розумного міста

- Сегментація мереж
- Шифрування каналів передачі даних
- Аудит журналів
- Сильна парольна політика
- Наявність ручного керування
- Оновлення системного, прикладного ПЗ та засобів кіберзахисту
- Створення Security Operations Center (SOC)
- Побудова комплексних систем захисту інформації (КСЗІ)

Security Operation Center (SOC)



- Реагування на інциденти
- Збір інформації про загрози
- Аналітика та обмін інформацією
- Дослідження
- Навчання та освіта
- (КСЗІ)

КСЗІ

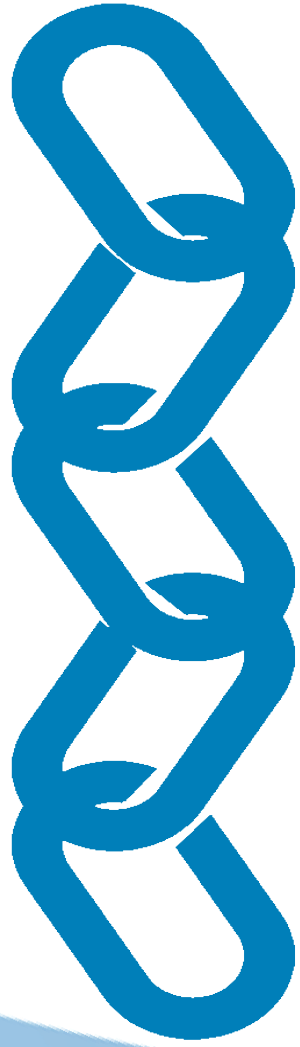
•ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про основні засади забезпечення кібербезпеки»
•Захист критичних інформаційних інфраструктур
•Аудит безпеки
•Впровадження КСЗІ в інформаційних системах та реєстрах

Напрямки діяльності

Cybersecurity
Постачання, інтеграція та впровадження систем комплексного захисту від кіберзагроз

Licensed Software
Постачання та впровадження ліцензійного програмного забезпечення

Telecommunications
Побудова локальних та розподілених корпоративних мереж



MSSP
Послуги з аутсорсингу інформаційної безпеки,
захист організації «під ключ»

Infrastructure Solutions
Інфраструктурні рішення для потреб бізнесу

infosafe

Зв’яжіться з нами


вул. Казимира Малевича, 86-г, оф. 5 Київ


(044) 596-00-44


sales@infosafe.ua


infosafe.ua