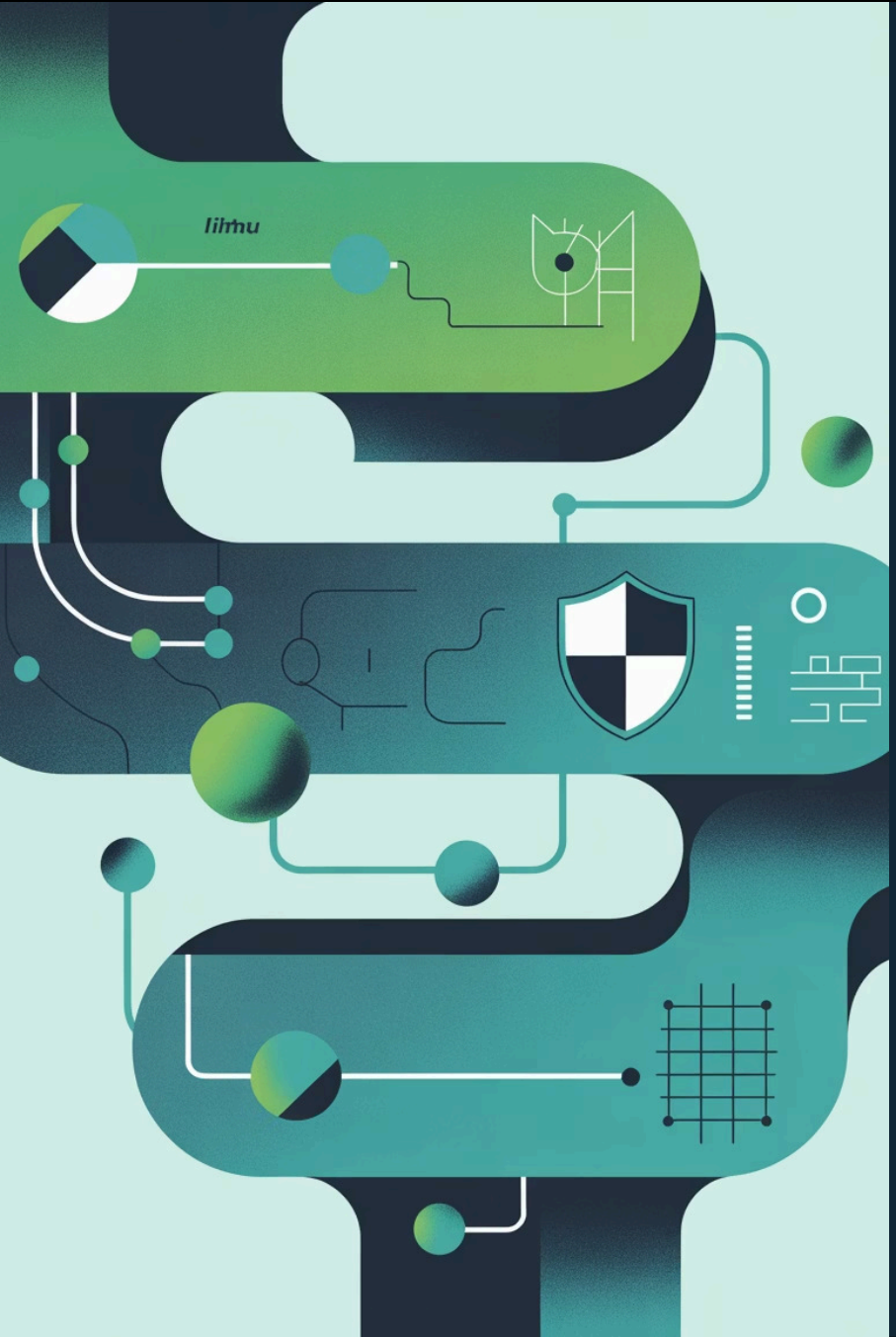


№13 Дәріс. Үлестірілген нақты уақыт жүйелеріндегі қауіпсіздік және сенімділік мәселелері

Дәріскер: Даркенбаев Д.К. PhD, қауымдастырылған профессор

Дәріс мақсаты

Үлестірілген нақты уақыт жүйелеріндегі (Distributed Real-Time Systems – DRTS) қауіпсіздік, сенімділік және қорғаныс талаптарын түсіндіру

Негізгі қауіптерді, шабуыл түрлерін және оларды болдырмау стратегияларын түсіндіру.

Кілт сөздер

- Real-time systems
- Distributed systems
- Security
- Reliability
- Fault tolerance
- Redundancy
- Cybersecurity
- DoS attack
- Integrity
- Confidentiality
- Availability

Дәрістің жоспары

01
Үлестірілген нақты уақыт жүйелеріне кіріспе

02
Қауіпсіздік талаптары

03
Сенімділік және fault tolerance

04
Негізгі қауіптер мен шабуыл түрлері

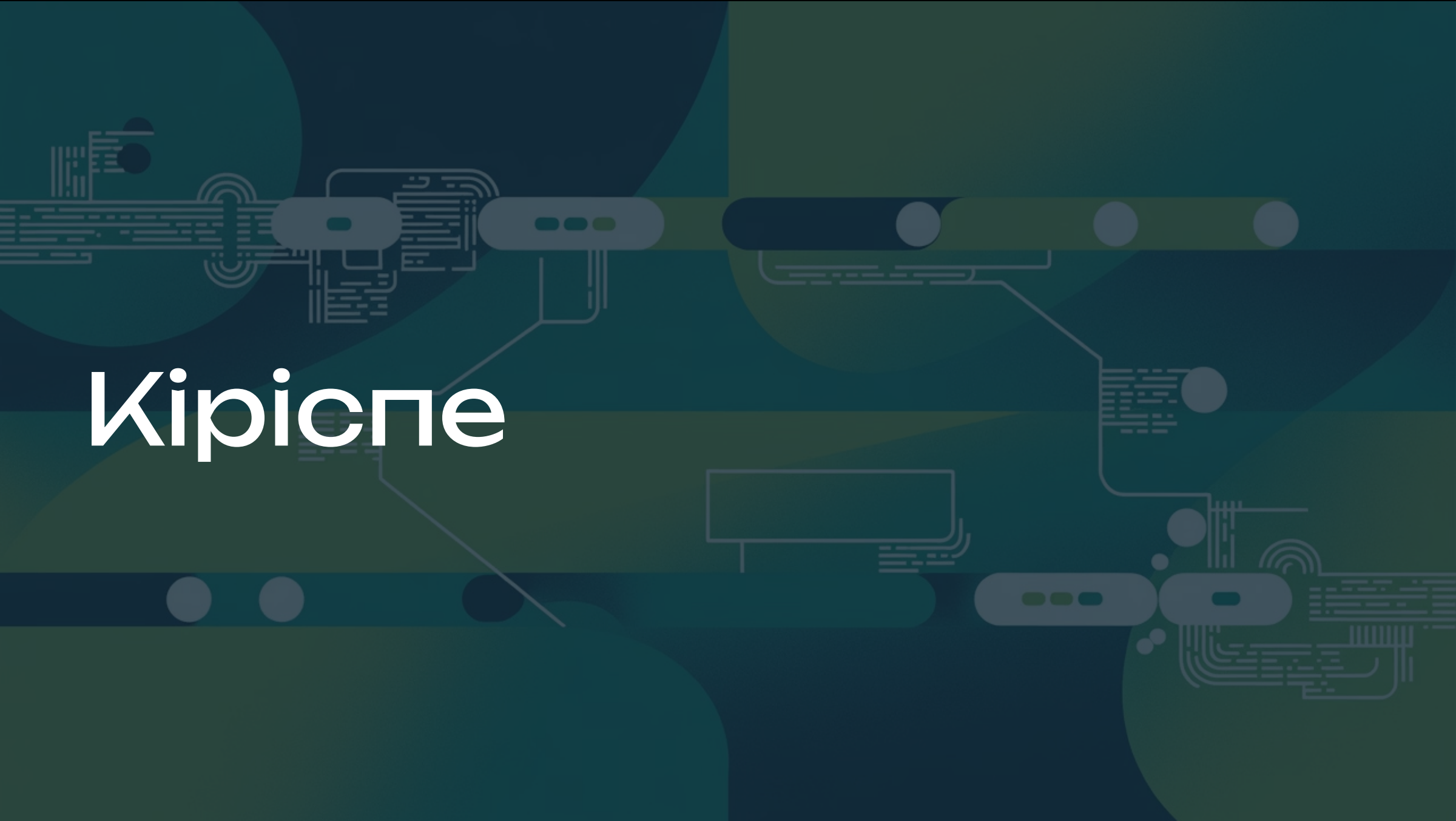
05
Қауіпсіздік архитектурасы

01
Сенімділікті қамтамасыз ету әдістері

02
Протоколдар мен технологиялар

03
Қолданылу салалары

04
Қорытынды


Kipicne

Үлестірілген нақты уақыт жүйелеріне кіріспе

Үлестірілген нақты уақыт жүйелері — әртүрлі түйіндерге бөлінген, нақты уақыт шектеулерін сақтай отырып ақпарат алмасатын және оқиғаларға шұғыл жауап беретін жүйелер.

Қолданылу аймақтары:

Автономды көліктер

Ұшқышсыз аппараттар (UAV, drones)

Өндірістік басқару (SCADA, IIoT)

Әскери және авиациялық жүйелер

Денсаулық сақтау мониторингі

Ақылды қала және көлік инфрақұрылымы

Негізгі талап: қауіпсіздік, кідіріс минимизациясы және үздіксіздік.

Қауіпсіздік талаптары

CIA моделі:

Талап	Түсініктеме
Confidentiality	Құпиялылық
Integrity	Деректердің бұрмаланбауы
Availability	Қолжетімділік

Қосымша талаптар

- Реал-тайм жауап уақыты
- Аутентификация және авторизация
- Трассировка және мониторинг
- Физикалық қауіпсіздік (CPS жүйелерінде)

Сенімділік және Fault Tolerance

Сенімділік (Reliability)

Жүйенің үздіксіз және қатесіз жұмыс жасау қабілеті.

Fault tolerance

Қателерге қарамастан жұмысты жалғастыру.

Стратегиялар:

- Репликация
- Қосарланған резерв (redundancy)
- Журнал жүргізу (logging)
- Watchdog таймерлері
- Error detection & recovery

Негізгі қауіптер мен шабуыл түрлері

Шабуыл түрі	Мақсаты
DoS/DDoS	Жүйені тоқтату, ресурстарды босату
Replay attacks	Алдыңғы пакеттерді қайта жіберу
Man-in-the-middle	Байланысты ұстап өзгерту
Sensor spoofing	Жалған сигнал беру (IoT/авто)
Ransomware	Жүйені блоктау
Time-sync attack	Уақытты бұзу (RT жүйелерде өте қауіпті)

Қауіпсіздік архитектурасы

Қорғаныс қабаттары:

Физикалық қауіпсіздік

Аутентификация және криптография

Бейне бақылау, IDS, firewall

Хаттамалық қорғаныс (TLS, DTLS)

Синхрондау қауіпсіздігі (NTP Secure)

Blockchain элементтері (опционалды)

Қауіпсіздік технологиялары:

TLS/DTLS, IPSec

Шифрлау протоколдары

Secure MQTT, Zero Trust IoT

IoT қауіпсіздігі

PKI infrastructure

Ашық кілт инфрақұрылымы

TPM / HSM модульдері

Аппараттық қауіпсіздік

Сенімділікті қамтамасыз ету әдістері

Әдіс	Сипаттамасы
Репликация	Бірнеше көшірме ұстап, бірі істемесе екіншісі жұмыс істейді
Мажоритарлы келісім	Paxos / Raft протоколдары
Hot-standby	Резервтік сервер дайын тұрады
Fault detection	Ping/watchdog, health-check
Load balancing	Жүктемені бөлу
Checkpointing	Қалпына келу үшін күйді сақтау

Протоколдар мен технологиялар

Технология	Қолдану аймағы
DDS (Data Distribution Service)	Авиация, робототехника
OPC UA Secure	Өндірістік жүйелер
MQTT-SN, CoAP DTLS	IoT қауіпсіз жіберу
IEEE 1588 PTP	Дәл уақыт синхрондауы
Kafka Security, Kerberos	Журнал/лог және жүйе бақылау

Қолданылу салалары

Өндіріс

PLC, SCADA, Industry 4.0

Автономды көлік

LIDAR, камера, ECU coordination

Энергетика

Smart Grid

Медицина

Пациент мониторингі

Әскери

UAV network, radar control

Қорытынды

Үлестірілген нақты уақыт жүйелерінде қауіпсіздік пен сенімділік — ең маңызды талаптардың бірі.

Мұндай жүйелерде:

Уақтылық (deadline)
Міндетті түрде сақталуы тиіс

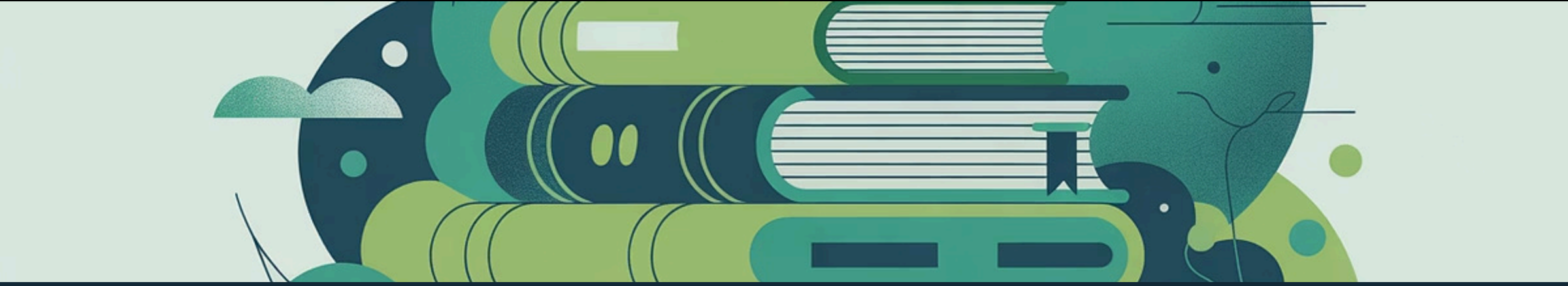
Деректер тұтастығы
Міндетті түрде сақталуы тиіс

Үздіксіз жұмыс
Міндетті түрде сақталуы тиіс

Қорғаныс механизмі – көпқабатты, адаптивті және fault-tolerant болуы қажет.

Бақылау сұрақтары

1. Үлестірілген нақты уақыт жүйесінің негізгі ерекшеліктері қандай?
2. CIA моделі қандай компоненттерден тұрады?
3. DoS және replay шабуылдарының айырмашылығы?
4. Fault tolerance дегеніміз не?
5. Нақты уақыттағы жүйелердің қауіпсіздігі неге күрделі?



Пайдаланылған әдебиеттер

1. Tanenbaum A.S., Steen M. Distributed Systems.
2. Kopetz H. Real-Time Systems Design Principles.
3. Leveson N. Safeware: System Safety and Computers.
4. NIST Cyber-Physical Systems Framework.
5. IEC 62443 Industrial Cybersecurity Standard.
6. MITRE ICS Security Guidelines.
7. IEEE 1588 Precision Time Protocol Standard.