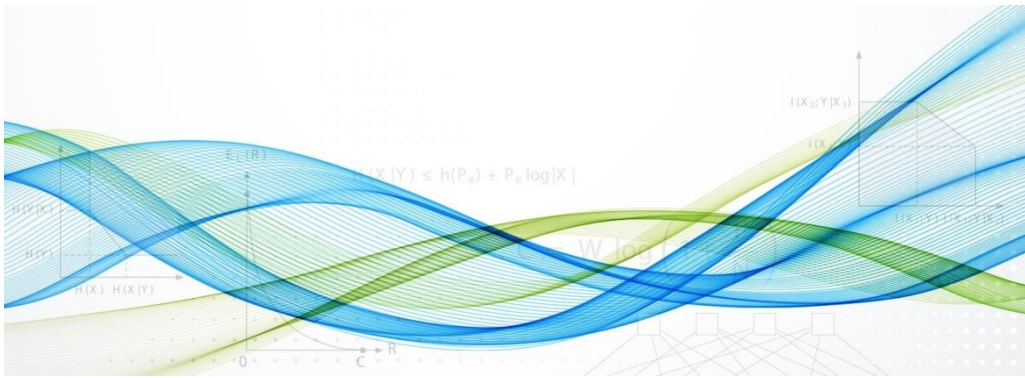
MicroCAD-2024

Методологія побудови багатоконтурної системи безпеки у соціокіберфізичних системах

Serhii Yevseiev

Olena Akhiiezer



National Technical University “Kharkiv Polytechnic Institute”

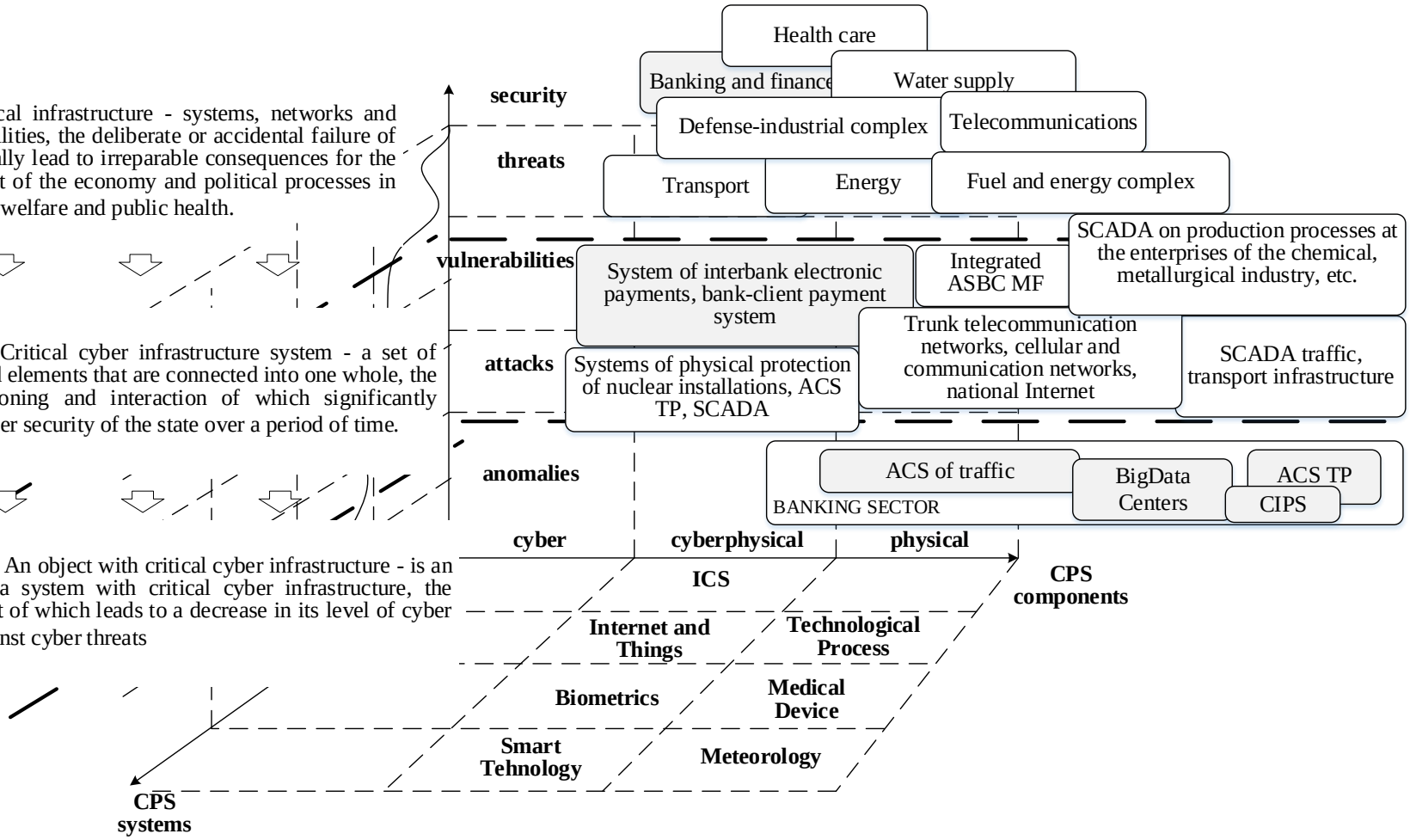

Internet of Things
Open Data
Smart Agriculture
Smart Retail
Smart Home
Smart Mobility
Education
Smart Health
Smart Grid/
Smart Energy
Smart Government

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

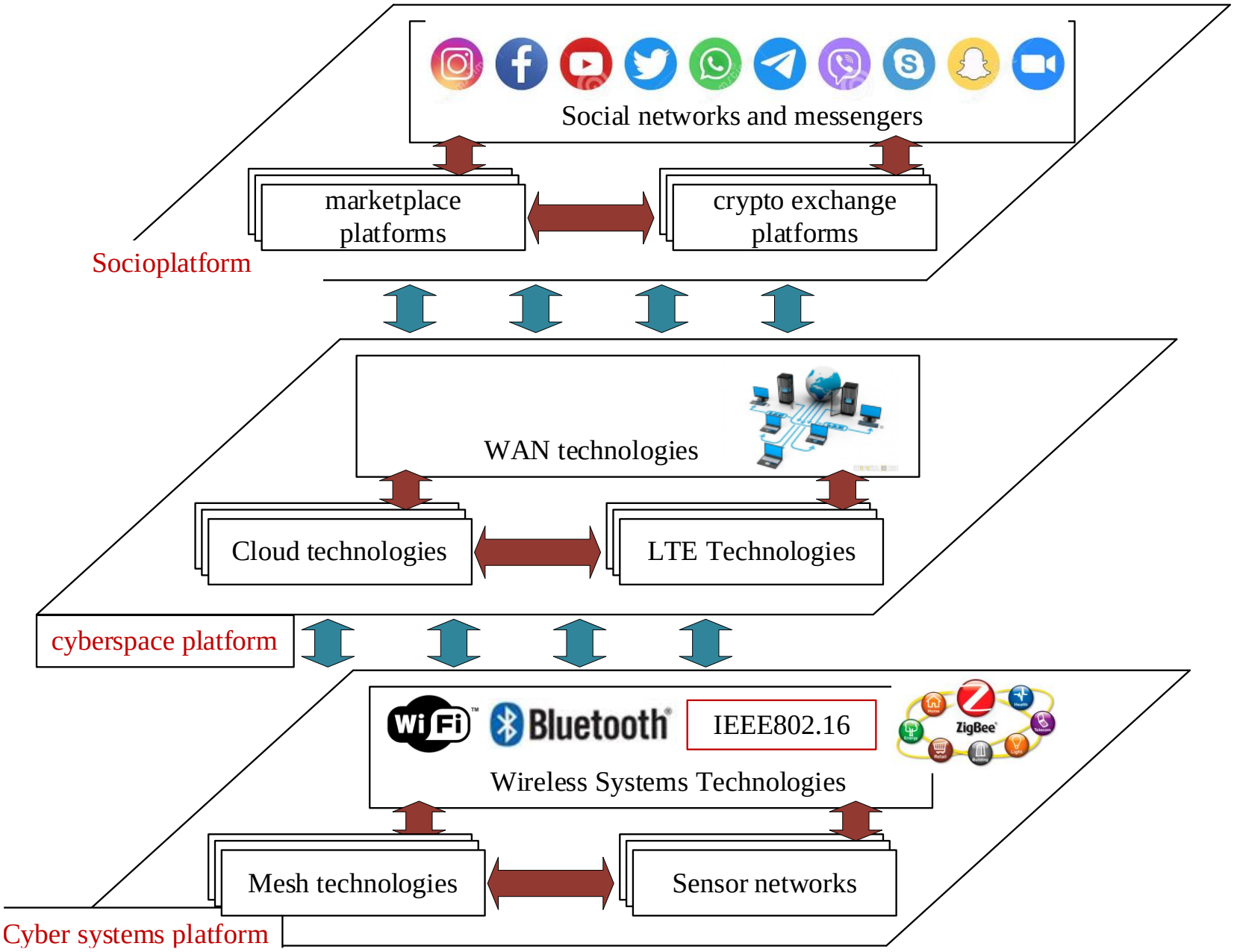
1st LEVEL. Critical infrastructure - systems, networks and (or) individual facilities, the deliberate or accidental failure of which can potentially lead to irreparable consequences for the stable development of the economy and political processes in the country, social welfare and public health.

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.

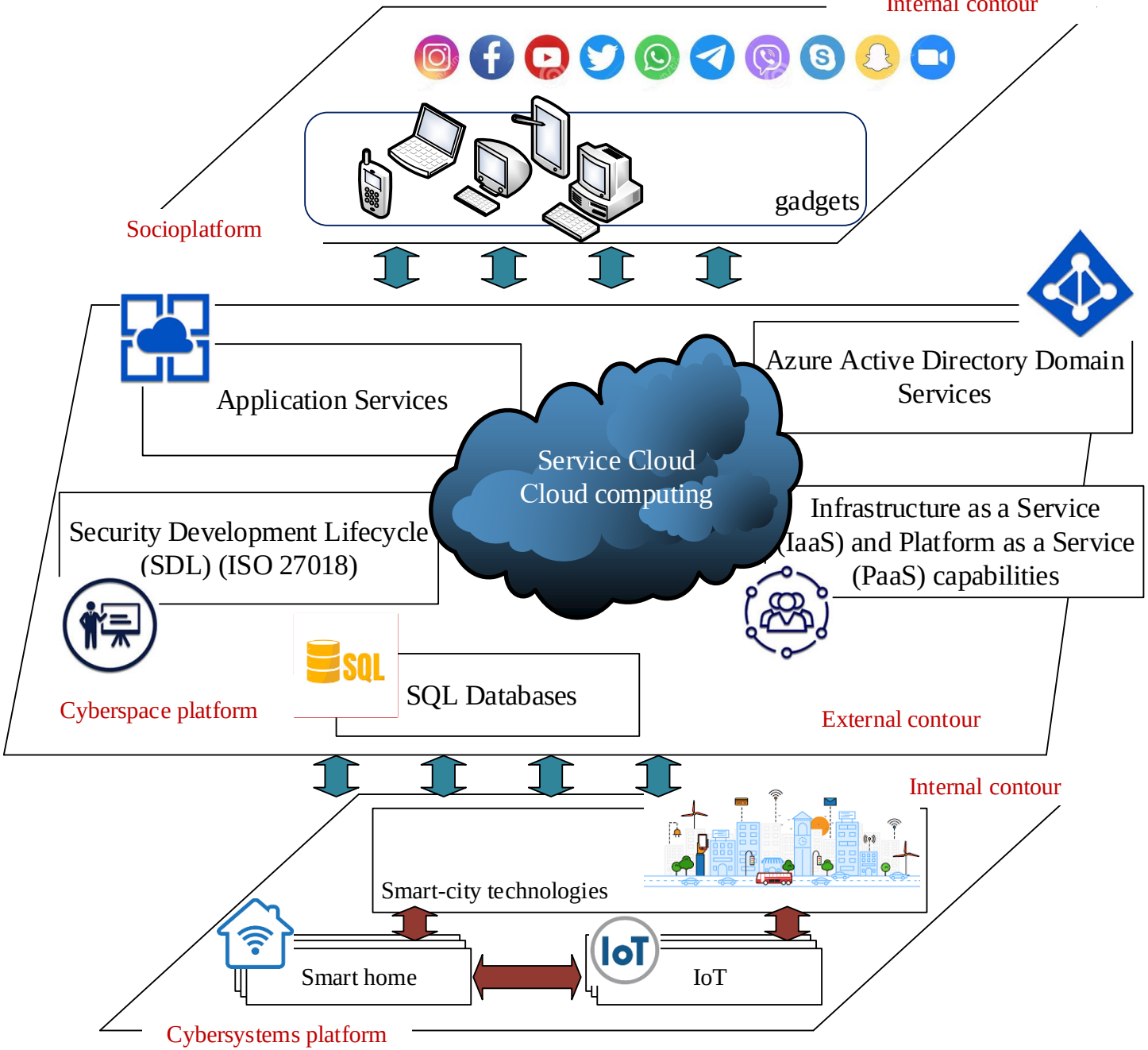
3rd LEVEL. An object with critical cyber infrastructure - is an element of a system with critical cyber infrastructure, the cyber impact of which leads to a decrease in its level of cyber security against cyber threats

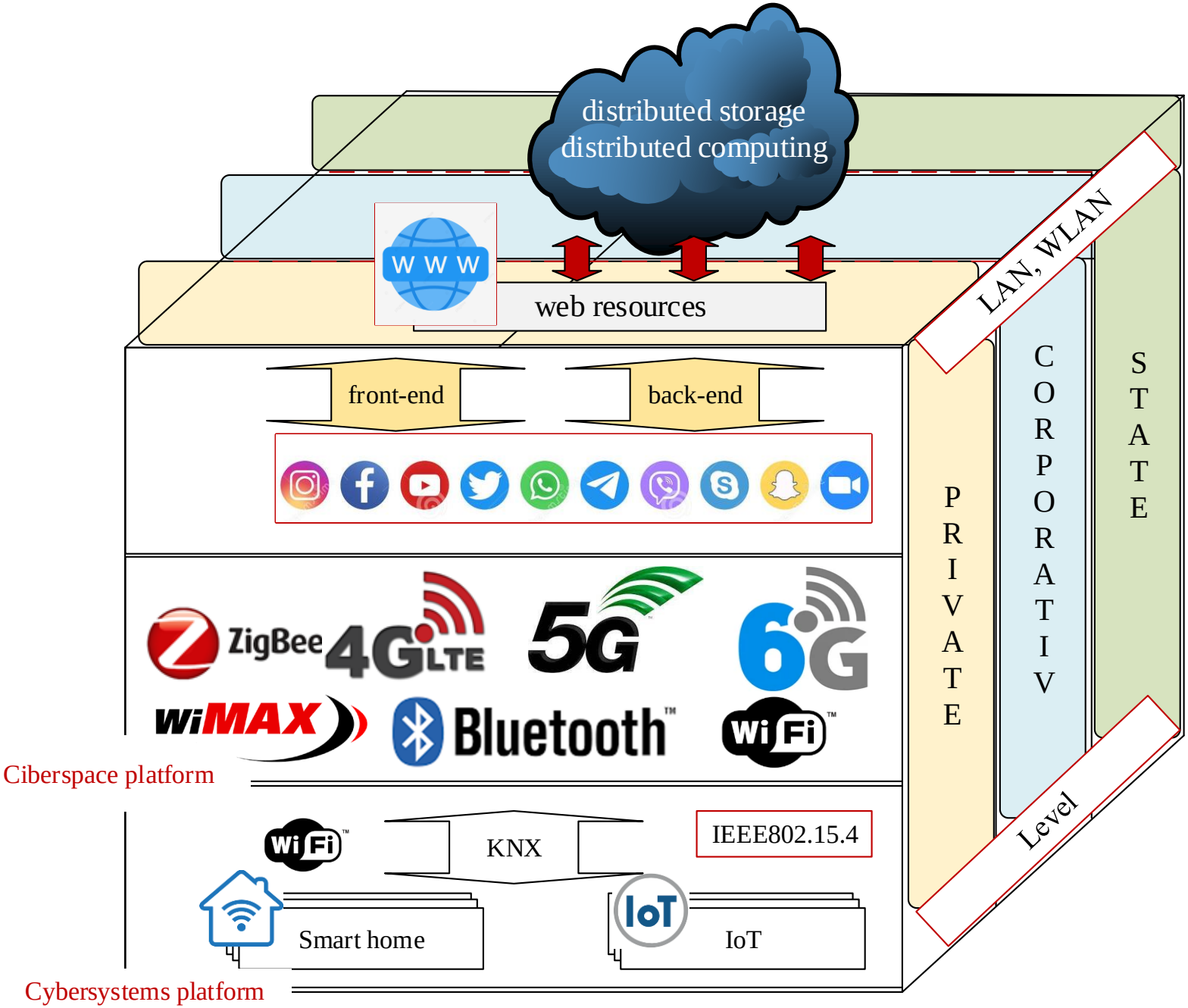


STRUCTURAL-LOGICAL SCHEME OF SCPS

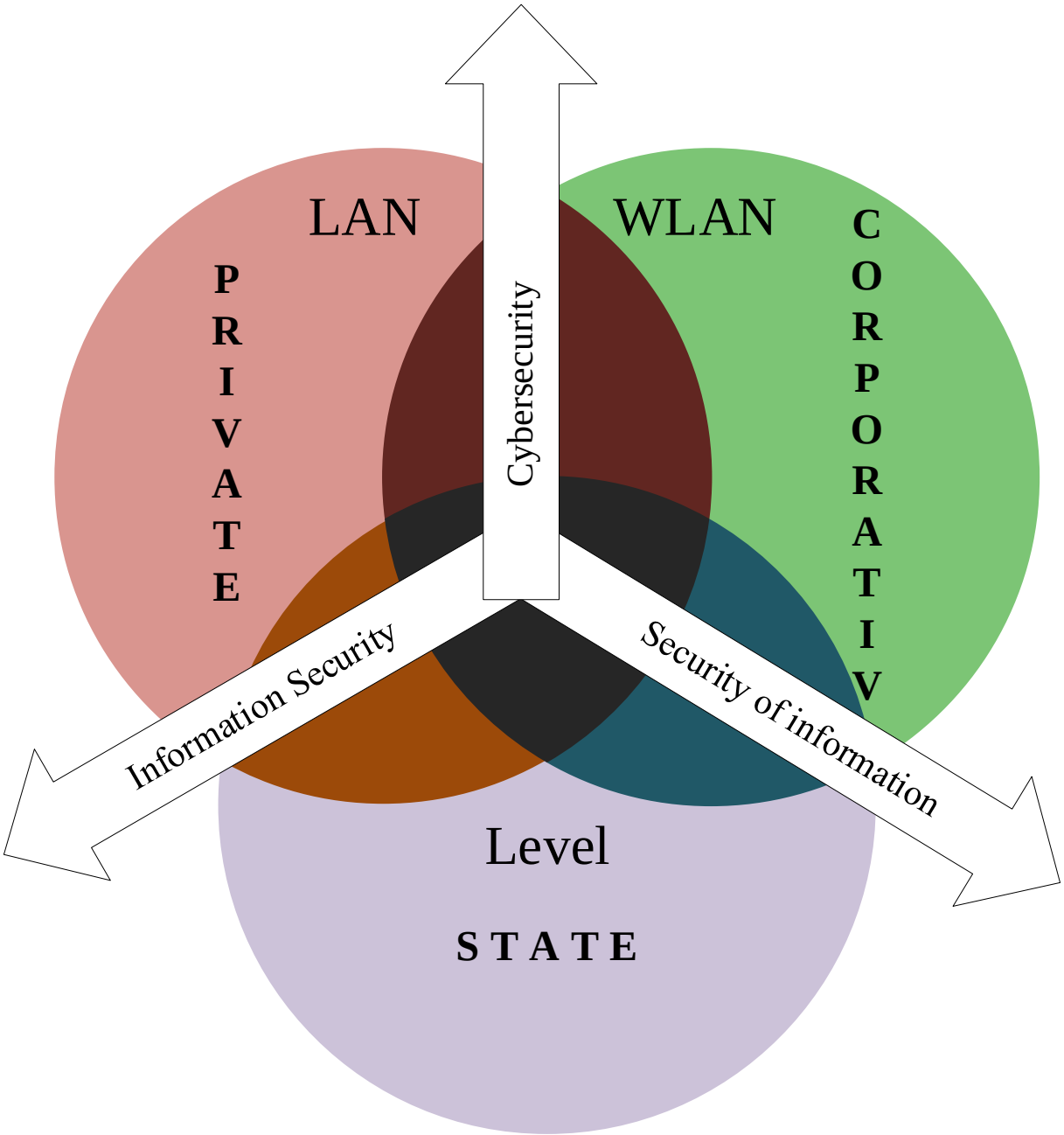


STRUCTURAL-PHYSICAL SCHEME OF SCPS

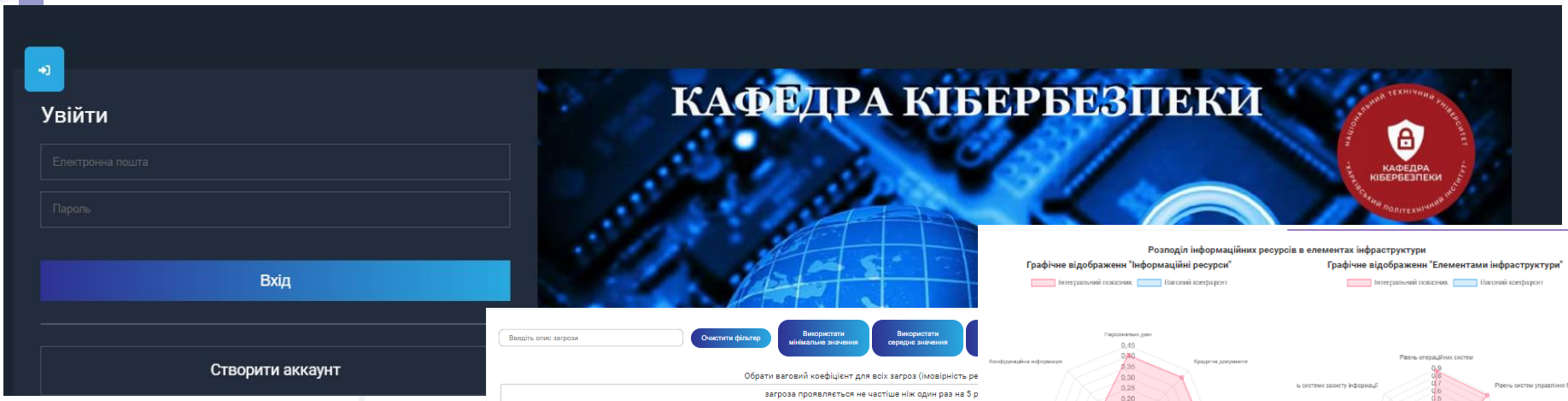


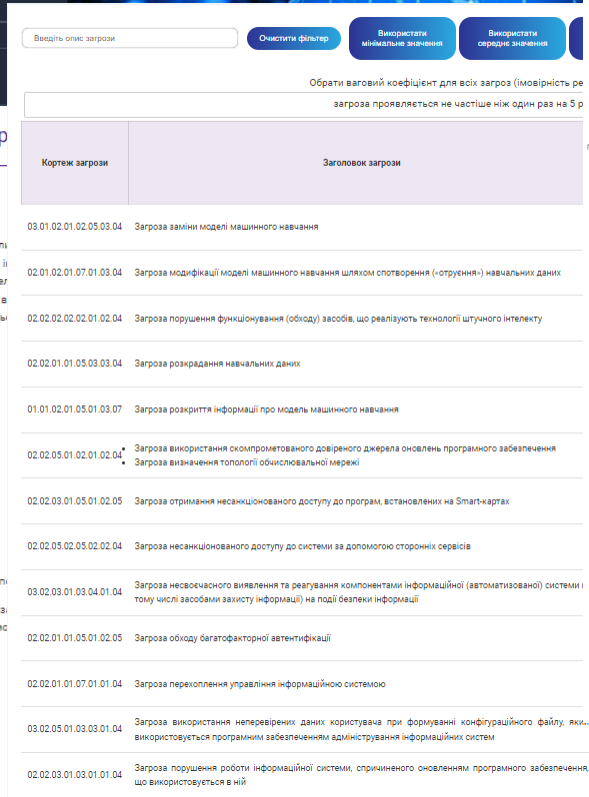

distributed storage
distributed computing
W W W
web resources
front-end
back-end
LAN, WLAN
PRIVATE
CORPORATIV
STATE
ZigBee
4G LTE
5G
6G
WiMAX
Bluetooth
Wi Fi
Ciberspace platform
Wi Fi
KNX
IEEE802.15.4
Smart home
IoT
IoT
Level
Cybersystems platform

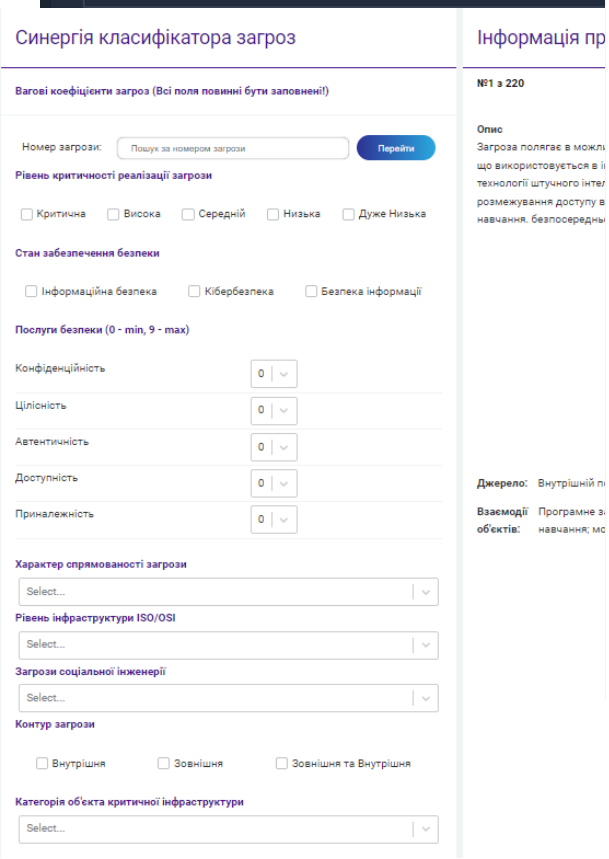
STRUCTURAL AND LOGICAL SCHEME OF THREATS TO SCPS

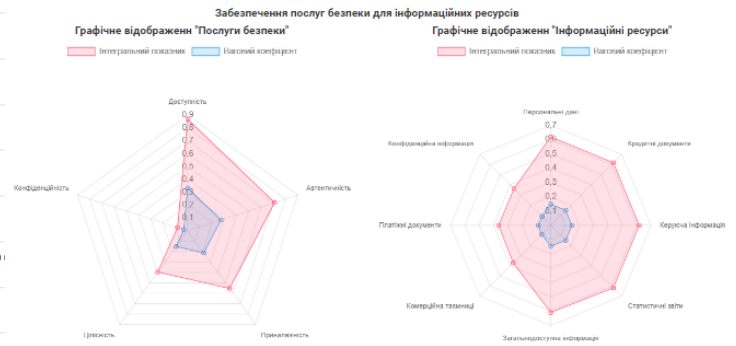


CLASSIFIER OF THREAT OF INFORMATION RESOURCES SCPS









https://skl.sspu.sumy.ua/

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

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

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

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

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

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

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

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

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

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

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

$$W_{ESL}^{CPSS} = W_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}}^{SS\ ESL} \bigcup$$

$$\bigcup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}}^{CS\ ESL} \bigcup W_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}}^{CPS\ ESL}$$

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

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

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

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

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

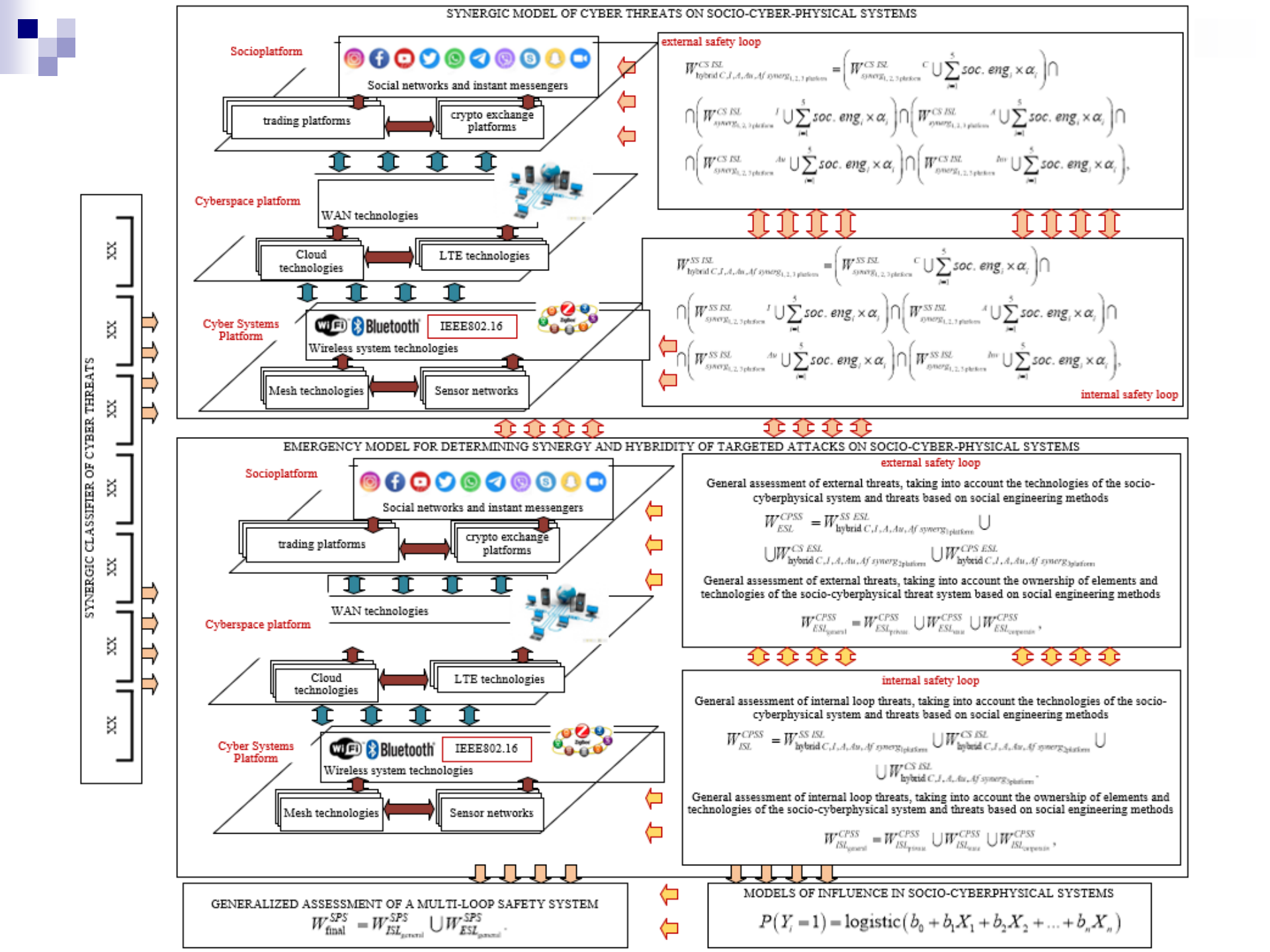
– for additive convolution

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

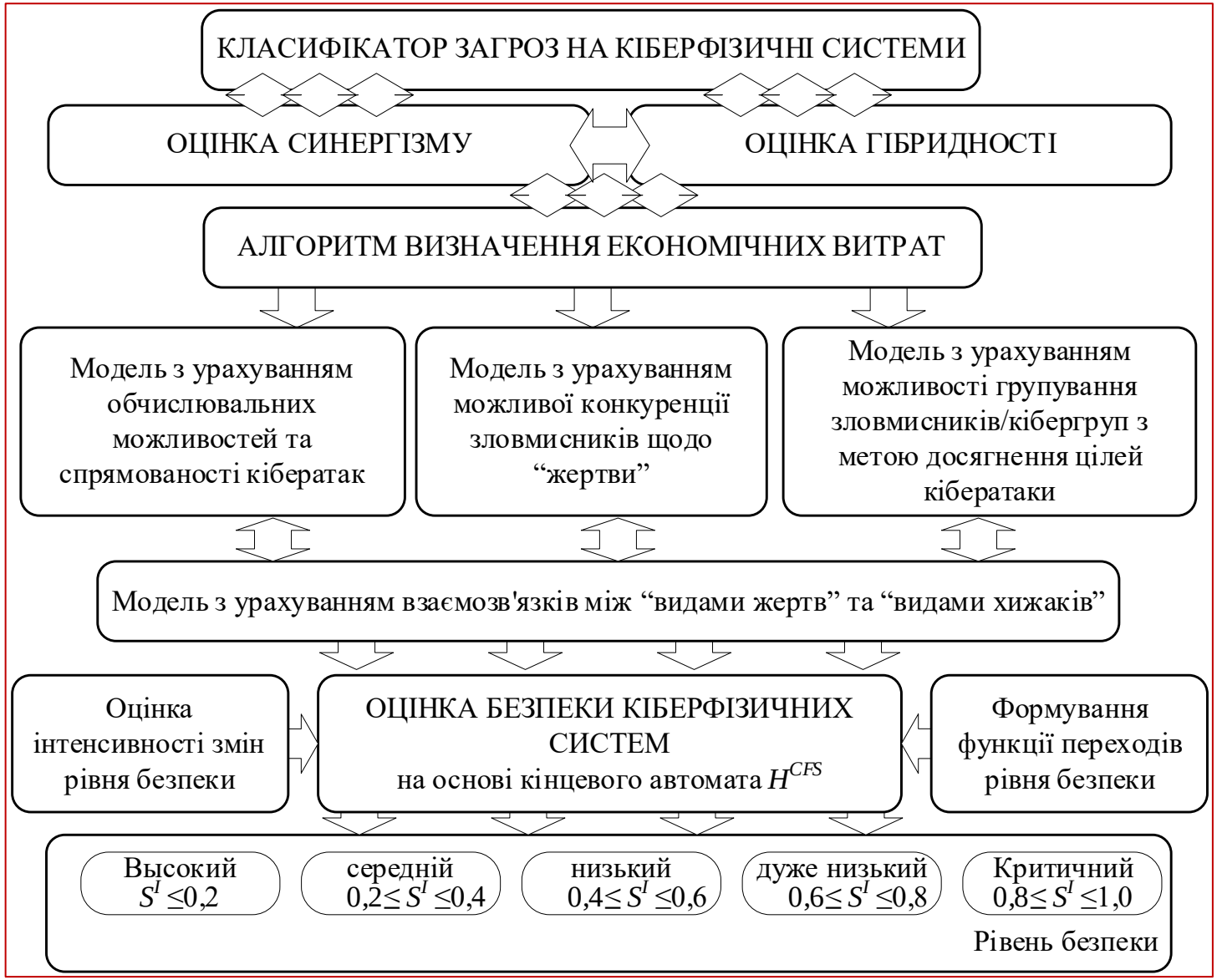
– for multiplicative convolution

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

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)


SYNERGIC MODEL OF CYBER THREATS ON SOCIO-CYBER-PHYSICAL SYSTEMS
Socioplatform
Social networks and instant messengers
trading platforms
crypto exchange platforms
Cyberspace platform
WAN technologies
Cloud technologies
LTE technologies
Cyber Systems Platform
IEEE802.16
Wireless system technologies
Mesh technologies
Sensor networks
external safety loop
internal safety loop
SYNERGIC CLASSIFIER OF CYBER THREATS
XX
XX
XX
XX
XX
XX
EMERGENCY MODEL FOR DETERMINING SYNERGY AND HYBRIDITY OF TARGETED ATTACKS ON SOCIO-CYBER-PHYSICAL SYSTEMS
Socioplatform
Social networks and instant messengers
trading platforms
crypto exchange platforms
Cyberspace platform
WAN technologies
Cloud technologies
LTE technologies
Cyber Systems Platform
IEEE802.16
Wireless system technologies
Mesh technologies
Sensor networks
external safety loop
General assessment of external threats, taking into account the technologies of the socio-cyberphysical system and threats based on social engineering methods
General assessment of external threats, taking into account the ownership of elements and technologies of the socio-cyberphysical threat system based on social engineering methods
internal safety loop
General assessment of internal loop threats, taking into account the technologies of the socio-cyberphysical system and threats based on social engineering methods
General assessment of internal loop threats, taking into account the ownership of elements and technologies of the socio-cyberphysical system and threats based on social engineering methods
GENERALIZED ASSESSMENT OF A MULTI-LOOP SAFETY SYSTEM
MODELS OF INFLUENCE IN SOCIO-CYBERPHYSICAL SYSTEMS

BLOCK DIAGRAM OF THE SCPS SAFETY ASSESSMENT METHOD BASED ON THE LOTKA-VOLTERRA "PREDATOR-PREY" MODEL"



Модель безпеки CPS, що розвивається, з урахуванням обчислювальних можливостей і спрямованості цільових кібератак

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \left(\sum\limits_{i=1}^{Q} \left(\begin{array}{l} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{array} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(\begin{array}{l} w_{CPSi}{}^C \bigcap w_{CPSi}{}^I \bigcap w_{CPSi}{}^A \bigcap \\ \bigcap w_{CPSi}{}^{Au} \bigcap w_{CPSi}{}^{Aff} \end{array} \right) \chi_i^{CPS} \right) \times \tilde{N}_1 \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af \text{ synerg}} \right| \right); \\ \dfrac{dN_2}{dt} = - \left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \tilde{N}_2 + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \tilde{N}_2 \tilde{N}_1. \end{cases}$$

Модель безпеки CPS на основі моделі "хижак-жертва" з урахуванням можливої конкуренції зловмисників щодо "жертви"

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \left(\sum\limits_{i=1}^{Q} \left(\begin{array}{l} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{array} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(\begin{array}{l} w_{CPSi}{}^C \bigcap w_{CPSi}{}^I \bigcap w_{CPSi}{}^A \bigcap \\ \bigcap w_{CPSi}{}^{Au} \bigcap w_{CPSi}{}^{Aff} \end{array} \right) \chi_i^{CPS} \right) \times \tilde{N}_1 \left(\tilde{N}_2^1 \bigcap \tilde{N}_2^2 \bigcap \ldots \bigcap \tilde{N}_2^w \right); \\ \dfrac{dN_2}{dt} = - \left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \times \left(\tilde{N}_2^1 \bigcap \tilde{N}_2^2 \bigcap \ldots \bigcap \tilde{N}_2^w \right) + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \times \\ \times \left(\tilde{N}_2^1 \bigcap \tilde{N}_2^2 \bigcap \ldots \bigcap \tilde{N}_2^w \right) \tilde{N}_1, \end{cases}$$

Модель безпеки CPS на основі моделі “хижак-жертва” з урахуванням можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \bigcap w_{CPSi}{}^I \bigcap w_{CPSi}{}^A \bigcap \\ \bigcap w_{CPSi}{}^{Au} \bigcap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \tilde{N}_1 \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right); \\ \dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1, \end{cases}$$

Модель безпеки CPS на основі моделі “хижак-жертва” з урахуванням взаємозв'язків між “типами жертв” і “типами хижаків”

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \bigcap w_{CPSi}{}^I \bigcap w_{CPSi}{}^A \bigcap \\ \bigcap w_{CPSi}{}^{Au} \bigcap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \times \tilde{N}_1 \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) - \varepsilon \tilde{N}_2^2; \\ \dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1 - \xi \tilde{N}_2^2, \end{cases}$$

Comparative analysis of factorization complexity for classical and quantum algorithms

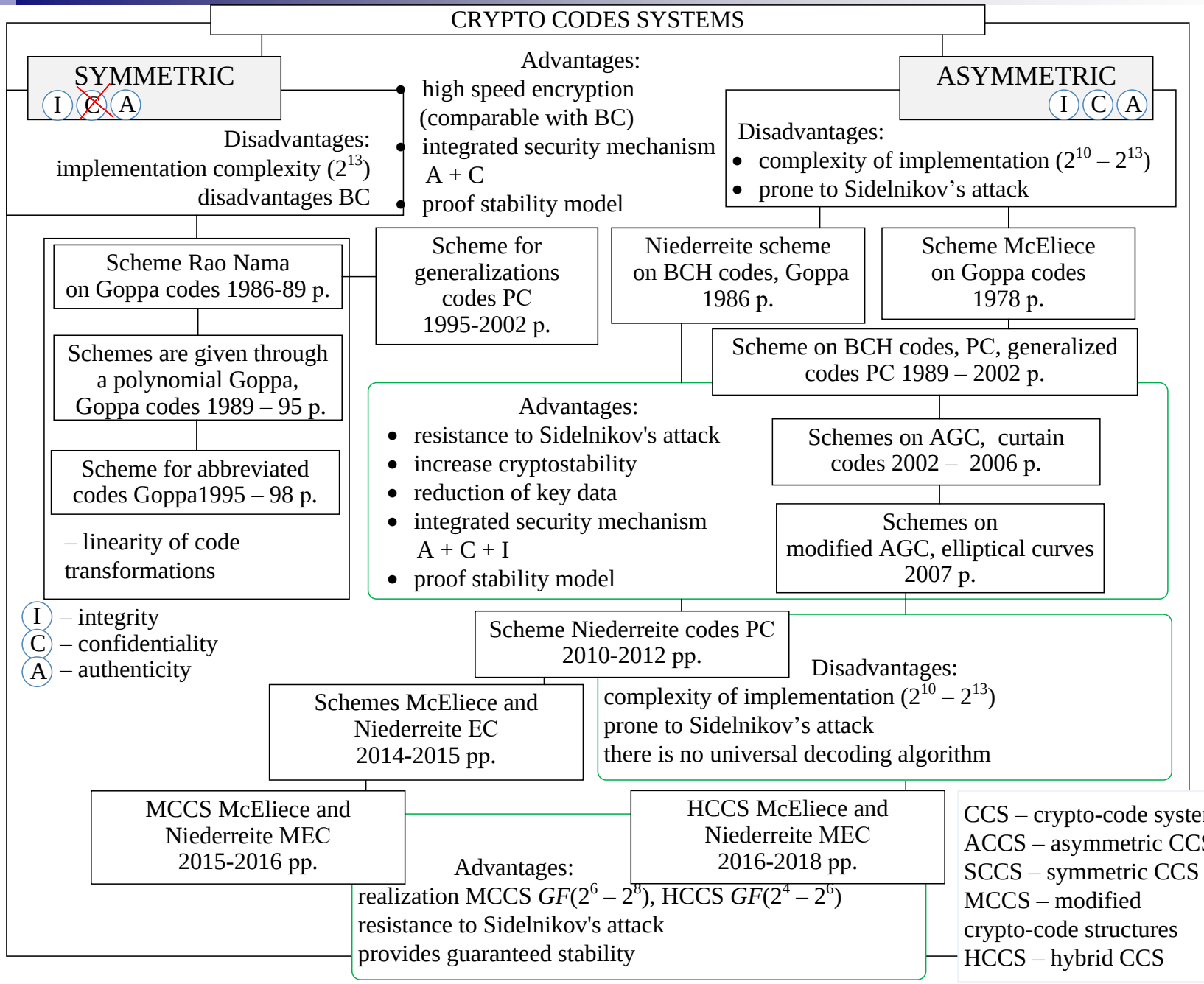
Module size N, bit	The number of required qubits $2n$	The complexity of the quantum algorithm $4n^3$	The complexity of the classical algorithm
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

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}

CLASSIFICATION OF CRYPTIC CODE STRUCTURES

MicroCAD-2024



Statement.

Any linear code K with parameters [n,k,d]r , d≤n/2 has a decoding algorithm within its code distance whose complexity is at most

$$O\left(\min\left(nr^k, n\sum_{j=0}^{t}\left(\binom{n}{j}\right)\right)\right), \text{ где } t=\left[\frac{d-1}{2}\right]$$

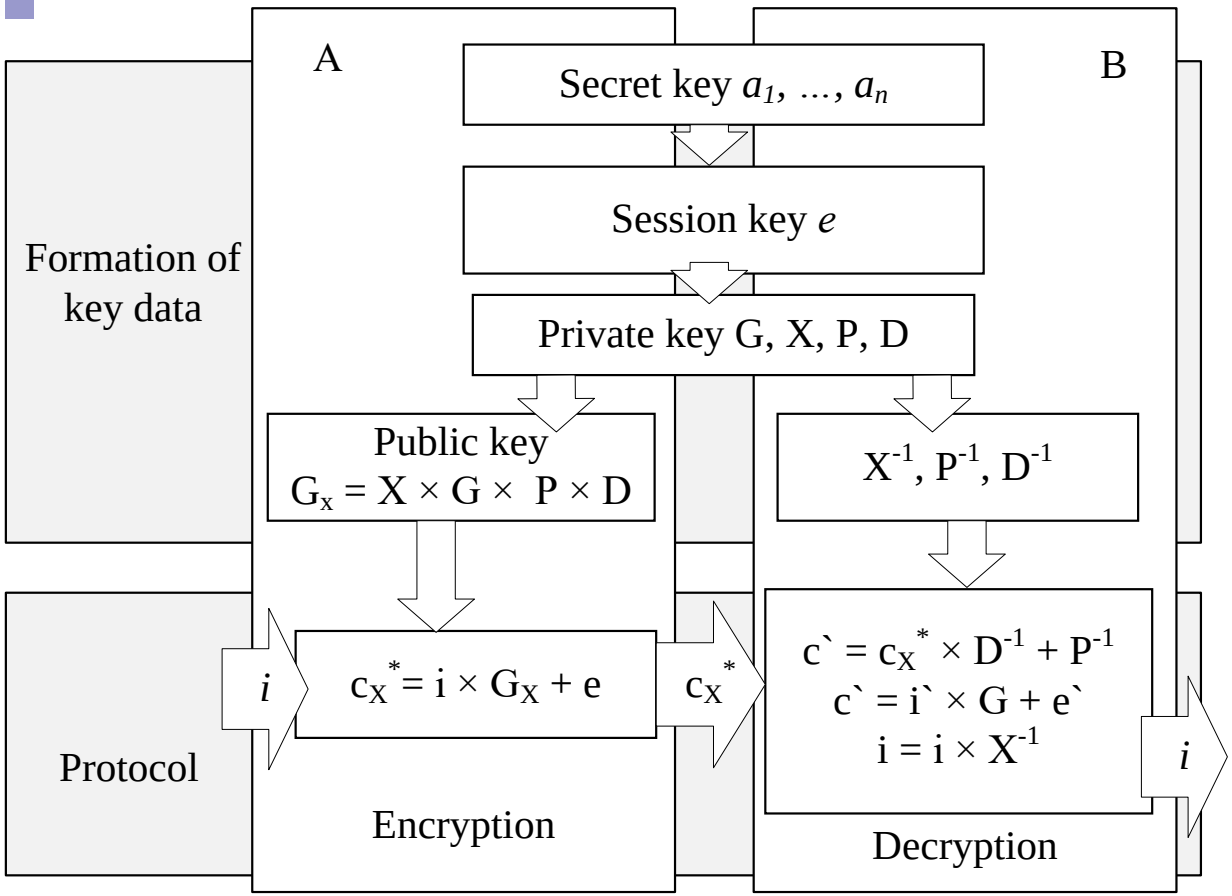
r^k - number of elements in the code;

$O\left(nr^k\right)$ - the number of operations required to iterate over all elements of the code;

$\sum_{j=0}^{t}\binom{n}{j}(r-1)^j$ - number elements in a ball of radius t;

$\left(n\sum_{j=0}^{t}\binom{n}{j}\right)$ - the number of operations required

to enumerate all elements of the ball in order to find the code vector



secret (closed) key – matrices *X, P, and D*.

X – non-degenerate k×k matrix over GF(q),
P – permutational n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
G^{EC}– generating k×n matrix of elliptical code over GF(q),

public key – matrix

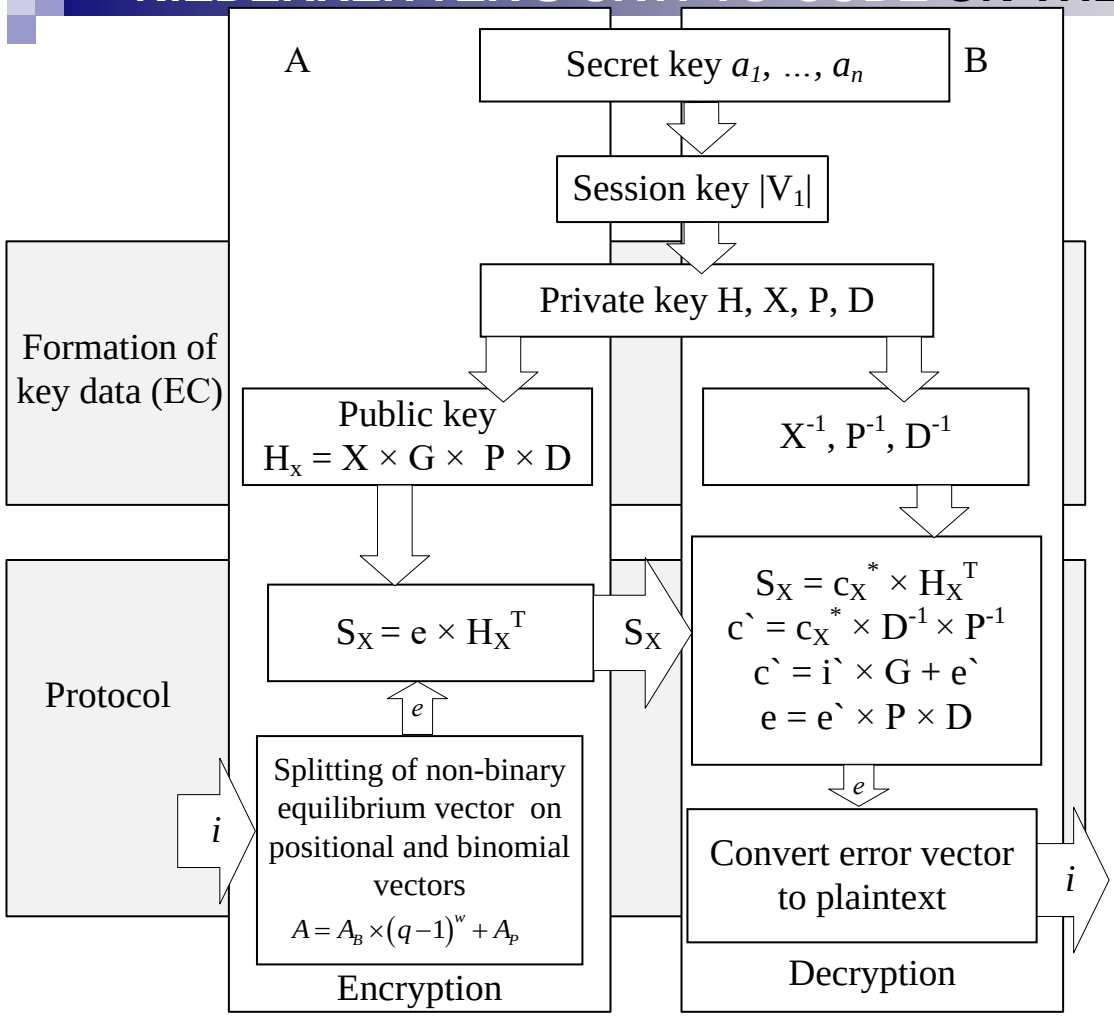
$$G_X^{EC} = X \times G^{EC} \times P \times D$$

Closed information (a codogram)

$$c_X^* = i \cdot G_X^{EC} + e,$$

vector *e* is the secret weight error vector $\leq t$

An elliptic curve (EC) in the affine space $\boldsymbol{A^2}$ over field *GF(q)* is a smooth curve given by equation $\boldsymbol{y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6}$, *or in* $\boldsymbol{P^2}$ *given by homogeneous equation* $\boldsymbol{y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3}$, $a_i \in GF(q)$, the genus of the curve $g=1$.



secret (closed) key – matrices *X, P, and D.*
X – non-degenerate k×k matrix over GF(q),
P – permutational n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
$\boldsymbol{H^{EC}}$– check $n \times (n-k)$ matrix of an algebra-geometric block (n, k, d) code

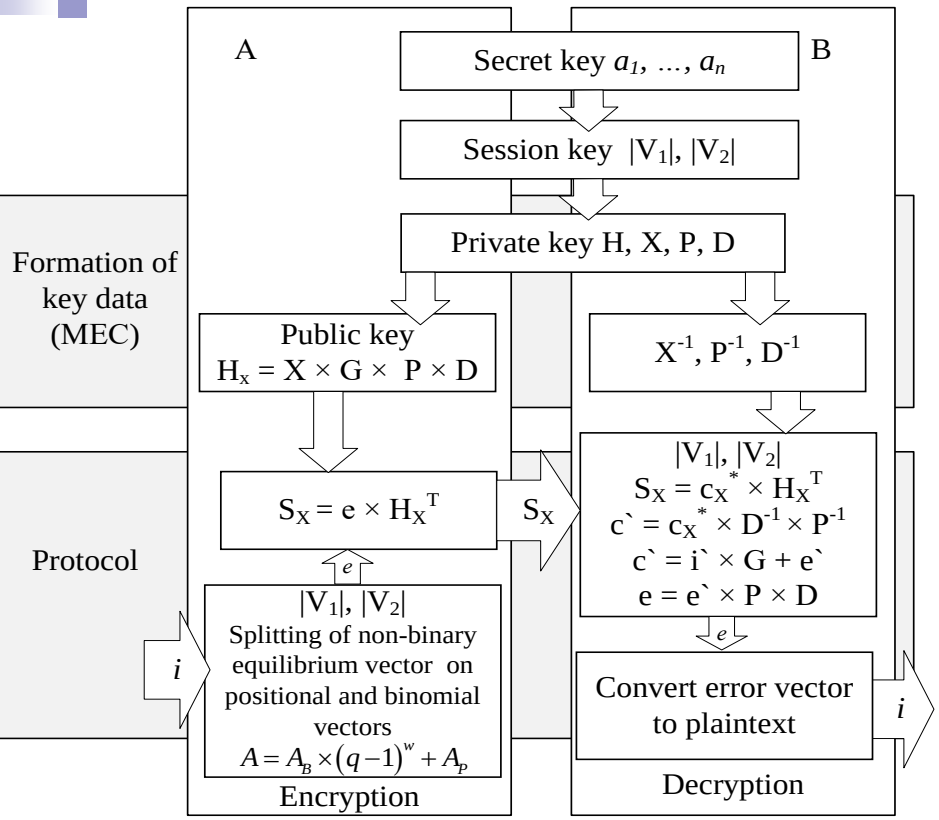
public key – matrix

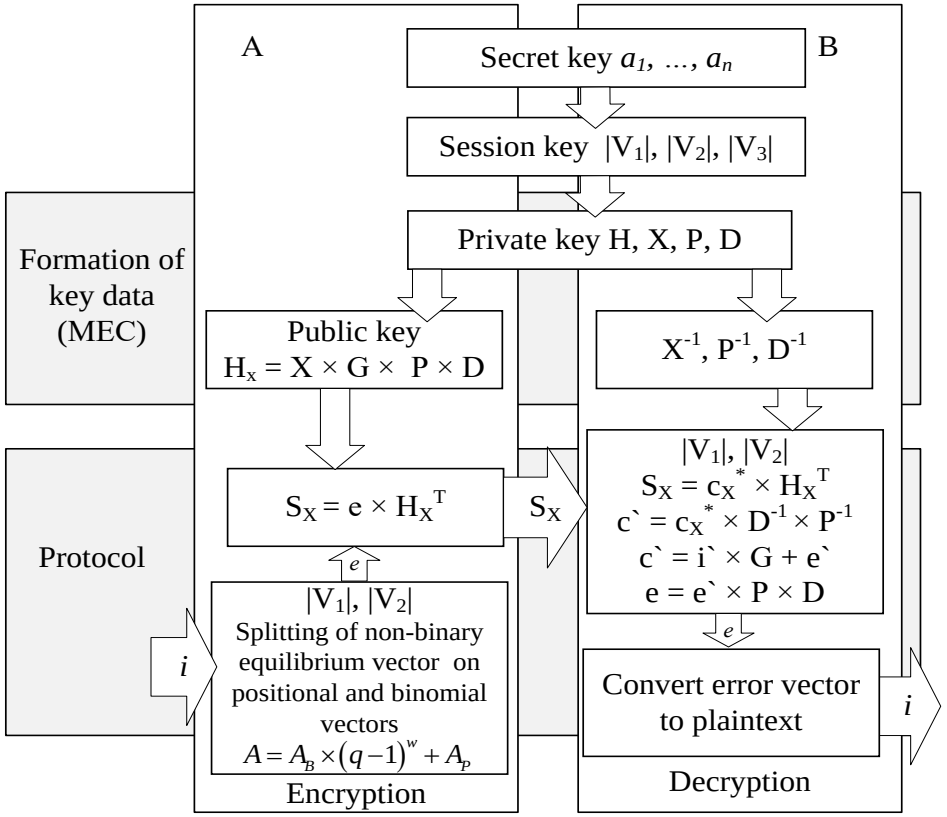
$$H_X^{EC} = X \times H^{EC} \times P \times D,$$

Closed information (a codogram)

$$S_X = e \cdot \left(H_X^{EC}\right)^T$$

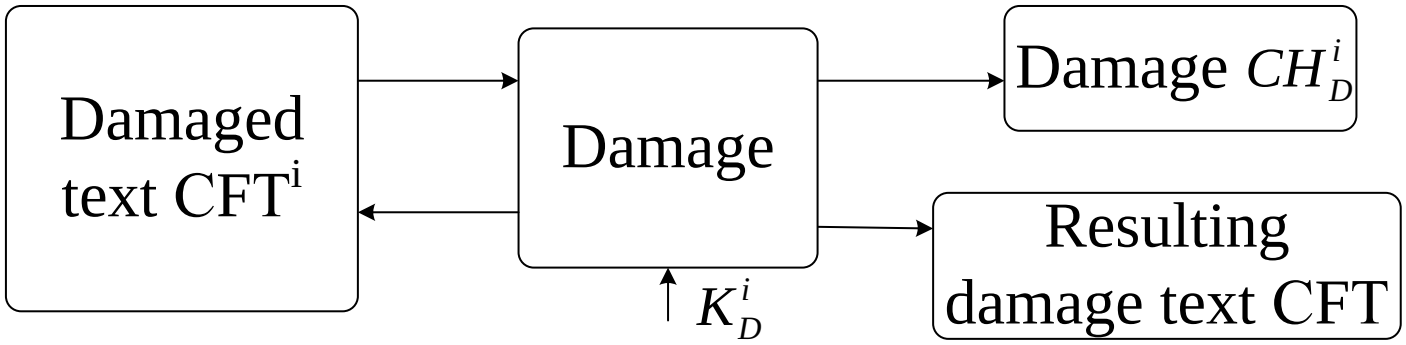
vector $\mathbf{IV_1}$ (sets of fixed positional sets of clear text $\{M_F\}$).





Dependence of software implementation on field power

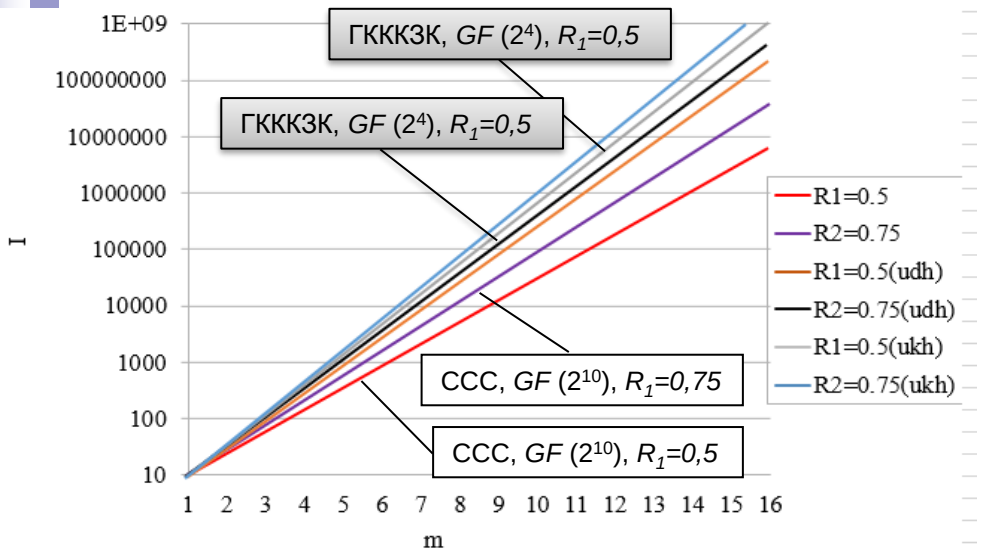
Cryptosystems	2^5	2^6	2^7	2^8	2^9	2^{10}
Mc-Elice on the EC	10018042	18048068	32847145	47489784	63215578	**82467897**
Mc-Elice on the shortened MEC	10007947	**17787431**	28595014	44079433	61974253	79554764
Mc-Elice on the extended MEC	11156138	**18561228**	33210708	48297112	65171690	84051337



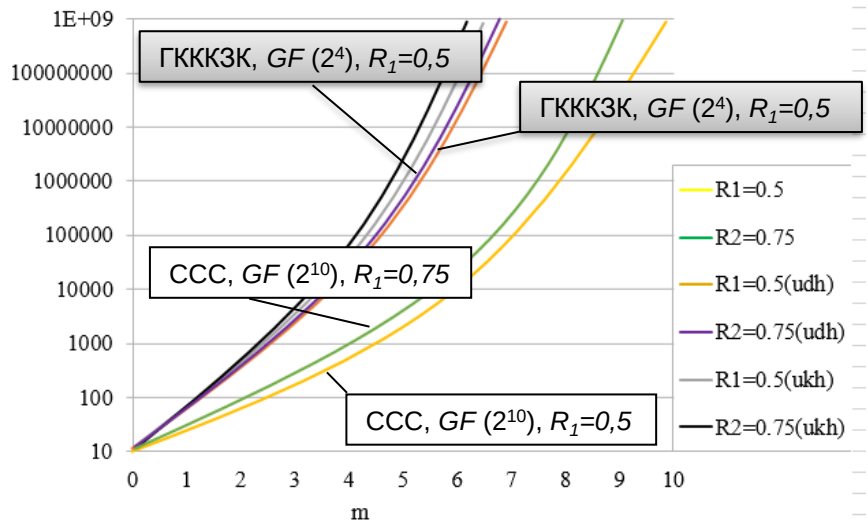
Block diagram of one step of the mechanism of damage

$$B(M) = B_A L_0 = \left(\log N - \frac{H(M)}{L_0} \right) \times L_0,$$

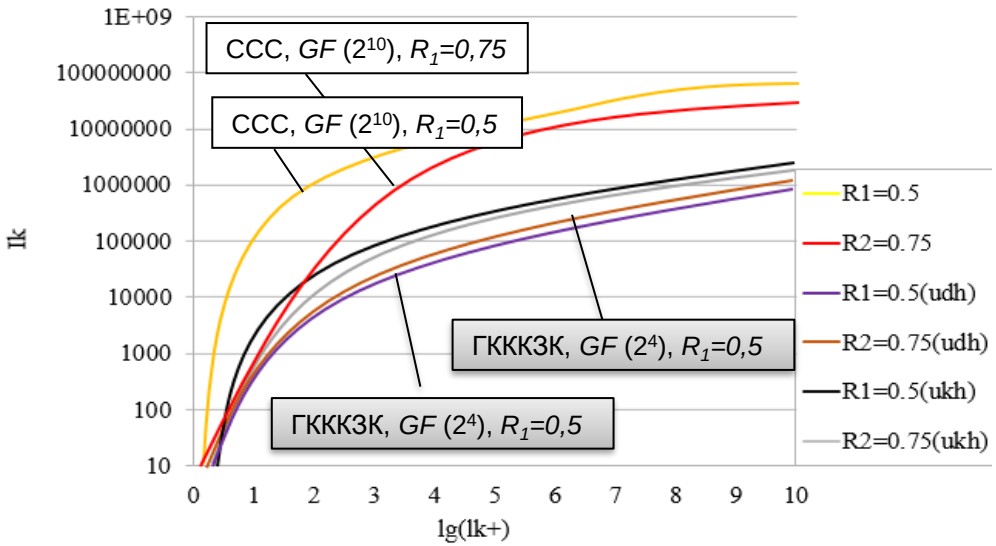
где M – source text; B – language redundancy ($B = R–r$, R – absolute entropy of a language ($R=logN$, N – alphabet power, r – language entropy per character, $r=H(M)/L$, L – message length M in symbols of the language; $H(M)$ –entropy (uncertainty) of the message; L_0 – message length M in the symbols of the language with meaning; B_A – language redundancy.



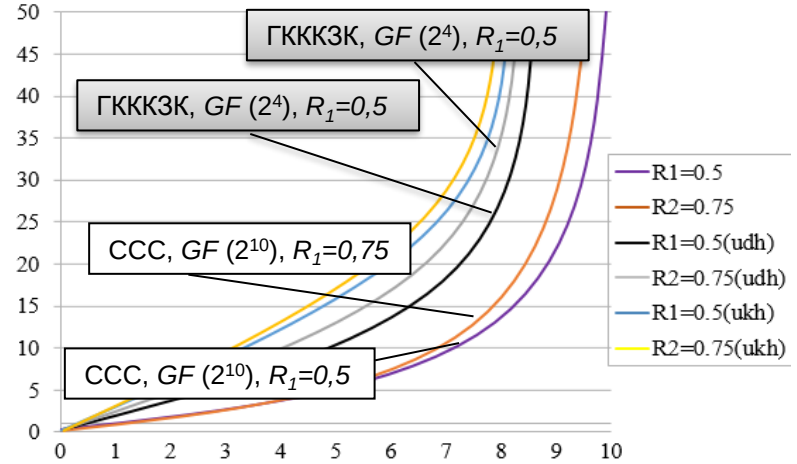
Залежність складності формування криптограми в різних GF (2^m)



Залежність складності розкодування криптограми в різних GF (2^m)



Залежність обсягу відкритих ключових даних



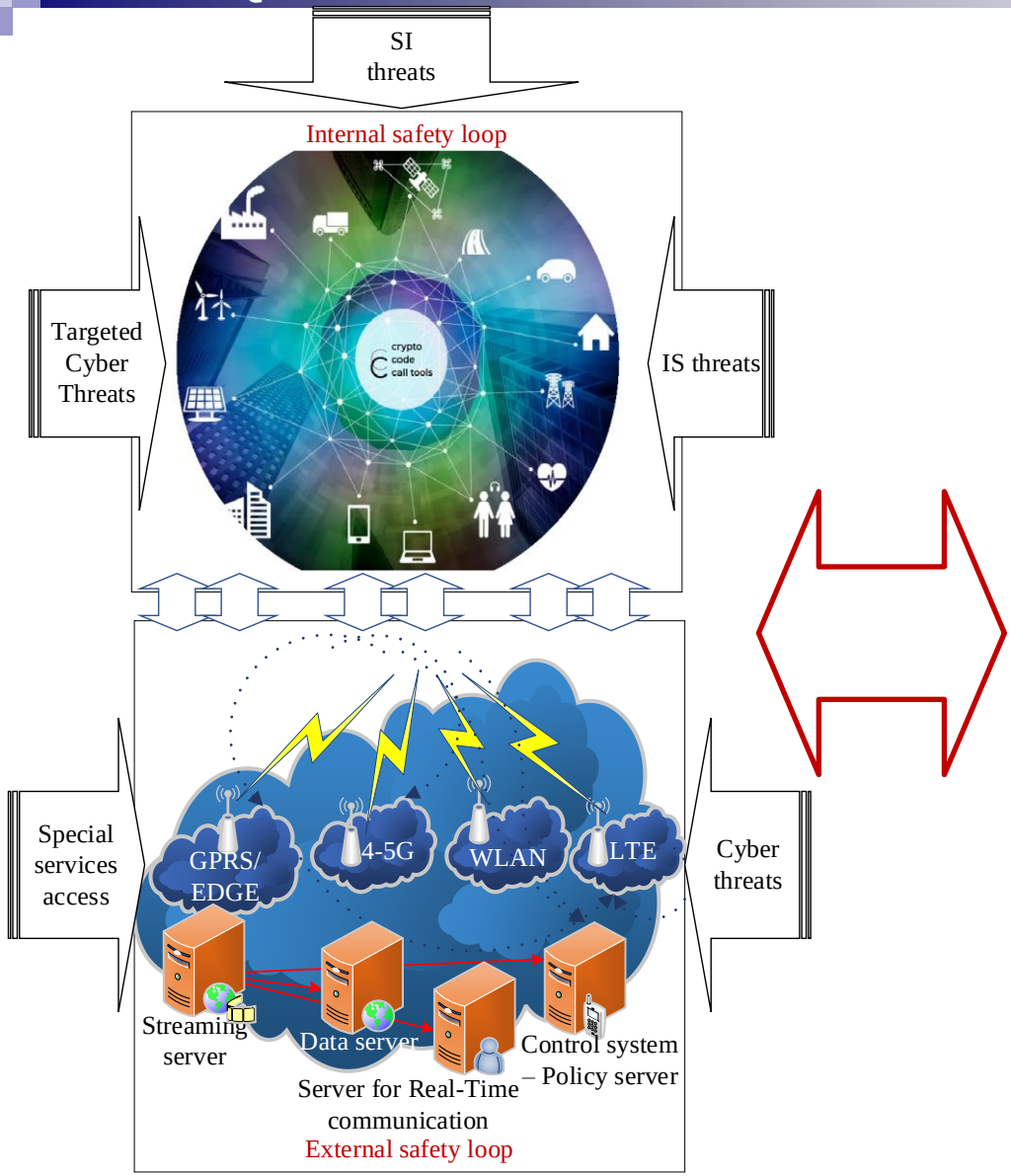
Залежність складності злому

Залежність швидкості програмної реалізації від потужності поля

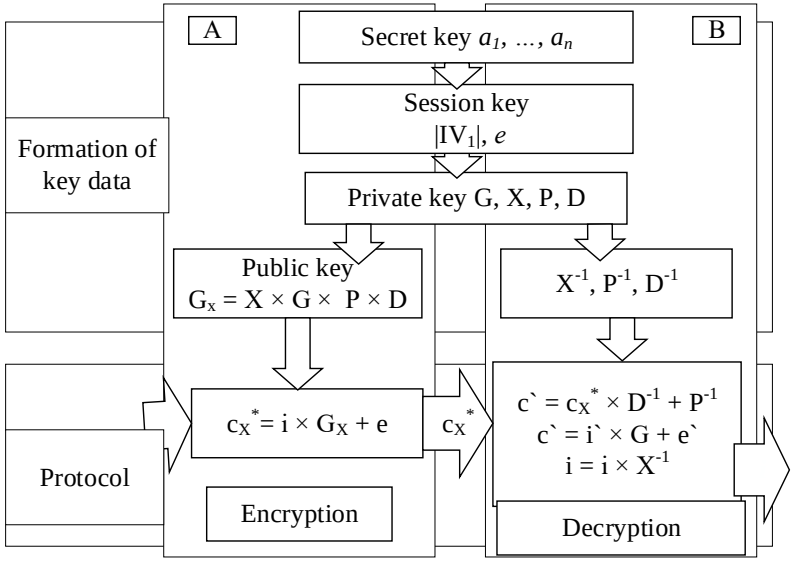
Криптосистеми	$GF(q^m)$						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
ССС Mc-Eliece на укорочених МЕС	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
ССС Mc-Eliece на подовжених МЕС	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
НССС Mc-Eliece подовжених МЕС	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
НССС Mc-Eliece укорочених МЕС	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Результати дослідження статистичної безпеки (NIST STS 822)

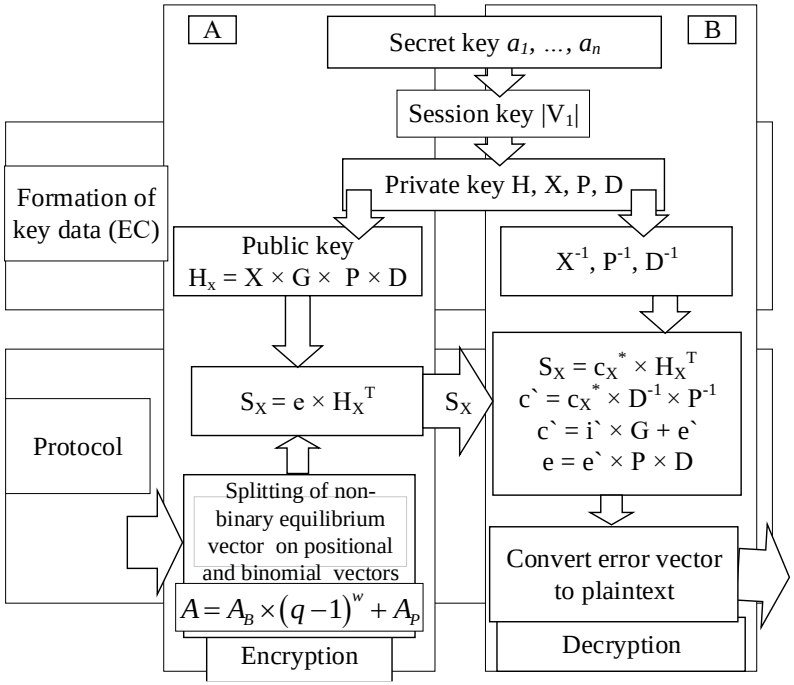
Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
ССС Mc-Eliece	149 (78,83%)	189 (100%)	0 (0%)
ССС Mc-Eliece на укорочених МЕС	151 (79,89%)	189 (100%)	0 (0%)
ССС Mc-Eliece на подовжених МЕС	152 (80,42%)	189 (100%)	0 (0%)
НССС Mc-Eliece на подовжених МЕС	153 (80,95%)	189 (100%)	0 (0%)
НССС Mc-Eliece на укорочених МЕС	155 (82 %)	189 (100%)	0 (0%)



https://www.calltools.ua



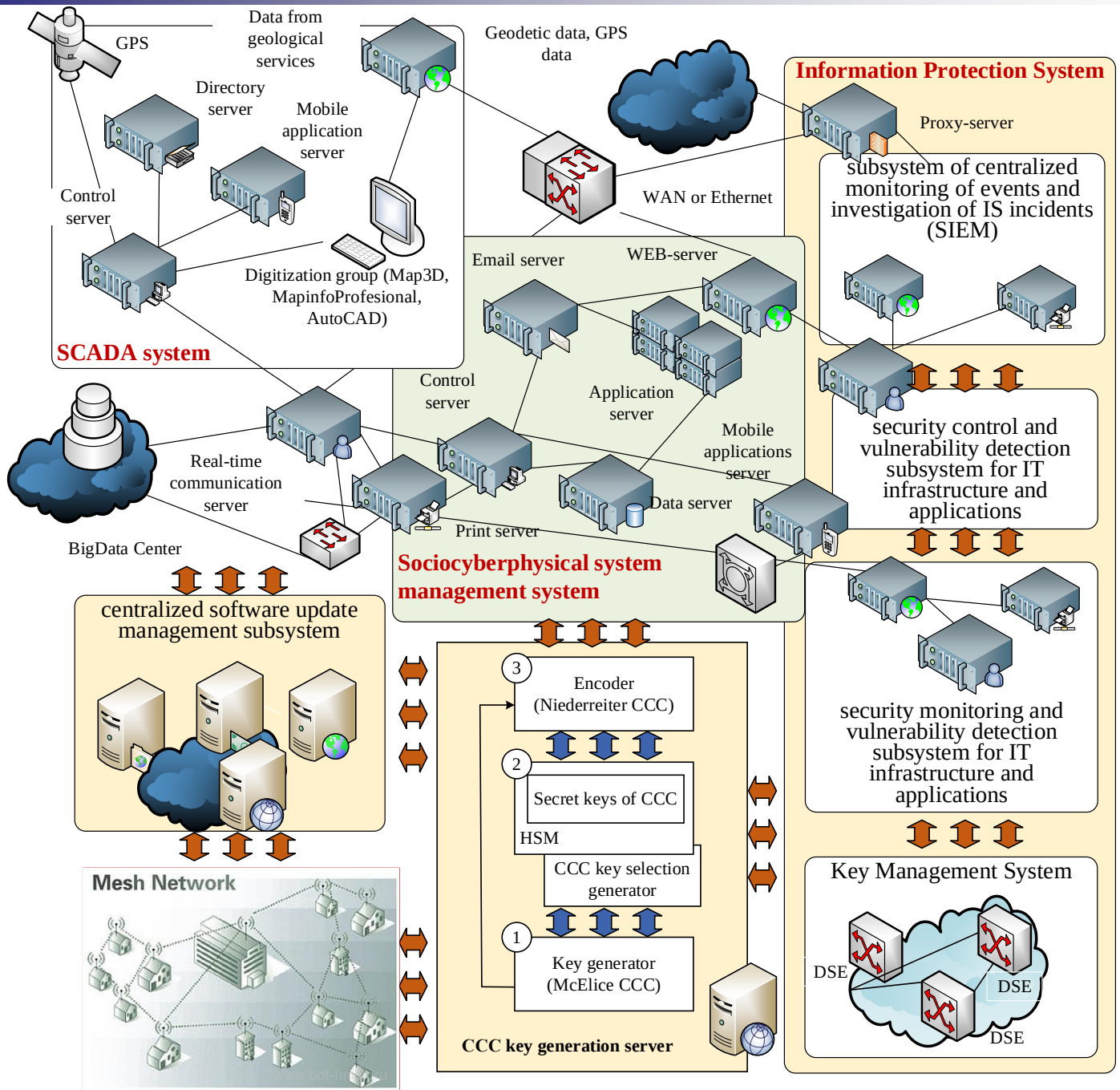
McEliece crypto-code construction on the EC



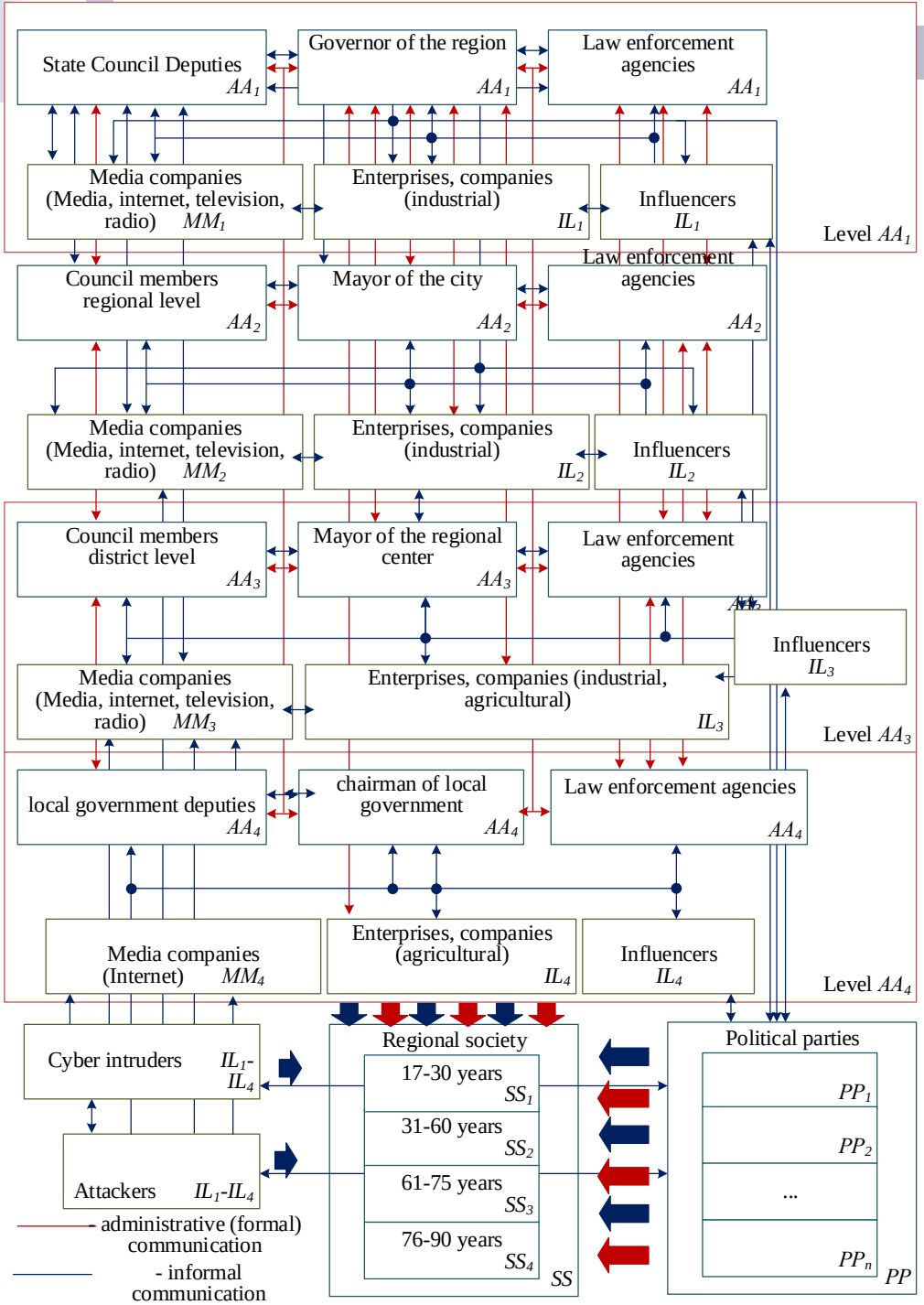
Niederreiter crypto-code construction on EC

Comparative characteristics of wireless and mobile Internet technologies

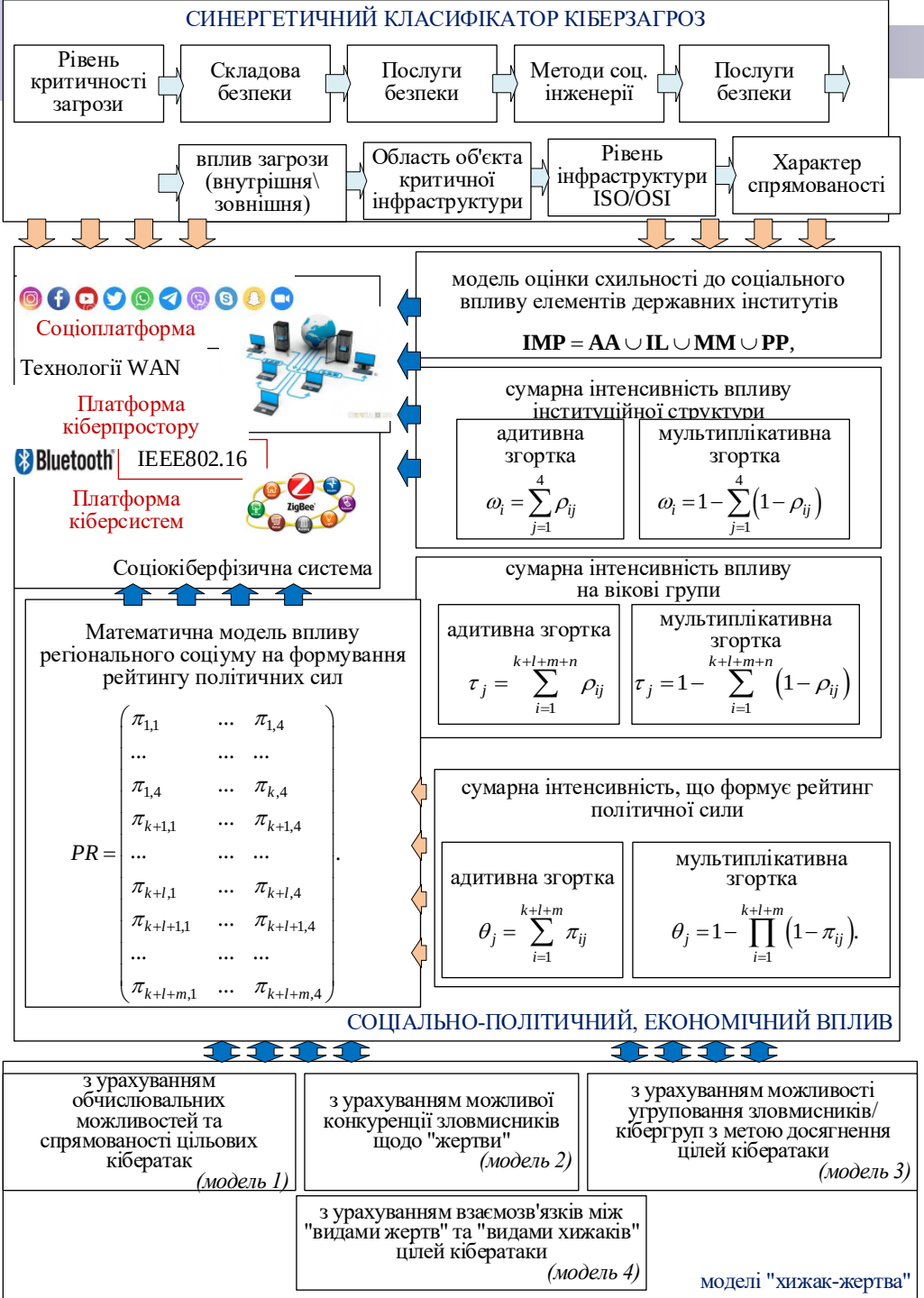
Technology	Provision of security services					The degree of information secrecy (β_i)				
	C	I	A	A_u	B	1,0	0,75	0,5	0,25	0,01
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (Wi-Fi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
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	+	+	+	+	+	–	–	+	+	+


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
Real-time communication server
BigData Center
Sociocyberphysical system management system
security control and vulnerability detection subsystem for IT infrastructure and applications
centralized software update management subsystem
security monitoring and vulnerability detection subsystem for IT infrastructure and applications
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

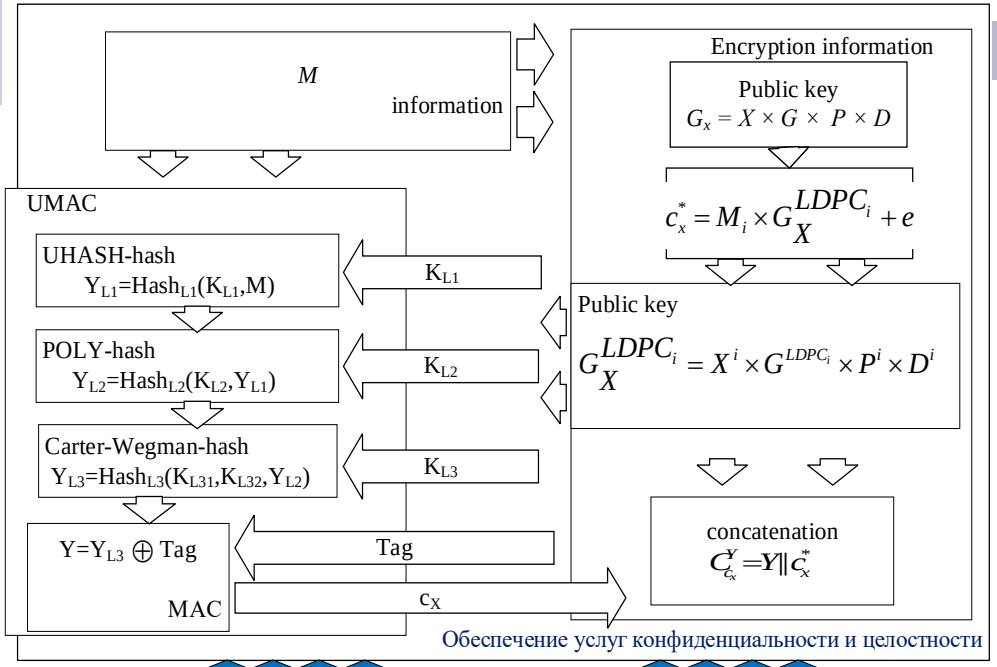
FORECASTING MODEL FOR ASSESSING SOCIAL IMPACT IN REGIONAL COMMUNITIES

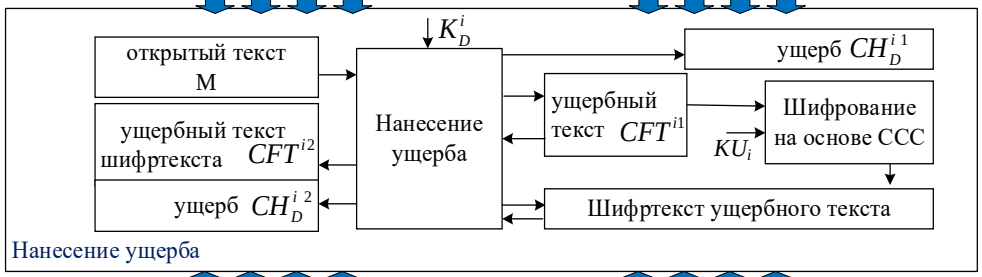


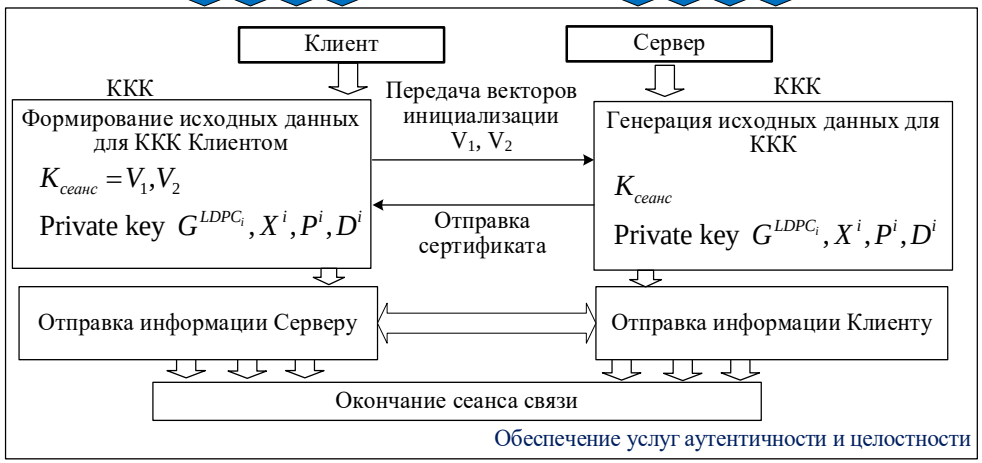
PP ={PP1, PP2, …, PPn} – множина політичних сил (партій, блоків;
IL={IL1, IL2, …, ILl} – множина неформальних лідерів регіональної громади;
MM={M1, M2, …, Mm} – множина елементів медіа (media), до яких належать: засоби масової інформації;
SS={SS1, SS2, SS3, SS4} – регіональна громада (соціум), представлена безліччю своїх вікових груп.



створення багато контурної системи безпеки інформації у соціальних інтернет сервісах та соціокіберфізичних систем в цілому, в основу якої покладено запропоновані концепцію побудови багатоконтурної безпеки, удосконалений універсальний класифікатор загроз,







методи забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів на крипто-кодових конструкціях Мак-Еліса на LDPC-кодах, метод прогнозування оцінки соціального впливу в регіональних спільнотах, метод оцінювання інформаційних ресурсів з урахуванням комплексного показника ефективності інвестицій в системи захисту інформаційних ресурсів у соціальних інтернет сервісах

Дякуємо за увагу !