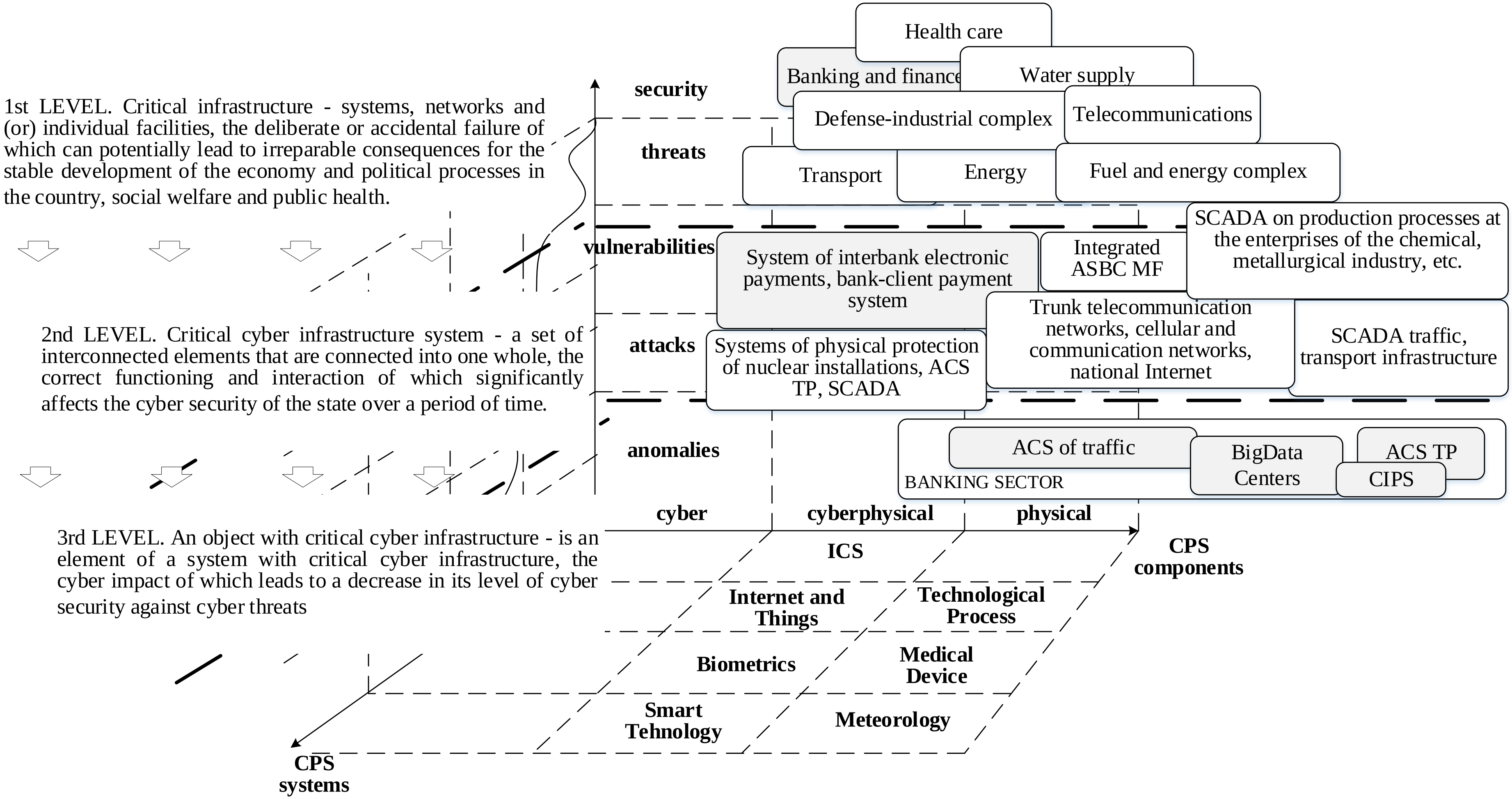
Cyber security in innovative technologies

Oleksandr Milov

National Technical University “Kharkiv polytechnic institute”

Internet of Things
Open Data
Smart Agriculture
Smart Retail
Smart Home
Smart Mobility
Education
Smart Grid/ Smart Energy
Smart Health
Smart Government

The scheme of interconnection of the structure with CCIS, on the example of organizations in the transport sector

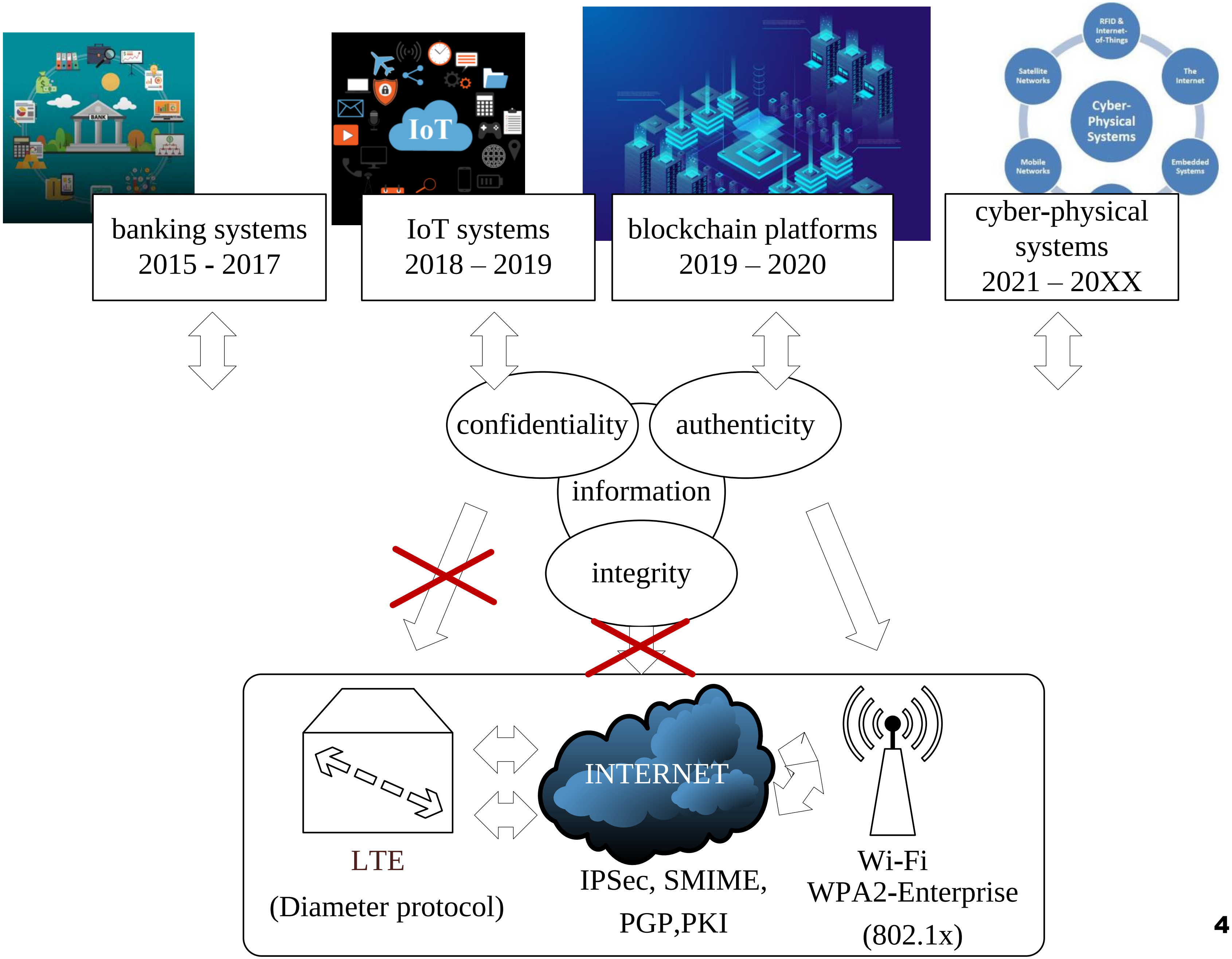


1st LEVEL. Critical infrastructure - systems, networks and (or) individual facilities, the deliberate or accidental failure of which can potentially lead to irreparable consequences for the stable development of the economy and political processes in the country, social welfare and public health.

2nd LEVEL. Critical cyber infrastructure system - a set of interconnected elements that are connected into one whole, the correct functioning and interaction of which significantly affects the cyber security of the state over a period of time.

3rd LEVEL. An object with critical cyber infrastructure - is an element of a system with critical cyber infrastructure, the cyber impact of which leads to a decrease in its level of cyber security against cyber threats

security
threats
vulnerabilities
attacks
anomalies
Health care
Banking and finance
Water supply
Defense-industrial complex
Telecommunications
Transport
Energy
Fuel and energy complex
SCADA on production processes at the enterprises of the chemical, metallurgical industry, etc.
System of interbank electronic payments, bank-client payment system
Integrated ASBC MF
Trunk telecommunication networks, cellular and communication networks, national Internet
SCADA traffic, transport infrastructure
Systems of physical protection of nuclear installations, ACS TP, SCADA
ACS of traffic
BigData Centers
ACS TP
CIPS
BANKING SECTOR
cyber
cyberphysical
physical
CPS components
ICS
Internet and Things
Technological Process
Biometrics
Medical Device
Smart Tehnology
Meteorology
CPS systems



banking systems
2015 - 2017

IoT systems
2018 – 2019

blockchain platforms
2019 – 2020

cyber-physical
systems
2021 – 20XX

confidentiality

authenticity

information

integrity

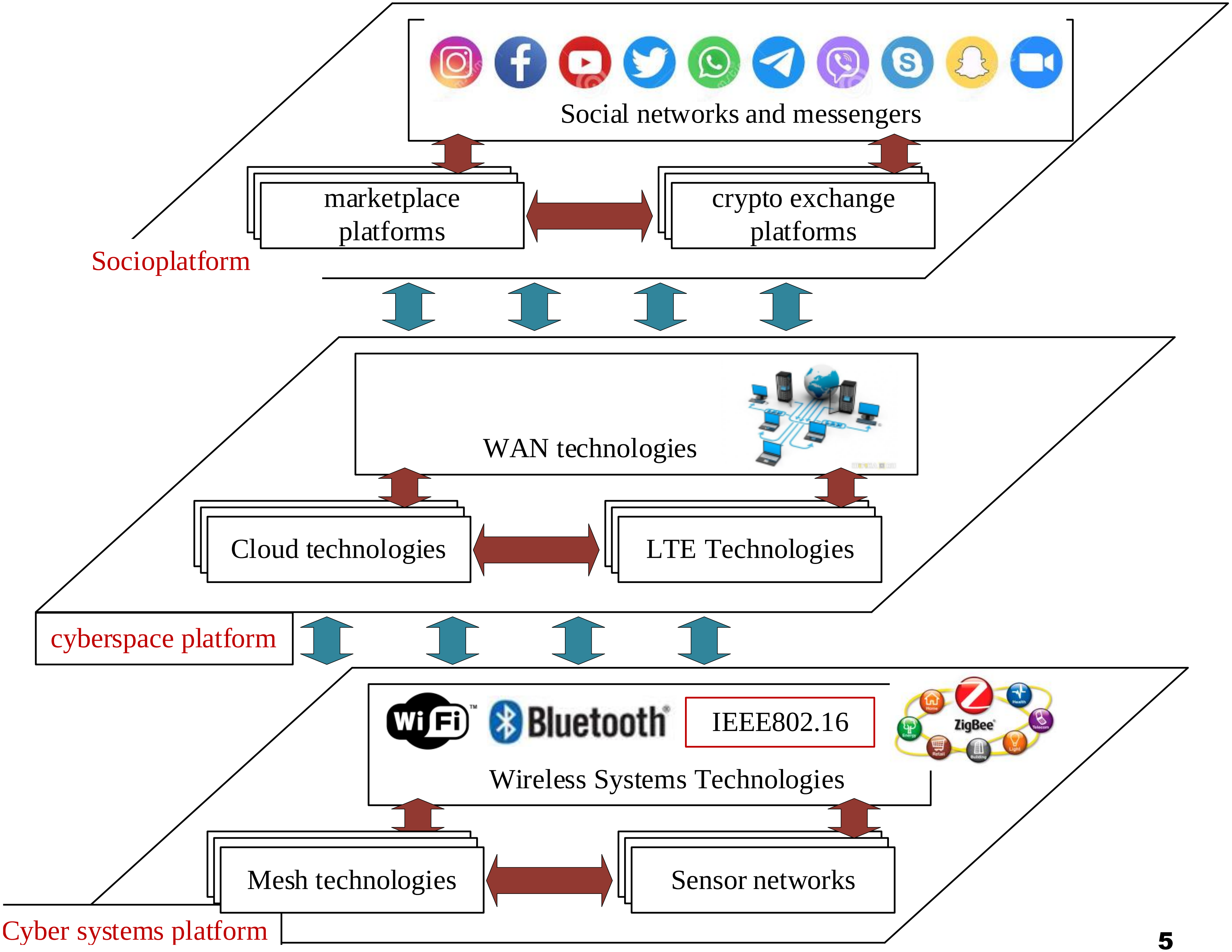
INTERNET

LTE
(Diameter protocol)

IPSec, SMIME,
PGP,PKI

Wi-Fi
WPA2-Enterprise
(802.1x)

Structural-logical scheme of SCPS



Social networks and messengers

marketplace platforms

crypto exchange platforms

Socioplatform

WAN technologies

Cloud technologies

LTE Technologies

cyberspace platform

IEEE802.16

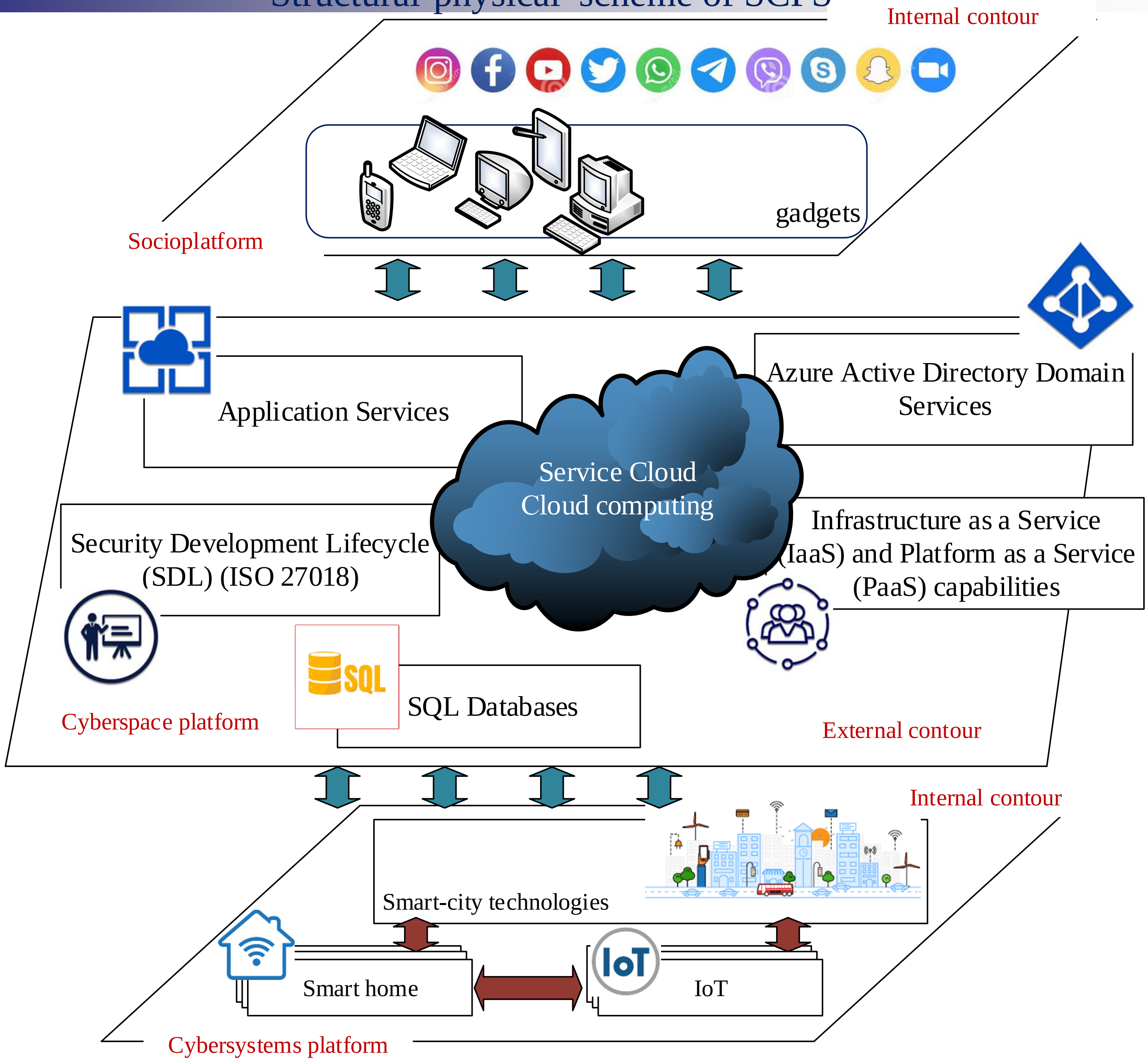
Wireless Systems Technologies

Mesh technologies

Sensor networks

Cyber systems platform

Structural-physical scheme of SCPS



Internal contour

gadgets

Socioplatform

Application Services

Azure Active Directory Domain Services

Service Cloud
Cloud computing

Security Development Lifecycle (SDL) (ISO 27018)

Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) capabilities

SQL Databases

Cyberspace platform

External contour

Internal contour

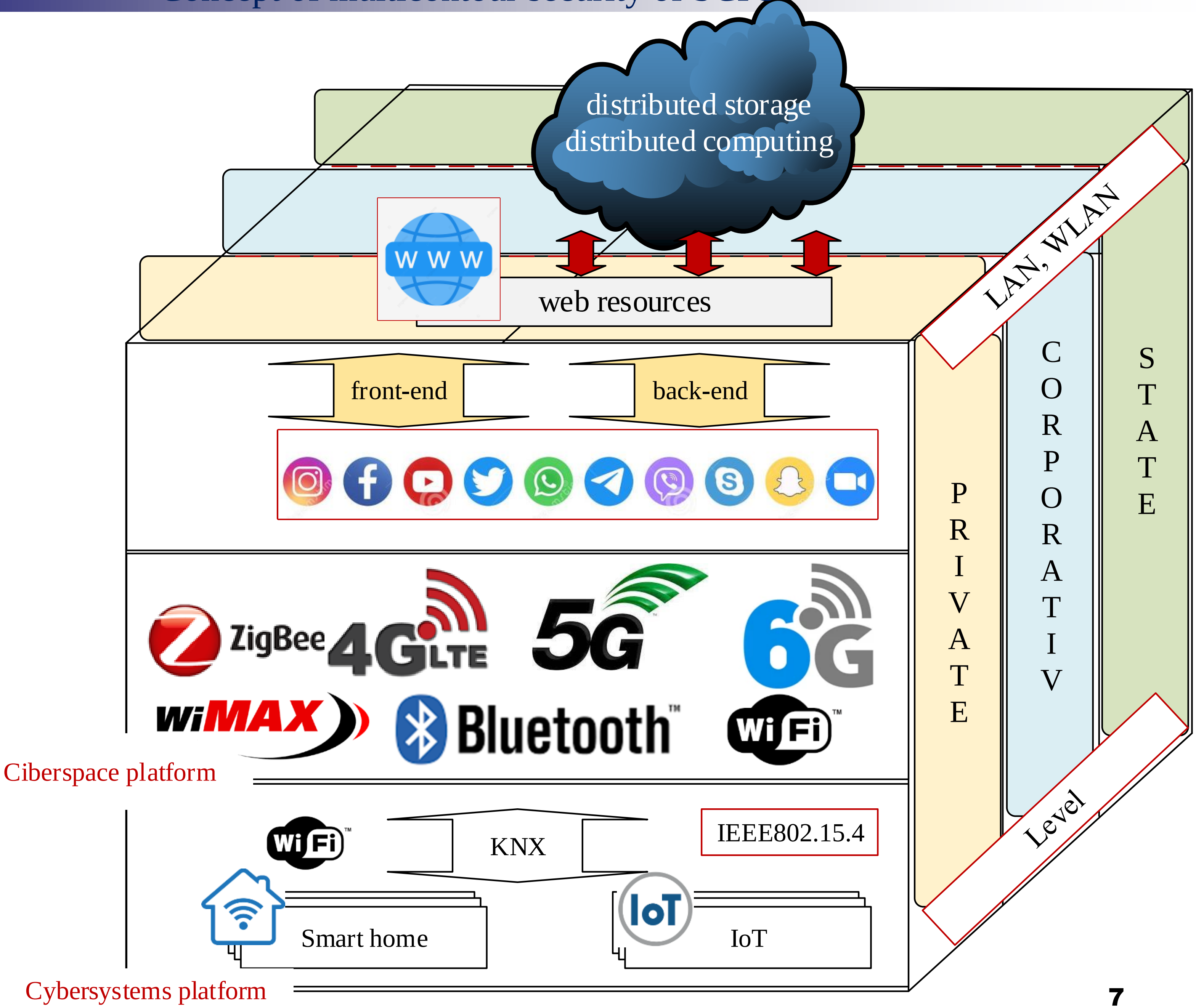
Smart-city technologies

Smart home

IoT

Cybersystems platform

Concept of multicontour security of SCPS



distributed storage
distributed computing

web resources

front-end

back-end

Ciberspace platform

KNX

IEEE802.15.4

Smart home

IoT

Cybersystems platform

LAN, WLAN

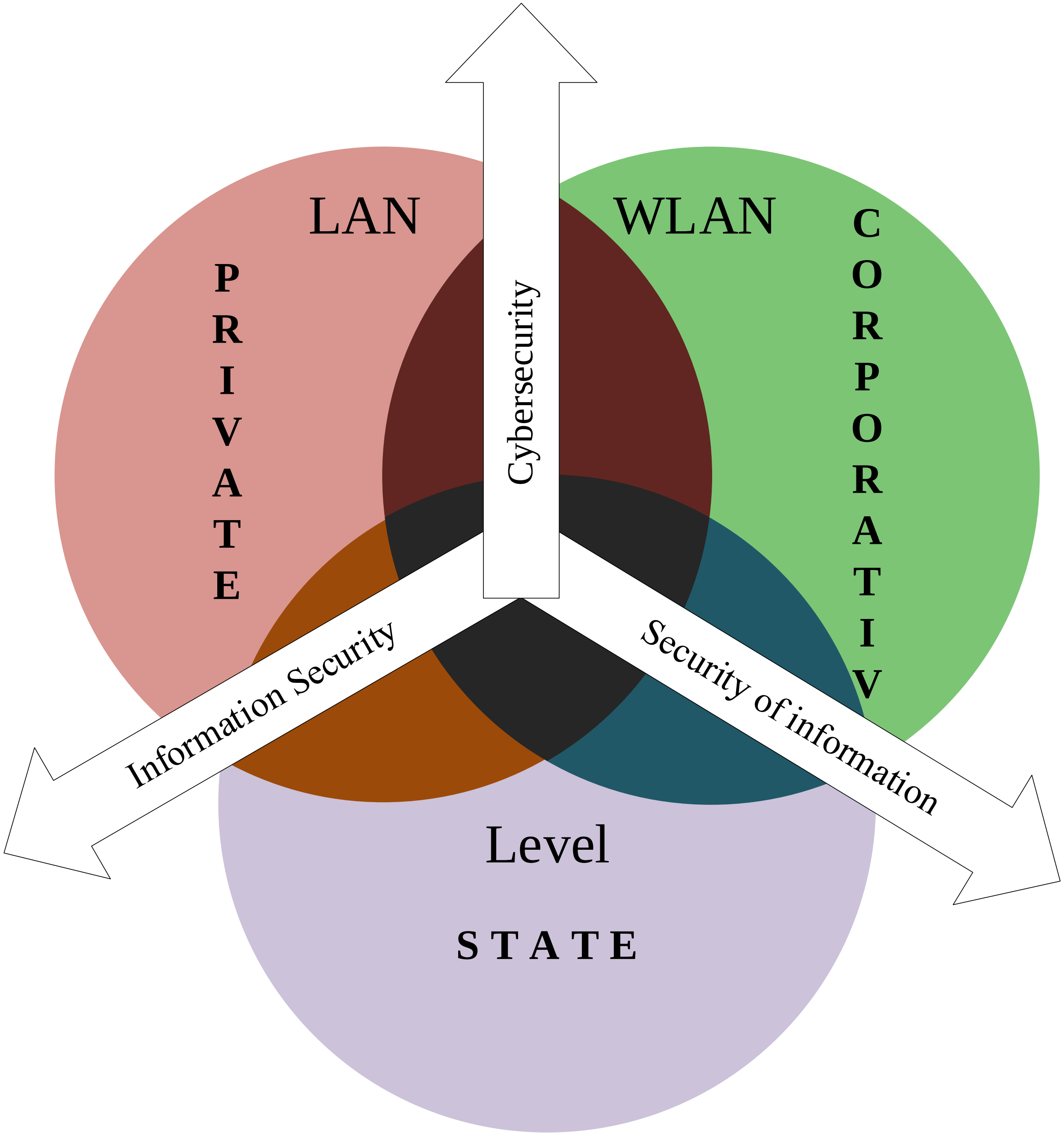
PRIVATE

CORPORATIV

STATE

Level

Structural and logical scheme of threats to SCPS



Formal description of the Concept

– *threats of the internal contour, taking into account the hybridity and synergy of threats* for the 1st platform – social networks:

$$W^{SS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{1\text{platform}}} = W^{SS\ ISL\qquad C}_{synerg_{1\text{platform}}} \cap W^{SS\ ISL\qquad I}_{synerg_{1\text{platform}}} \cap W^{SS\ ISL\qquad A}_{synerg_{1\text{platform}}} \cap W^{SS\ ISL\qquad Au}_{synerg_{1\text{platform}}} \cap W^{SS\ ISL\qquad Inv}_{synerg_{1\text{platform}}},$$

– *threats of the internal contour, taking into account the hybridity and synergy of threats* for the 2nd platform – cyberspace:

$$W^{CS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} = W^{CS\ ISL\qquad C}_{synerg_{2\text{platform}}} \cap W^{CS\ ISL\qquad I}_{synerg_{2\text{platform}}} \cap W^{CS\ ISL\qquad A}_{synerg_{2\text{platform}}} \cap W^{CS\ ISL\qquad Au}_{synerg_{2\text{platform}}} \cap W^{CS\ ISL\qquad Inv}_{synerg_{2\text{platform}}},$$

– *threats of the internal contour, taking into account the hybridity and synergy of threats* for the 3rd platform – cyber-physical systems:

$$W^{CPS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}} = W^{CPS\ ISL\qquad C}_{synerg_{3\text{platform}}} \cap W^{CPS\ ISL\qquad I}_{synerg_{3\text{platform}}} \cap W^{CPS\ ISL\qquad A}_{synerg_{3\text{platform}}} \cap W^{CPS\ ISL\qquad Au}_{synerg_{3\text{platform}}} \cap W^{CPS\ ISL\qquad Inv}_{synerg_{3\text{platform}}},$$

Formal description of the Concept

General assessment of threats of the internal contour, taking into account the technologies of the socio-cyber-physical system

$$\boxed{W_{ISL}^{CPSS} = W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{1platform}}}^{SS\ ISL} \cup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{2platform}}}^{CS\ ISL} \cup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{3platform}}}^{CPS\ ISL}}$$

General assessment of threats of the internal contour, taking into account the form of ownership of the elements and technologies of the socio-cyber-physical system

$$\boxed{W_{ISL_{\text{general}}}^{CPSS} = W_{ISL_{\text{private.}}}^{CPSS} \cup W_{ISL_{\text{state}}}^{CPSS} \cup W_{ISL_{\text{corporativ}}}^{CPSS},}$$

General assessment of threats of the internal contour, taking into account the technologies of the socio-cyber-physical system

$$\boxed{\begin{gathered} W_{ESL}^{CPSS} = W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{1platform}}}^{SS\ ESL} \cup \\ \cup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{2platform}}}^{CS\ ESL} \cup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{\text{3platform}}}^{CPS\ ESL} \end{gathered}}$$

General assessment of threats of the internal contour, taking into account the form of ownership of the elements and technologies of the socio-cyber-physical system

$$\boxed{W_{ESL_{\text{general}}}^{CPSS} = W_{ESL_{\text{private.}}}^{CPSS} \cup W_{ESL_{\text{state}}}^{CPSS} \cup W_{ESL_{\text{corporativ}}}^{CPSS},}$$

Formal description of the Concept

generalized assessment of a multicontour security system, we use the formula

$$W^{CPSS}_{\text{final}} = W^{CPSS}_{ISL_{\text{general}}} \bigcup W^{CPSS}_{ESL_{\text{general}}} .$$

general (current) level of socio-cyber-physical systems security based on wireless mobile technologies is described by the expression:

– for additive convolution

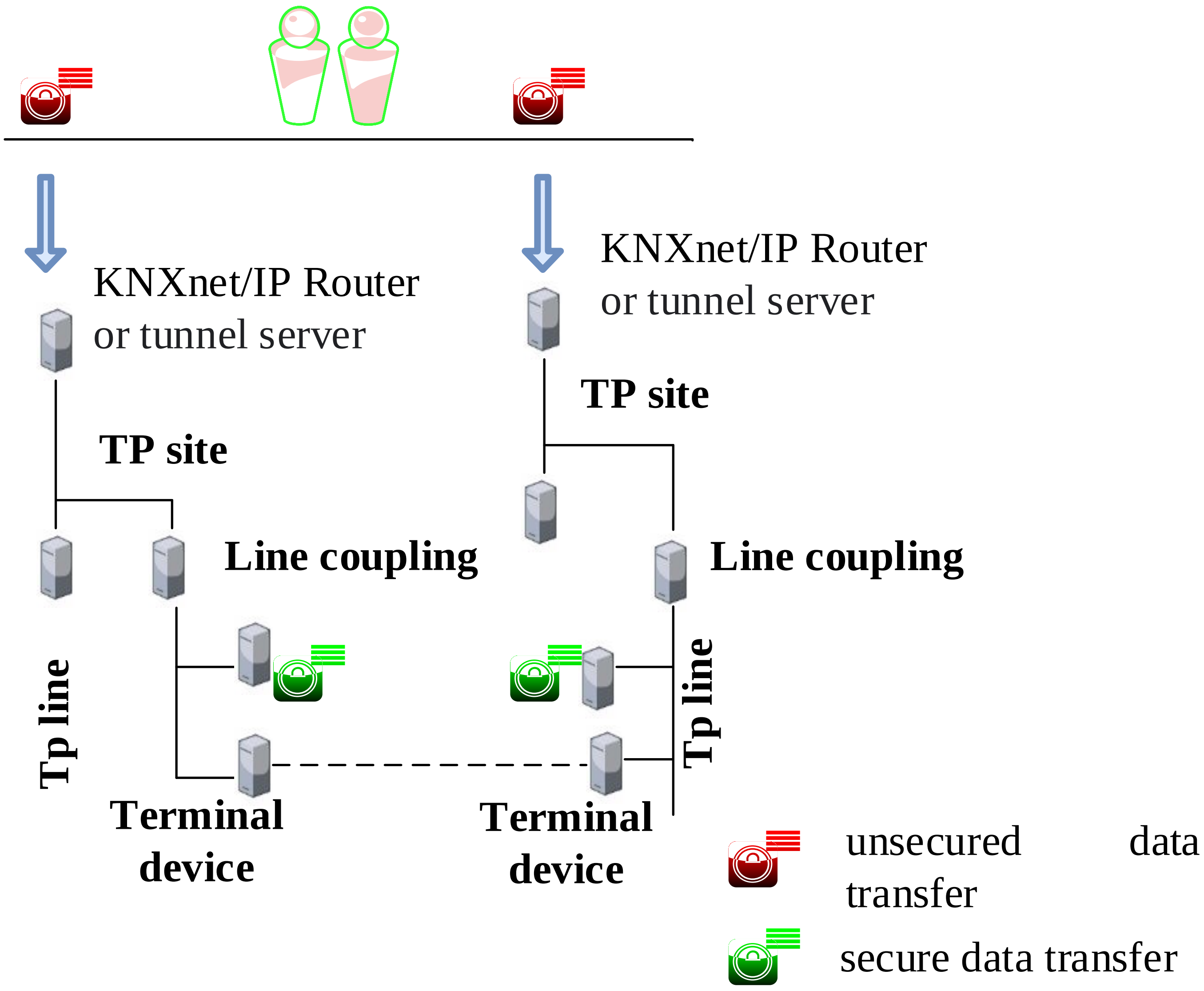
$$L_{W^{CPSS}_{\text{security}}} = L_{ISL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij} \right) + L_{ESL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij} \right).$$

– for multiplicative convolution

$$L_{W^{CPSS}_{\text{security}}} = 1 - \left[1 - L_{ISL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij} \right) \right] \times \left[1 - L_{ESL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij} \right) \right].$$

β_i – a metric of the ratio of time and information confidentiality degree for an asset (critical – 1,0; high – 0,75; medium – 0,5; low – 0,25; very low – 0,01)

Ensuring security in mobile wireless channels based on KNX



KNXnet/IP Router or tunnel server

KNXnet/IP Router or tunnel server

TP site

TP site

Line coupling

Line coupling

Tp line

Tp line

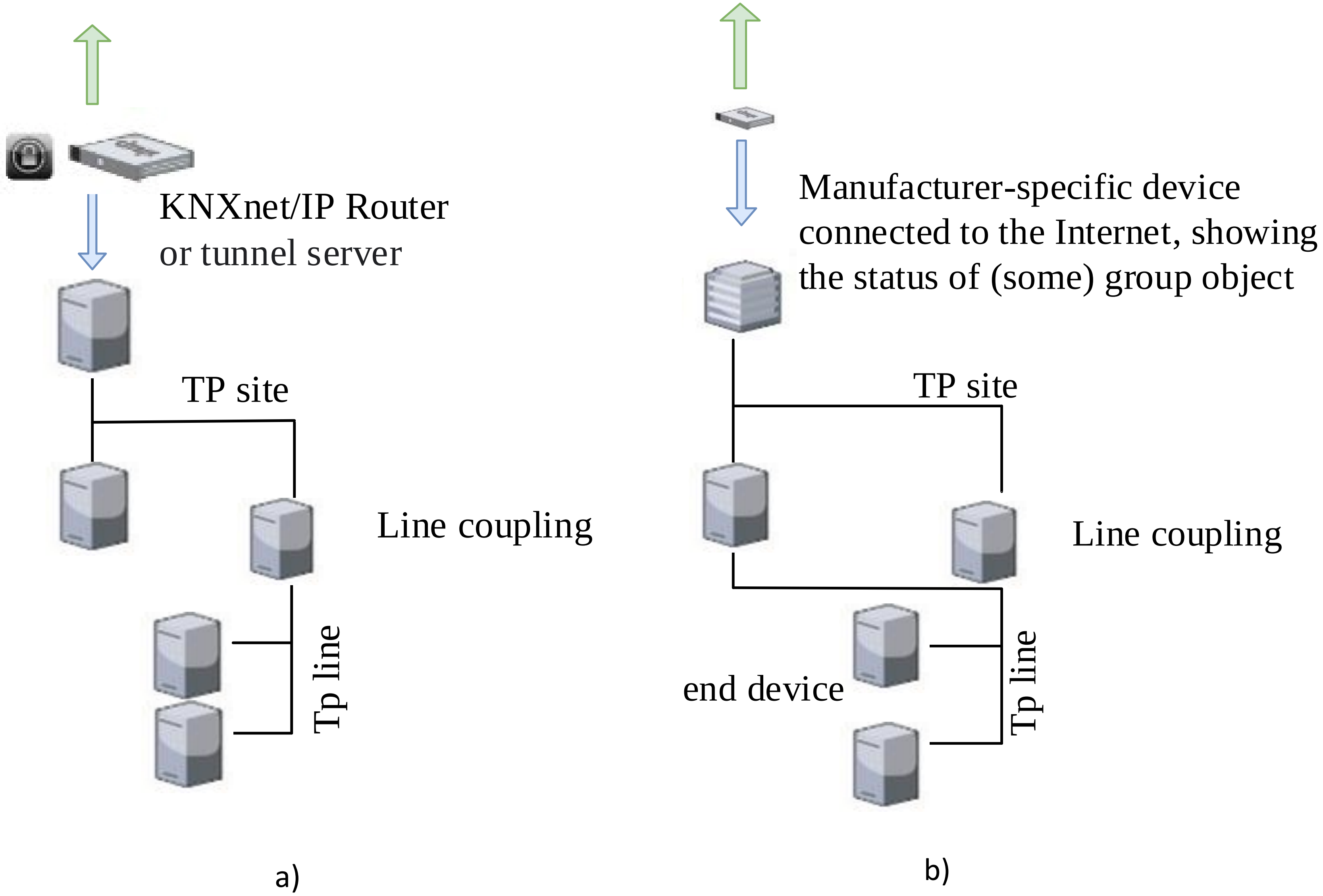
Terminal device

Terminal device

🟥 unsecured data transfer

🟩 secure data transfer

Ensuring security in mobile wireless channels based on KNX



KNXnet/IP Router
or tunnel server

TP site

Line coupling

Tp line

a)

Manufacturer-specific device
connected to the Internet, showing
the status of (some) group object

TP site

Line coupling

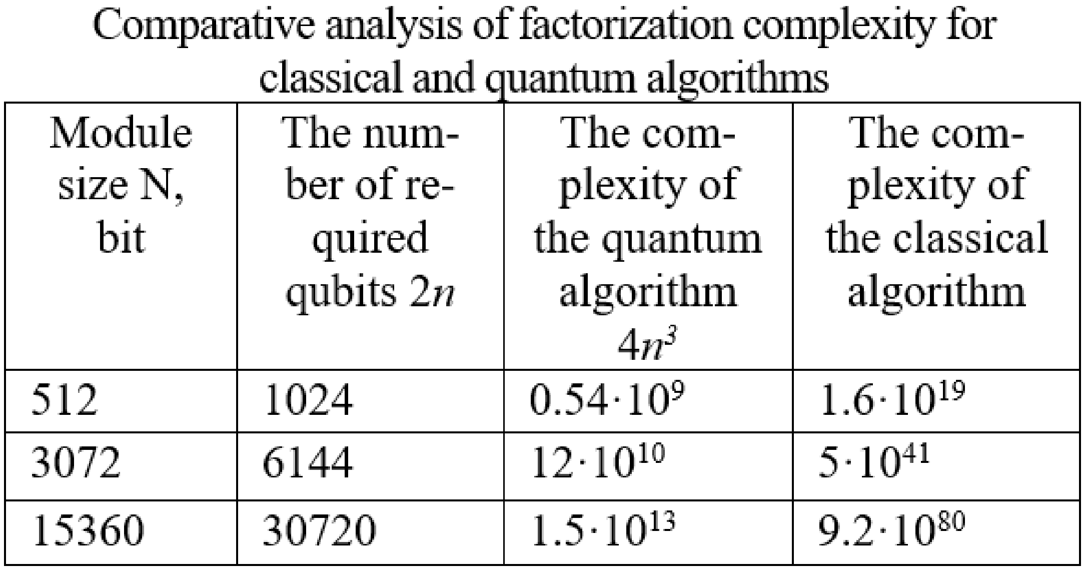
end device

Tp line

b)

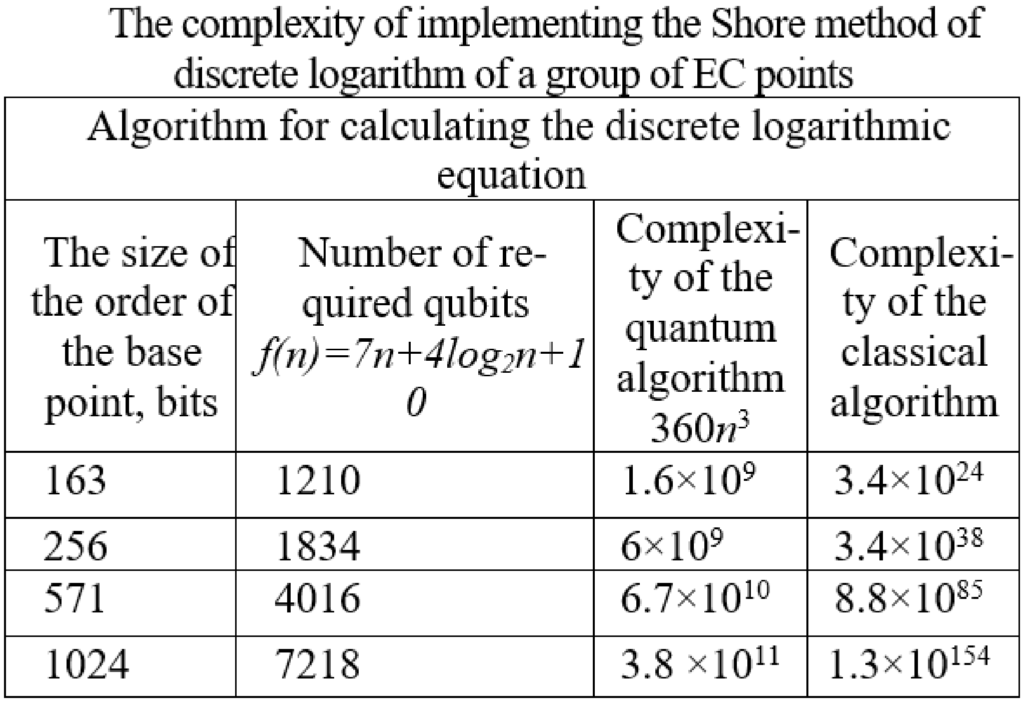
KNX Data Secure: *a* – KNX IP Secure; *b* – KNX Data Secure

the possibilities of quantum computing



Comparative analysis of factorization complexity for classical and quantum algorithms

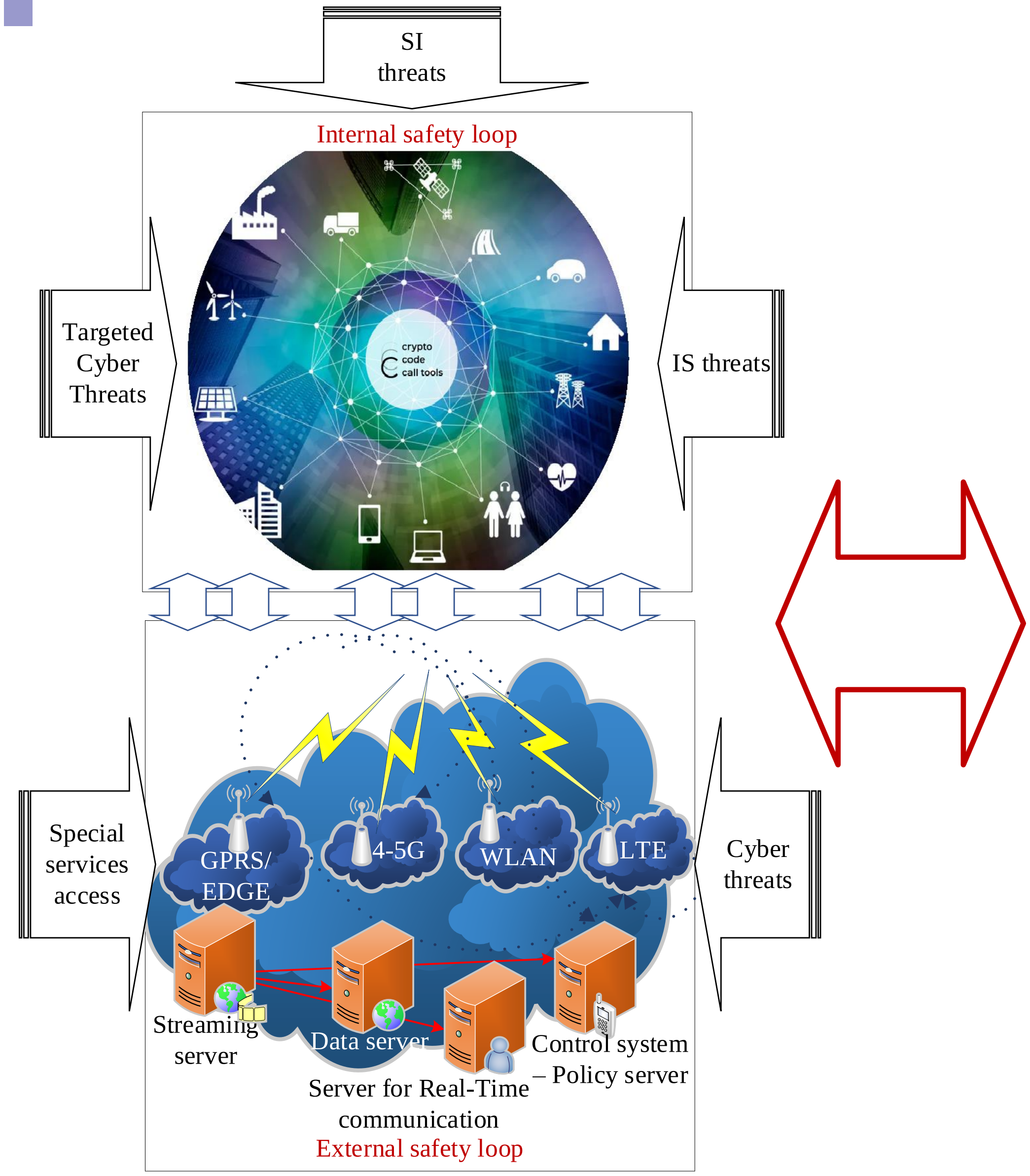
Module size N, bit	The number of required qubits $2n$	The complexity of the quantum algorithm $4n^3$	The complexity of the classical algorithm
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

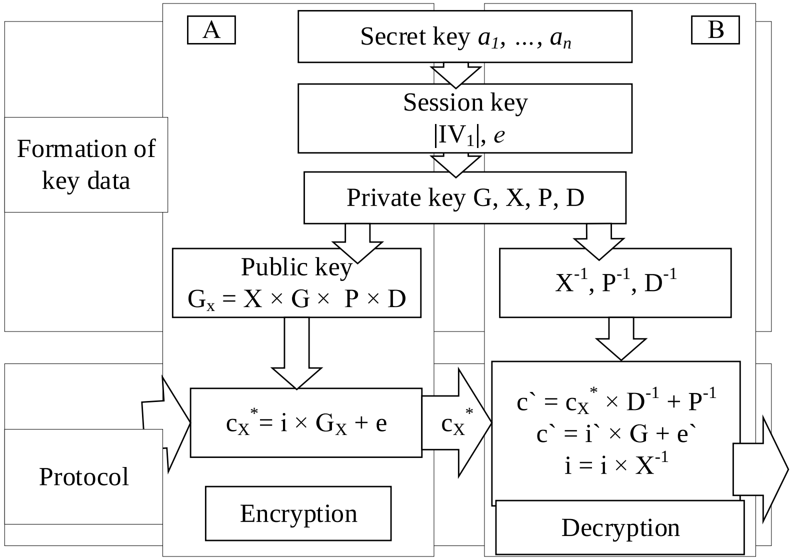


The complexity of implementing the Shore method of discrete logarithm of a group of EC points

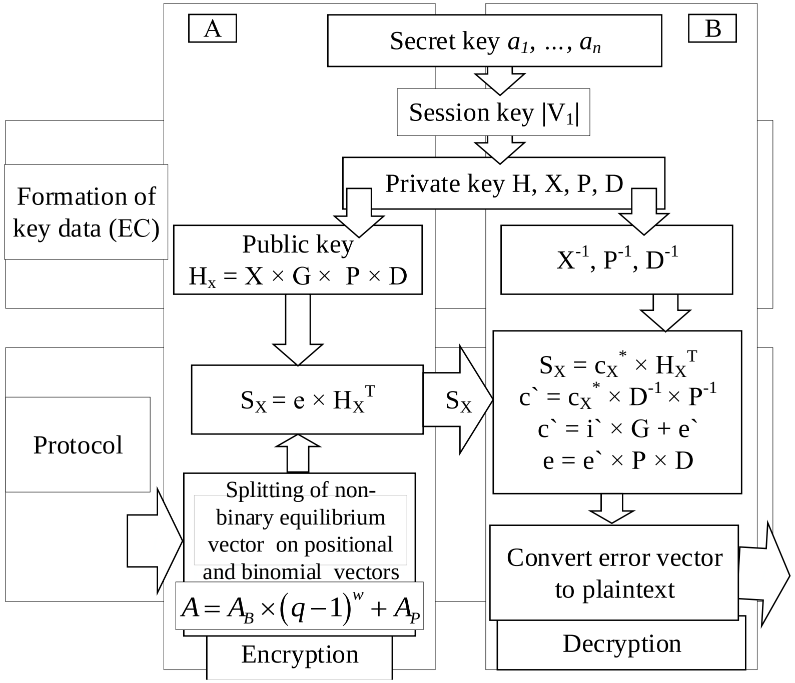
Algorithm for calculating the discrete logarithmic equation			
The size of the order of the base point, bits	Number of required qubits $f(n)=7n+4log_2n+10$	Complexity of the quantum algorithm $360n^3$	Complexity of the classical algorithm
163	1210	1.6×10^9	3.4×10^{24}
256	1834	6×10^9	3.4×10^{38}
571	4016	6.7×10^{10}	8.8×10^{85}
1024	7218	3.8×10^{11}	1.3×10^{154}

Post-quantum security algorithms





McEliece crypto-code construction on the EC

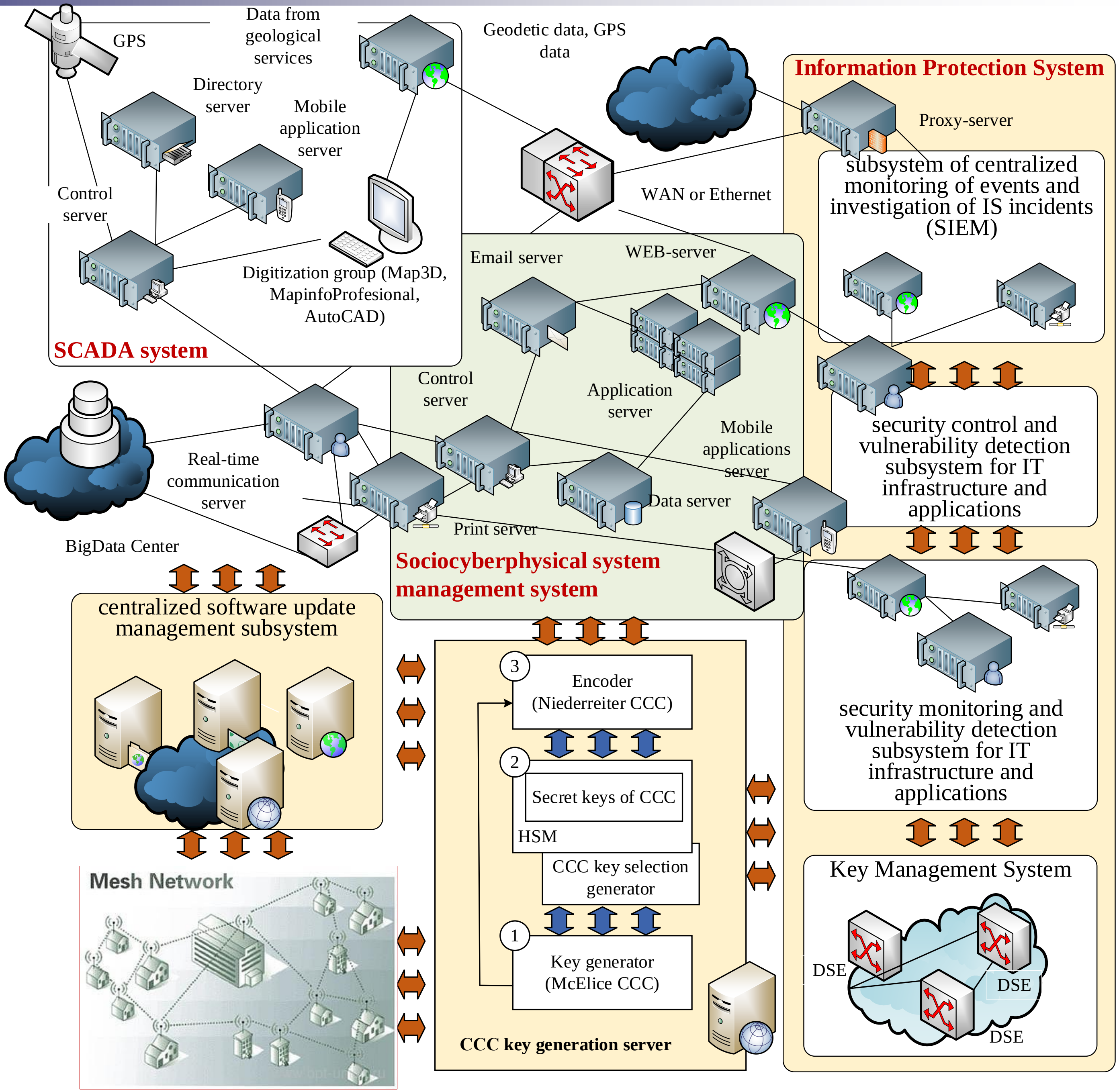


Niederreiter crypto-code construction on EC

Comparative characteristics of wireless and mobile Internet technologies

Technology	Provision of security services					The degree of information secrecy (β_i)				
	C	I	A	A_u	B	1,0	0,75	0,5	0,25	0,01
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (Wi-Fi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16m (WiMAX2)	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1 Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
Mobile technologies+ CCC EC(MEC)	+	+	+	+	+	+	+	+	+	+
Mobile technologies+ HCCC EC(MEC)	+	+	+	+	+	+	+	+	+	+
Mobile technologies+ CCC на LDPC	+	+	+	+	+	–	–	+	+	+

Ensuring security in a smart city



GPS

Data from geological services

Directory server

Mobile application server

Control server

Digitization group (Map3D, MapinfoProfesional, AutoCAD)

SCADA system

Geodetic data, GPS data

WAN or Ethernet

Information Protection System

Proxy-server

subsystem of centralized monitoring of events and investigation of IS incidents (SIEM)

Email server

WEB-server

Control server

Application server

Mobile applications server

Data server

Print server

Sociocyberphysical system management system

Real-time communication server

BigData Center

security control and vulnerability detection subsystem for IT infrastructure and applications

security monitoring and vulnerability detection subsystem for IT infrastructure and applications

centralized software update management subsystem

Mesh Network

3 Encoder (Niederreiter CCC)

2 Secret keys of CCC

HSM

CCC key selection generator

1 Key generator (McElice CCC)

CCC key generation server

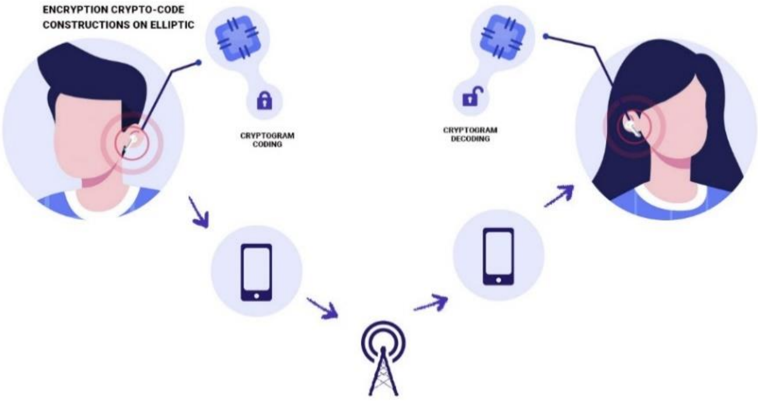
Key Management System

DSE

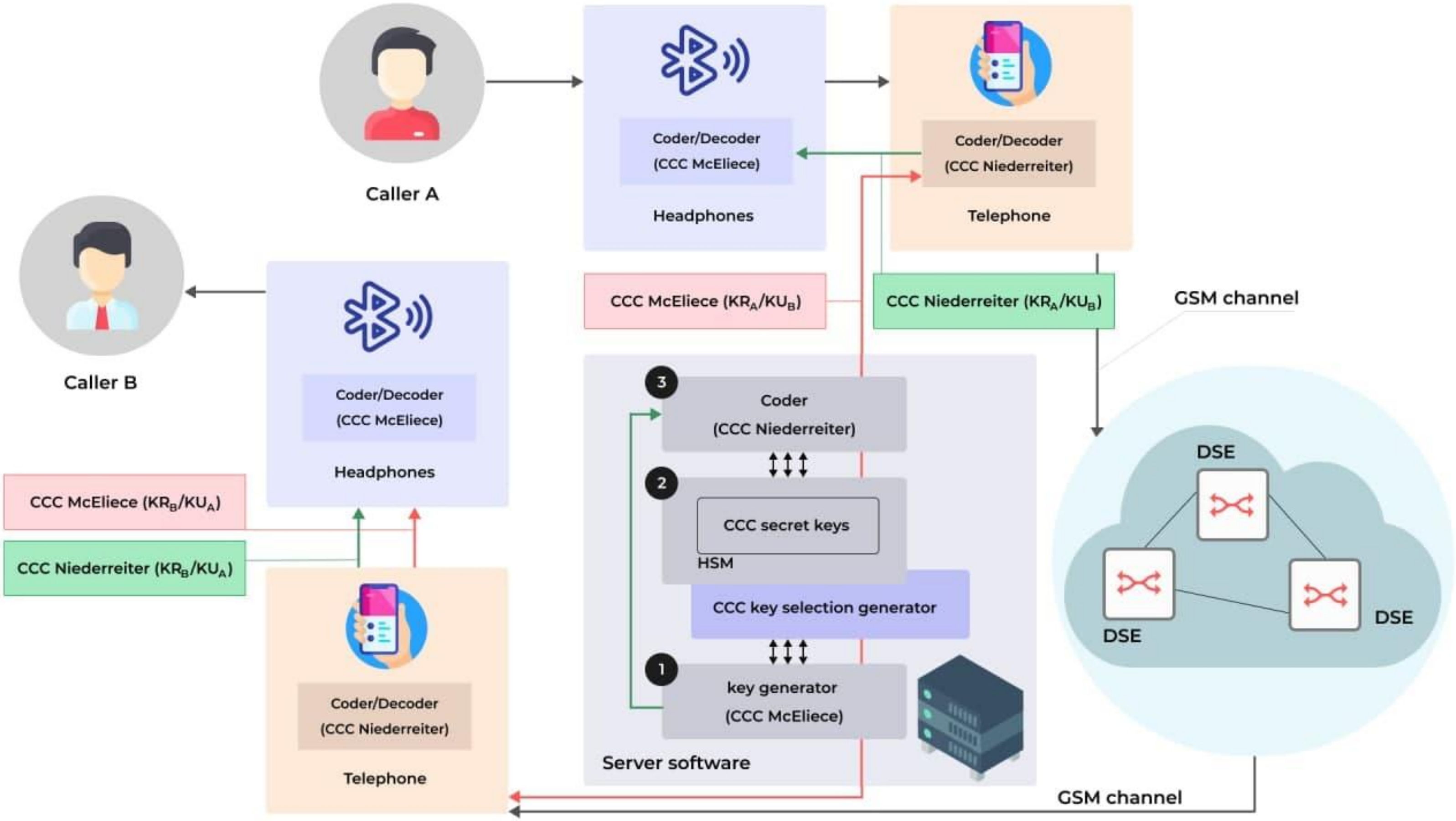
DSE

DSE

Ensuring security in a smart city



https://www.calltools.ua/


Caller A
Coder/Decoder (CCC McEliece)
Headphones
Coder/Decoder (CCC Niederreiter)
Telephone
CCC McEliece (KR$_A$/KU$_B$)
CCC Niederreiter (KR$_A$/KU$_B$)
GSM channel
Caller B
Coder/Decoder (CCC McEliece)
Headphones
CCC McEliece (KR$_B$/KU$_A$)
CCC Niederreiter (KR$_B$/KU$_A$)
Coder/Decoder (CCC Niederreiter)
Telephone
3
Coder (CCC Niederreiter)
2
CCC secret keys
HSM
CCC key selection generator
1
key generator (CCC McEliece)
Server software
DSE
DSE
DSE
GSM channel

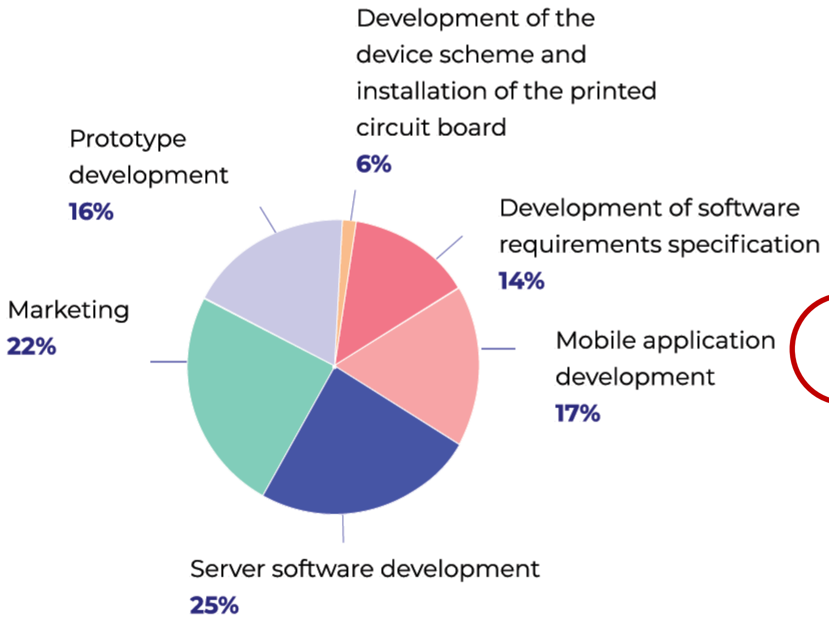
Ensuring security in a smart city

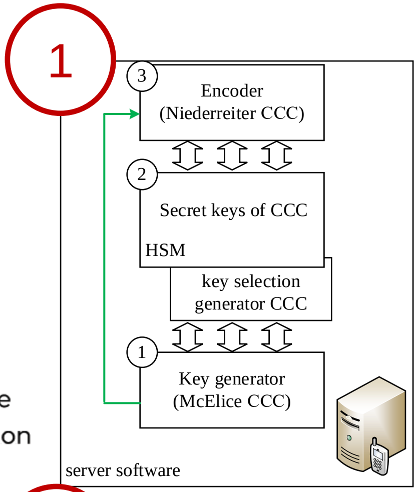
Creating an MVP

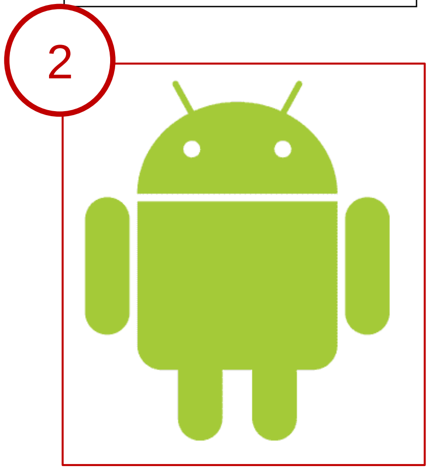
To create an MVP of the project

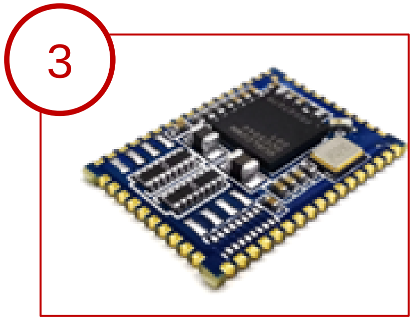
and to promote it, we need to

attract - **260000 $**





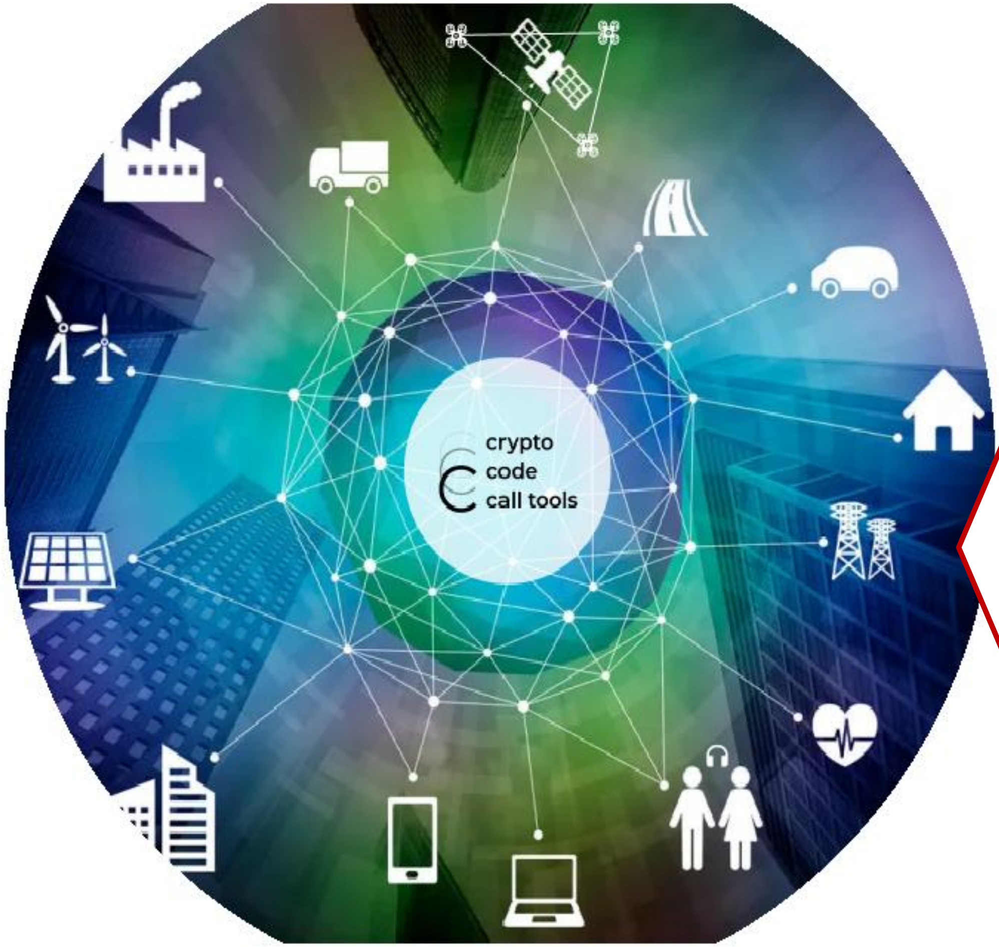


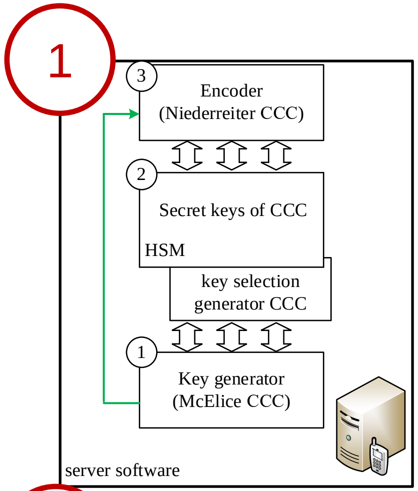


https://www.calltools.ua/

National Technical University “Kharkiv polytechnic institute”

Ensuring security in a smart city





3 Encoder (Niederreiter CCC)

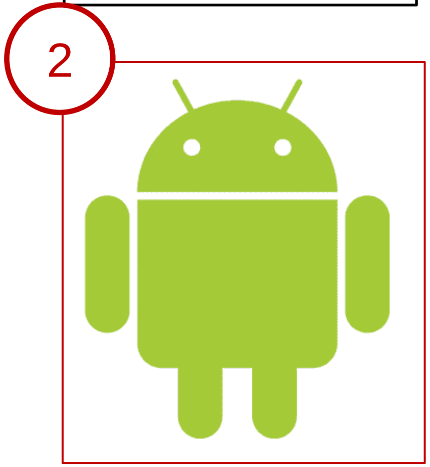
2 Secret keys of CCC

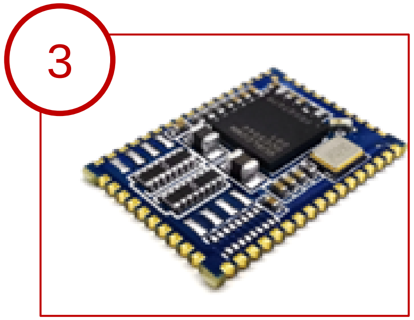
HSM

key selection generator CCC

1 Key generator (McElice CCC)

server software





Thank you for attention !

National Technical University “Kharkiv polytechnic institute”