BANKING SECURITY SYNERGETIC MODELS

4th International Congress of 3D Printing (Additive Manufacturing) Technologies and Digital Industry

Serhii Yevseiev
Doctor of Technical Science, Senior Research
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics

Serhii.Yevseiev@hneu.net

RELEVANCE OF THE TOPIC

Reason - the process of transformation of threats to the state information security has intensified. **Consequence** - threats have acquired signs of HYBRIDITY

Example - USA 2011

THREATS TO STATE INFORMATION SECURITY

INFORMATION THREATS

Action of civil disobedience "Take the Wall Street"

Coordination of actions with the help of social networks

+

CYBER THREATS

Massive cyberattacks on the OBS by hacking groups Anonymous, MoveOn.Org, Rebuild the Dream i Working Families Party

ABS blocking led to a social explosion in society, mass disorder and, as a chain reaction, spread to the largest cities in the United States and to a number of the most economically developed countries of the European Union

Serhii.Yevseiev@hneu.net

RELEVANCE OF THE TOPIC

EXAMPLE
June - July 2017

Cyberattacks with Malware Petya.A, Petya.B, Petya.C

ОЩАДБАНК
МІЙ БАНК. МОЯ КРАЇНА

ТАСКОМБАНК

УКРГАЗБАНК
НАЛЕЖИТЬ ДЕРЖАВІ

БАНК ПІВДЕННИЙ

otpbank

the process of providing banking services has been compromised, which caused dissatisfaction of clients with banks that are subjects of the state budget

A radical overview of the current methodological principles for building a security system for banking information resources is required

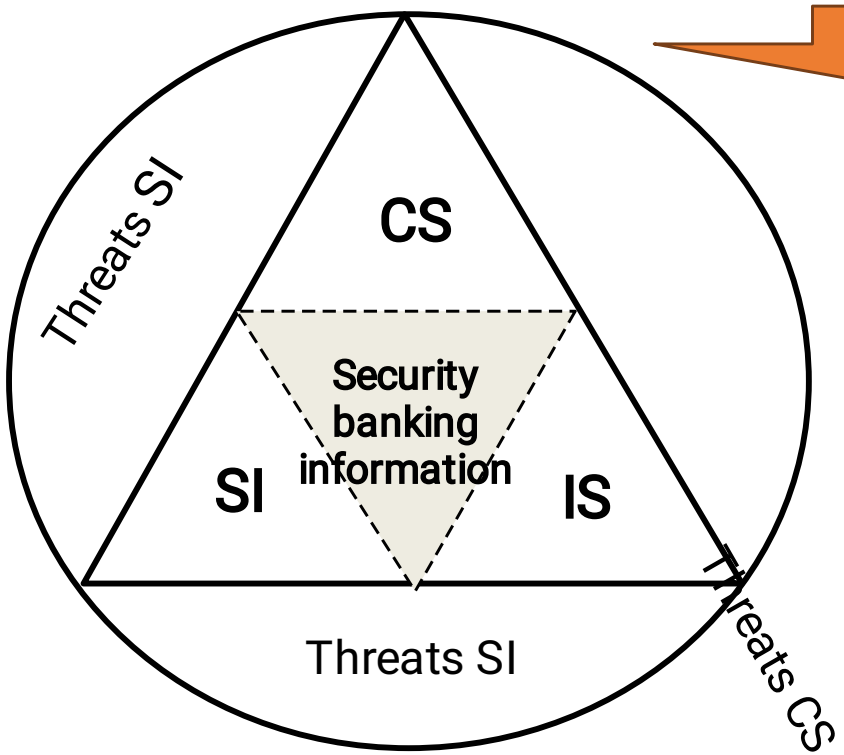
Serhii.Yevseiev@hneu.net

1. ANALYSIS OF THE CURRENT STATE OF THE PROBLEM: THE CONCEPTUAL ASPECT

The **first approach** to developing and modeling a security system is based on meeting the requirements of one of the security regulators (standards):

- family of standards ISO 13335;
- family of standards ISO/IEC 15408;
- family of standards ISO 27XXX

The **second approach** to developing and modeling a security system is based on the principle of “reasonable sufficiency”

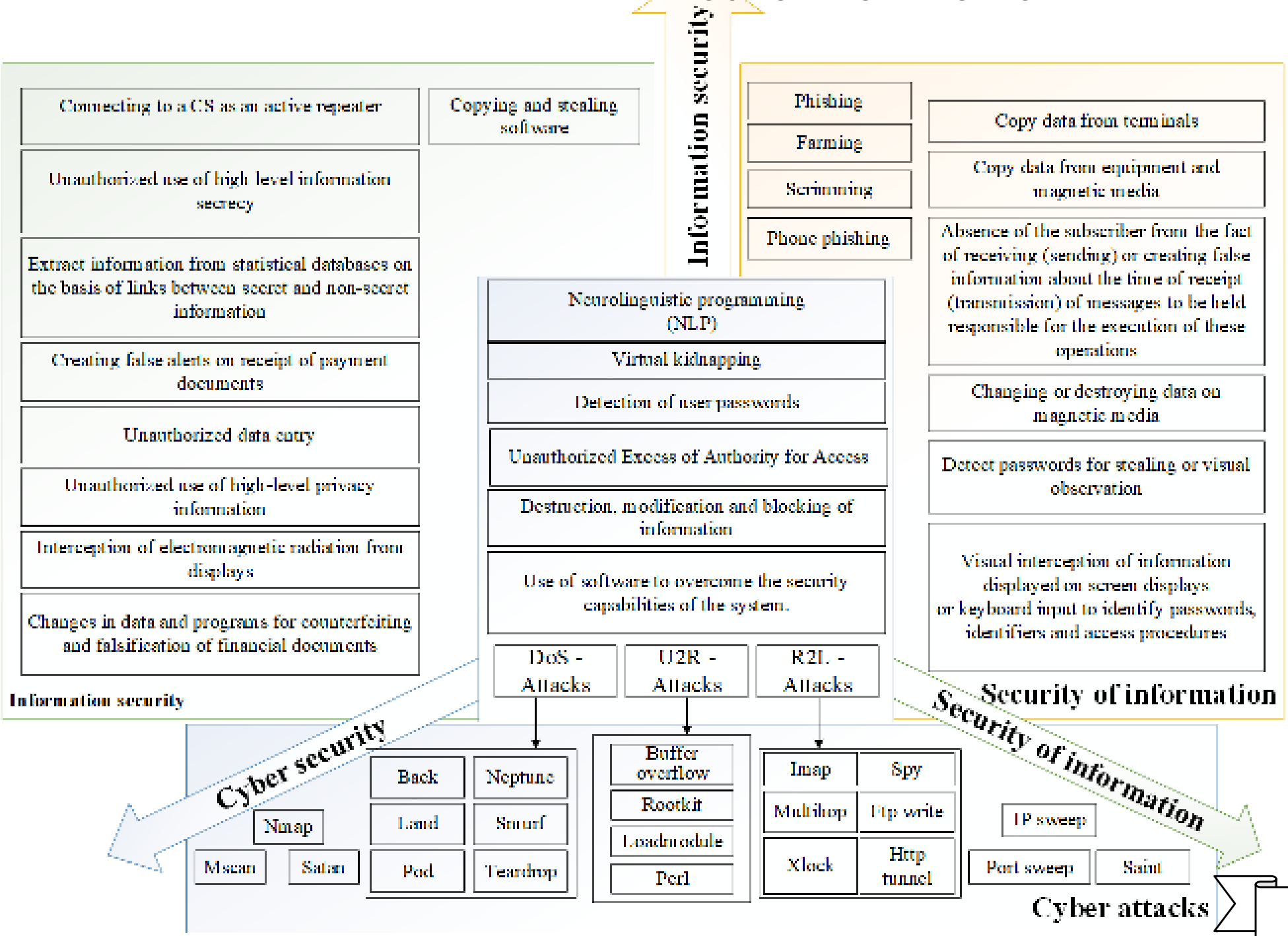


Disadvantages:

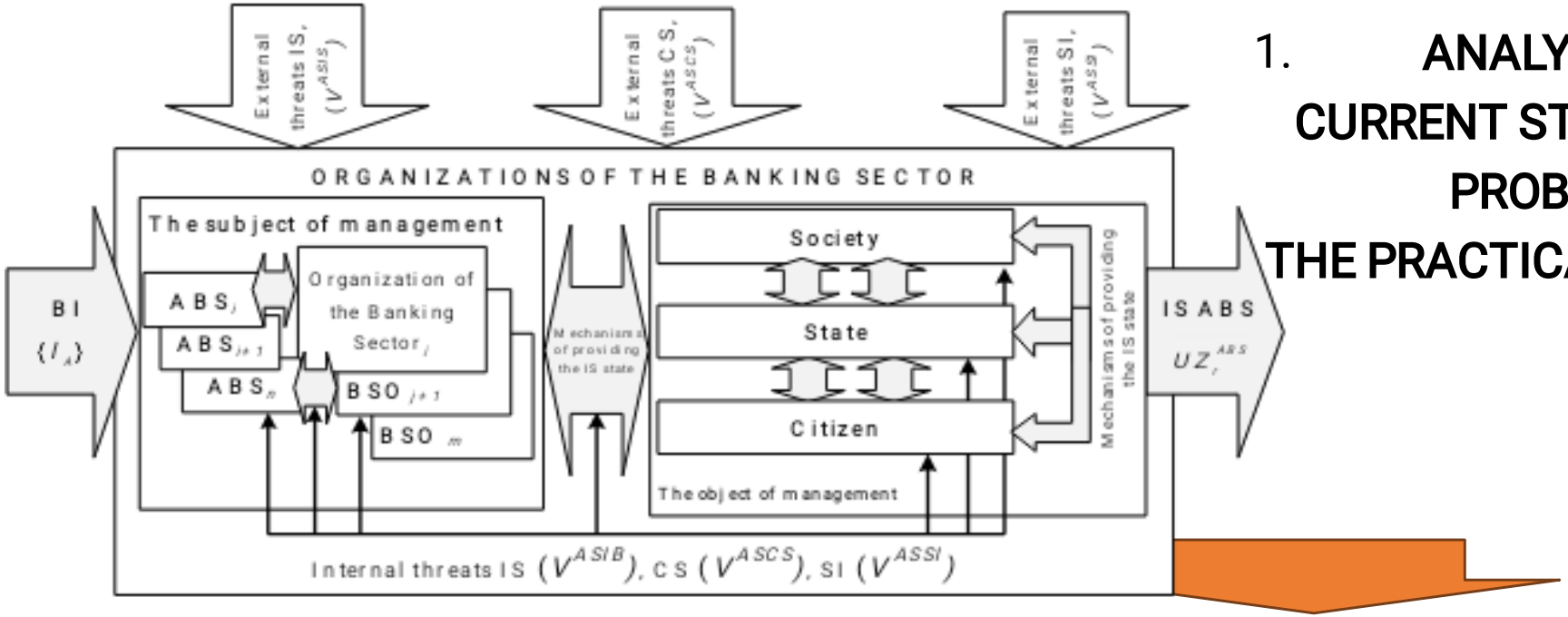
- the dynamics of growth and the improvement of threats aren’t taken into account
- the properties of hybridity and synergies of threats aren’t taken into account
- the integration of threats to security services isn’t taken into account

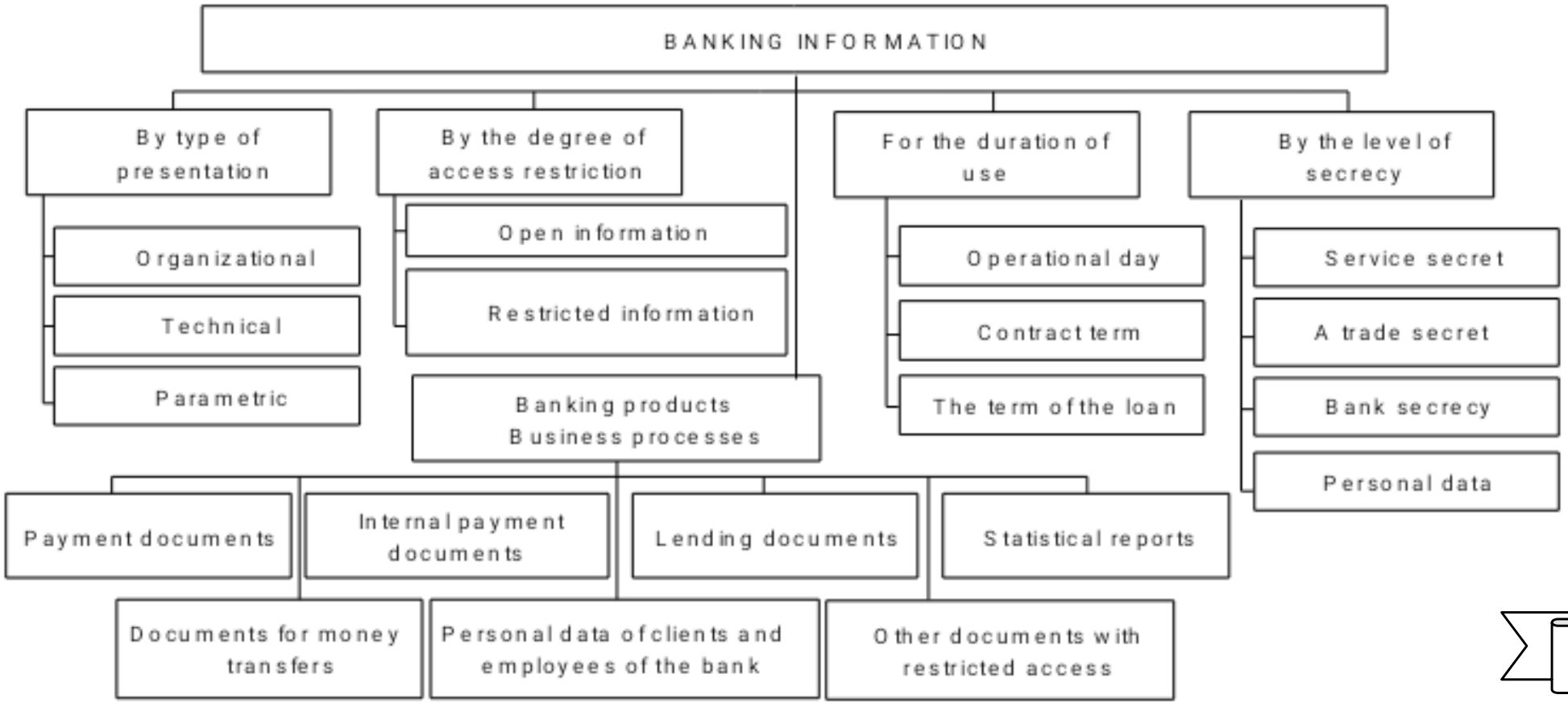
Serhii.Yevseiev@hneu.net

1. ANALYSIS OF THE CURRENT STATE OF THE PROBLEM: THE CONCEPTUAL ASPECT

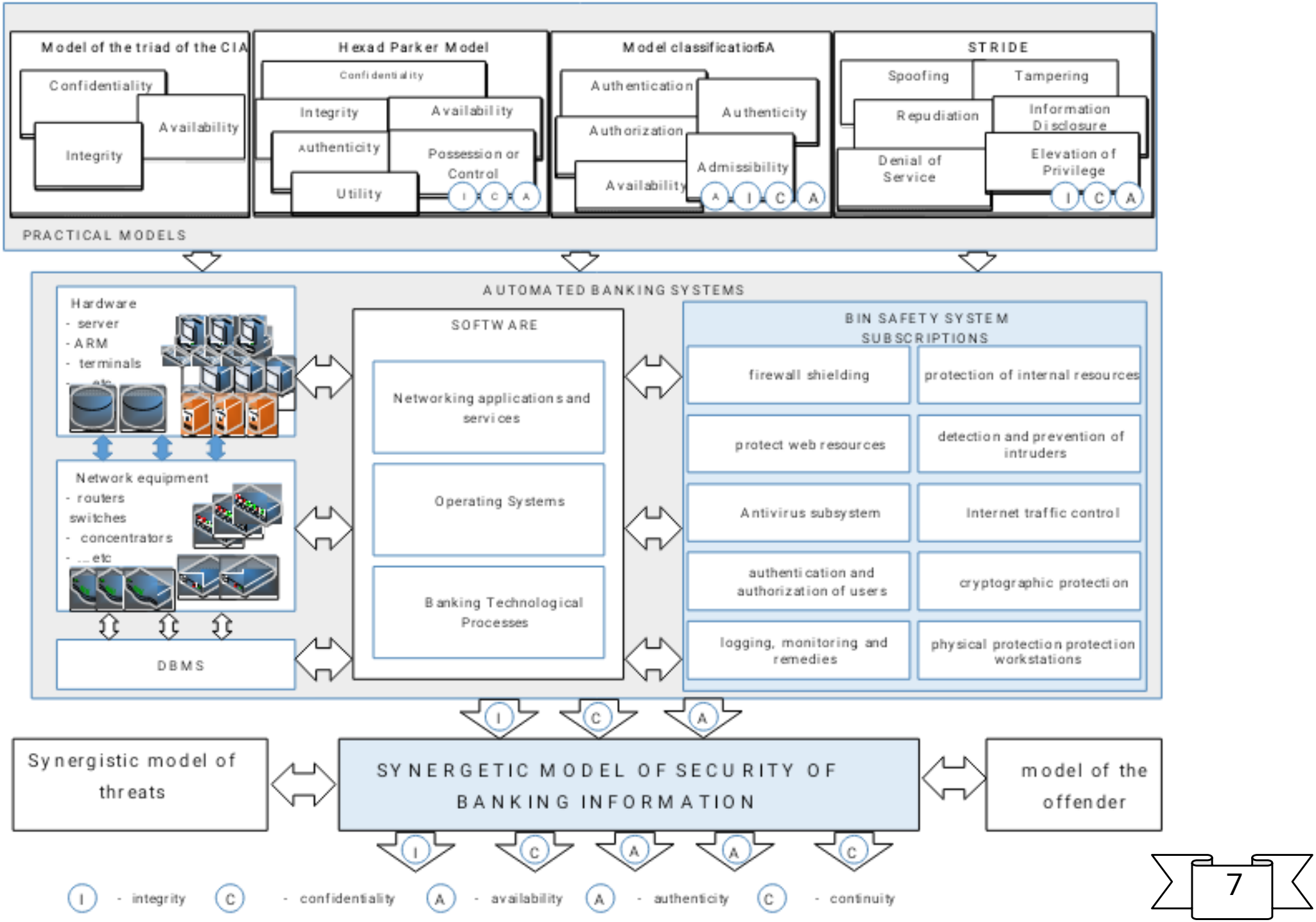


1. ANALYSIS OF THE CURRENT STATE OF THE PROBLEM: THE PRACTICAL ASPEC

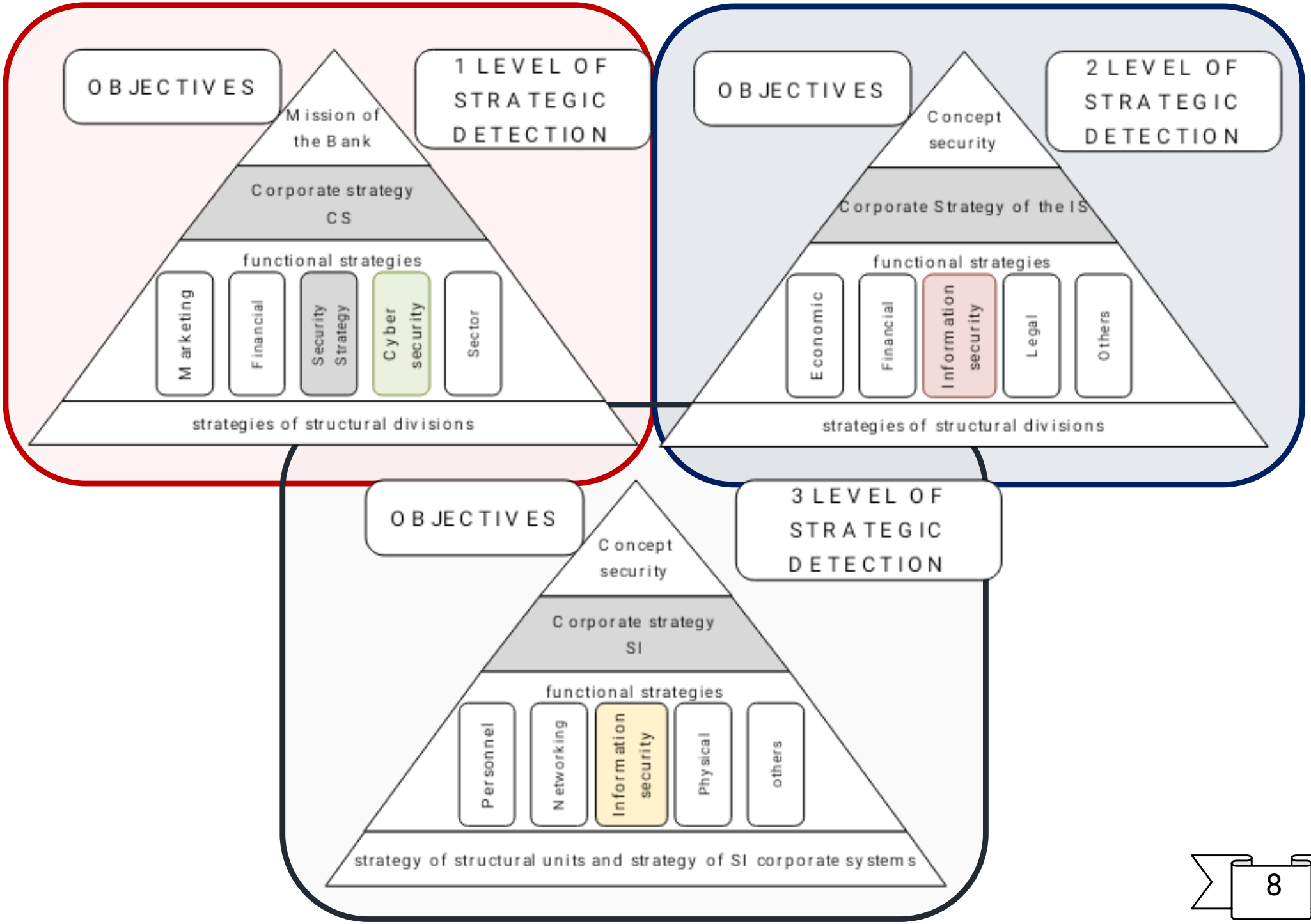




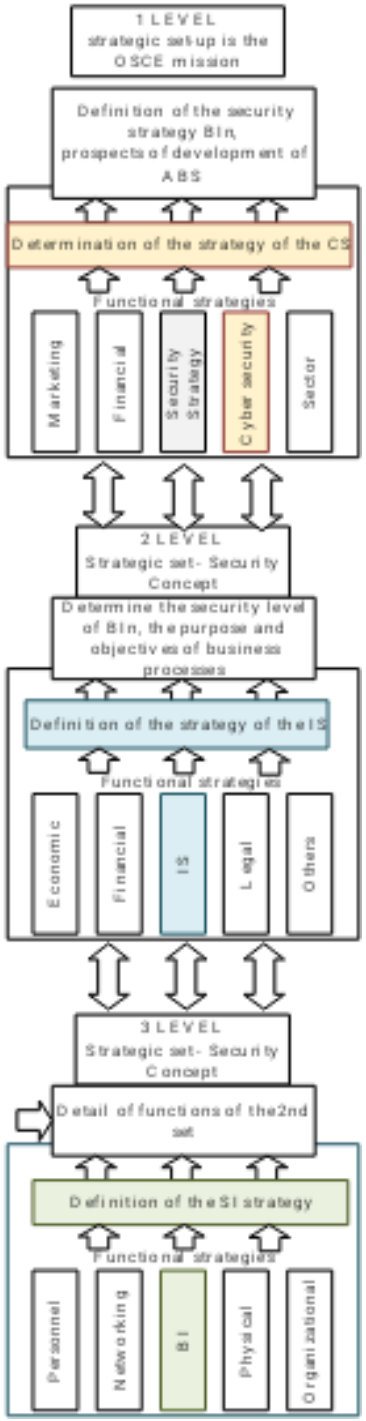
1. ANALYSIS OF THE CURRENT STATE OF THE PROBLEM: THE PRACTICAL ASPEC



2. THE CONCEPT OF CONSTRUCTING A SYNERGISTIC MODEL OF THREATS TO THE SECURITY OF BANKING INFORMATION RESOURCES



2. THE CONCEPT OF CONSTRUCTING A SYNERGISTIC MODEL OF THREATS TO THE SECURITY OF BANKING INFORMATION RESOURCES



The first level *describes the general corporate strategy of the bank and its functional strategies, determines the state of security of the BIR*

- the current state of the IS is determined;
- investments in the security system are estimated;
- minimization of investments into the security system is carried out;
- IS policies are implemented taking into account the hybridity of threats

2. THE CONCEPT OF CONSTRUCTING A SYNERGISTIC MODEL OF THREATS TO THE SECURITY OF BANKING INFORMATION RESOURCES

At the second level, the corporate strategy of IS BIR is formed

many requirements of BIR safety regulators

many assessments of the degree to which security requirements are met

the set of the final level of security compliance BIR

an assessment of the level of protection of BIR in accordance with the requirements of security regulators

At the **third level,** the corporate strategy of BIR SI is formed, the correspondence between applied TMIS and the threats to the InfoSec, CyberSec, SI on BIR is determined

OPZ [redacted]

the correspondence between the used technical means of information protection and threats in the BIR is determined

The concept is based on the synergetic approach to choosing the most effective directions for achieving the set objectives of the BIR security, taking into account the magnitude of risk at each level.

3. A SYNERGISTIC APPROACH TO BUILDING A SECURITY SYSTEM

Advanced Threat Classifier

generalized synergistic threat to BIR

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}$$

given its hybridity

$$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{I} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}.$$

Advanced ABS Infrastructure Model

$$G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}$$

Synergetic threat model

$$GR^{ABS} = \left\{\left\{DF^{ABS}\right\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\right\}$$

Evaluation of security of banking information in the ABS

Advanced intruder model

$$G_{IA}^{ABS} = \left\{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS}\right\}$$

$$\forall i \in n, \forall j \in m$$

Improved security assessment model

$$G_{OZ}^{ABS} = \left\{\begin{matrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{matrix}\right\},$$

value of the generalized indicator of the level of security of the ABS

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i \quad \Rightarrow \quad UZ^{ABS} = \begin{cases} \text{tall, if } OPZ^{ABS} = 3; \\ \text{average, if } 1 \le OPZ^{ABS} \le 3; \\ \text{low, if } OPZ^{ABS} = 0. \end{cases}$$

Stage 1. *Determination of the probability of the impact of IS, CS, and SI threats on the security of a BIR based on the threat classifier.*

Step 1. Formation of classifier metrics

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$$

w_{ik}^j – coefficient metric value; N – number of threats; K – number of experts.

Step 2. Formation of a digital identifier of the threat identifier

Step 3. Selection of weighting coefficients α_i, determining the conditions for the manifestation of the i-th threat

Step 4. Determining the implementation of each i-th threat, taking into account the likelihood of attacks

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j.$$

Step 5. Determining the implementation of the occurrence of multiple threats to the selected service:

$$W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C \quad W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I \quad W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A \quad W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au}$$

Step 6. Determination of the total threat by security components:

$$W_{synerg}^{IS} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i, \qquad W_{synerg}^{CS} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i$$

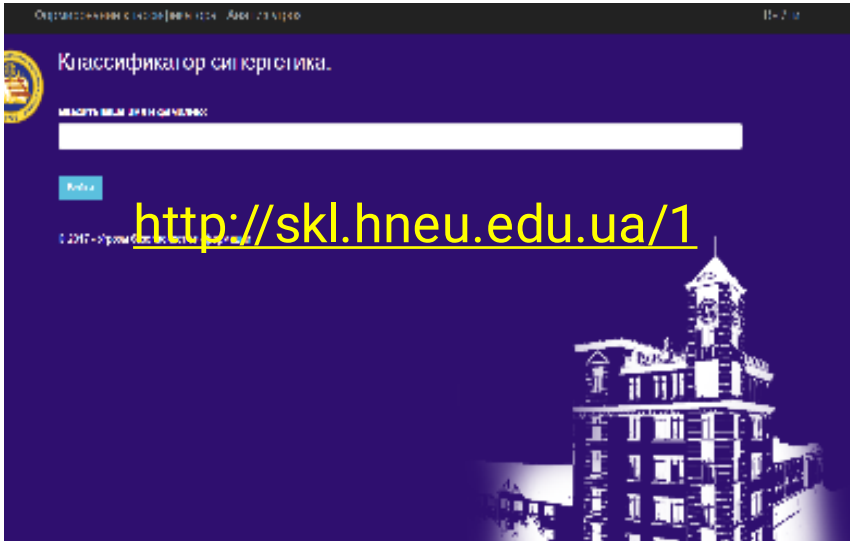
Step 7. Determination of the generalized synergetic threat of BIR:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI}$$

Step 8. Determination of the generalized synergetic threat of BIR, taking into account its hybridity:

$$W_{synerg}^{\text{hybrid}\,C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{\mathrm{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}.$$

3. SECURITY THREATS FOR BANKING INFORMATION



COMPOSITION OF THE CLASSIFICATOR:

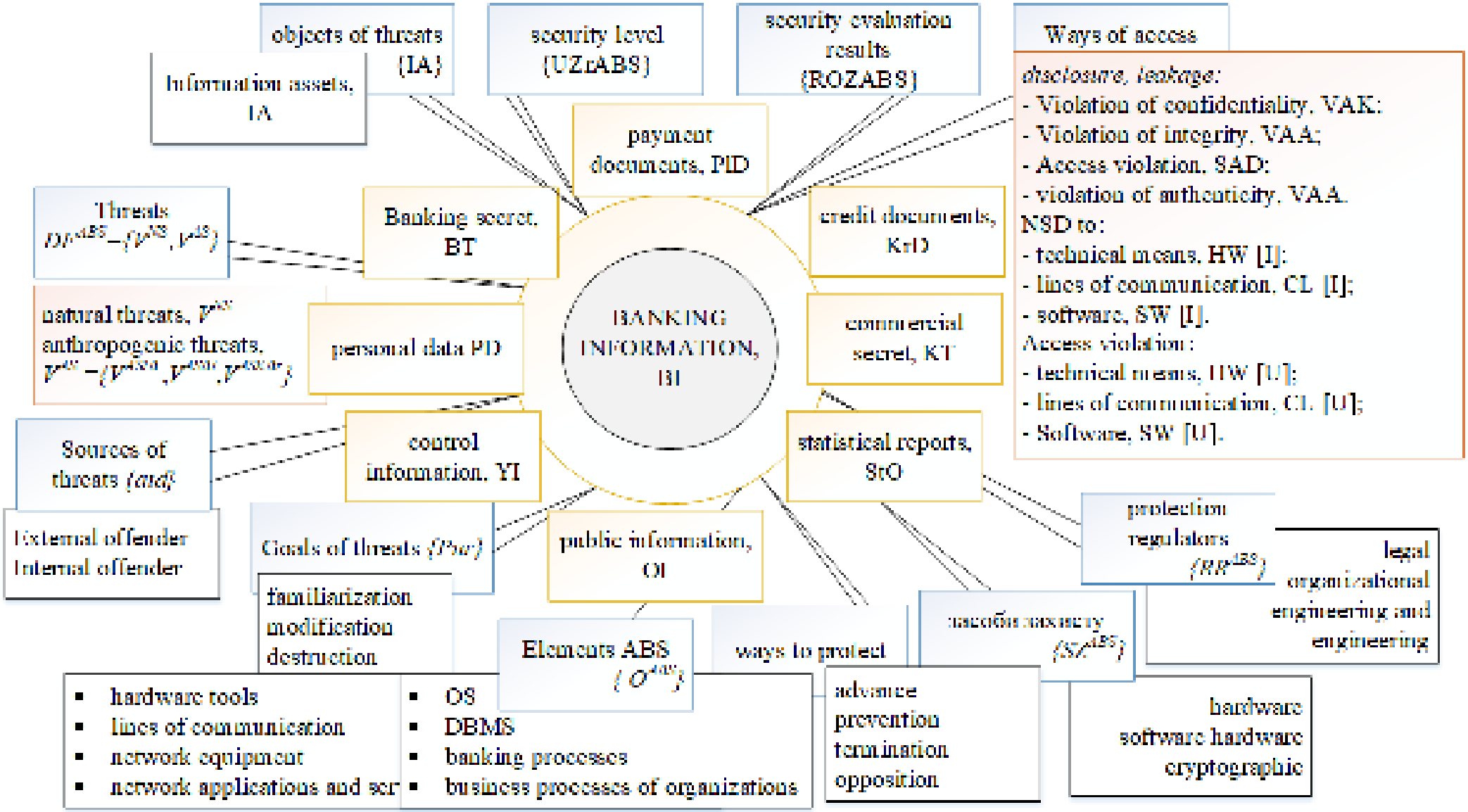
Security:
InfoSec (01), SI (02), CyberSec (03)

The nature of the security threats:
normative legal (01), organizational (02), engineering (03)

BIR Properties:
confidentiality (01), integrity (02), accessibility (03), authenticity (04);

Levels of ABS infrastructure hierarchy:
PL - Physical level (01),
NL - Network level (02),
OSL - Operating System Level (OS) (03),
DBL - level of database management systems (04),
BL - level of banking technological applications and services (05).

4. METHOD OF ESTIMATING THE GENERALIZED INDICATOR OF THE LEVEL OF SECURITY OF BANKING INFORMATION



CONCEPTUAL SYNERGETIC MODEL OF SECURITY OF BANKING INFORMATION

Stage 2. *Determination of dependencies between the elements of the ABS infrastructure, information assets of BIn, threats to IS, CS, SI and technical protection tools*

Step 1. Identify the relationship between information assets and infrastructure elements based on the model.

$$A^{ABS} = \left\| a_{ij}^{ABS} \right\|$$

Step 2. Determining the relationship between information assets and environment elements

$$IO^{R} = \left\| IO_{il}^{R} \right\| \qquad IO_{il}^{R} = \begin{cases} 0, \text{ no connection} \\ cs, \text{ includes and stores} \\ pt, \text{ processes or transfers} \\ so, \text{ supports functioning} \end{cases}$$

Step 3. Determine the multiplexing of threats based on a synergistic threat model and an improved attacker model

$$A^{DF} = \left\| a_{ij}^{DF} \right\|$$

Step 4. Determine the total risk price of all assets:

$$R_{total} = \sum_{j=1}^{n} R_j$$

Step 5. Determine the likelihood of at least one threat for each asset:

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right)$$

Step 6. Determining the relationship between the sources of threats and elements of the ABS:

$$A^{DF} = \left\| a_{ij}^{DF} \right\|$$

4. METHOD OF ESTIMATING THE GENERALIZED INDICATOR OF THE LEVEL OF SECURITY OF BANKING INFORMATION

The main advantage of the method is the integration of hybrid threats, banking information assets, ABS elements and communication lines, and ABS information security tools.

This approach allows us to obtain a full and adequate assessment of the level of security of the BIR, which significantly affects the amount of investments in securing the banking sector and opens the way for sound management decisions on security issues of banking information resources.

4. METHOD OF ESTIMATING THE GENERALIZED INDICATOR OF THE LEVEL OF SECURITY OF BANKING INFORMATION

Stage 3. *Determination of the generalized indicator of the level of security of BID on the basis of an improved model*

Step 1. Determination of the relationship between threats and TSSI

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\| \qquad \left\| a_{ij}^{DFSZ} \right\| = \begin{cases} MZ, \text{ if } i \text{ the threat is closing } j\text{-м TSSI} \\ NMZ, \text{ if } i \text{ the threat does not close } j\text{-м TSSI} \end{cases}$$

Step 2. Determining the many requirements of regulators

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}$$

Step 3. Determination of the value of the generalized indicator of the level of security of the ABS

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i \qquad UZ^{ABS} = \begin{cases} \text{tall, if } OPZ^{ABS} = 3; \\ \text{average, if } 1 \le OPZ^{ABS} \le 3; \\ \text{low, if } OPZ^{ABS} = 0. \end{cases}$$

Serhii.Yevseiev@hneu.net

4. CONCLUSIONS

1. ***The concept of constructing a synergistic model of threats to the security of banking information resources, based on a three-level model of strategic management of security of banking information technologies through the integration of information security, cyber security and security of information components,*** opens a new direction in ensuring the security of banking information resources based on the model of strategic bank management taking into account the degree of risk at each level and effective control over the performance of Management system functions of Organizations Information Security of banking sector.

2. ***The proposed classification of threats to security of banking information resources, which, unlike the known ones,*** is based on a synergistic model of threats, which allows to classify threats to security components, types of services and levels of automated banking system infrastructure hierarchy, ***to assess*** **the synergy and hybridity of threats to information security, cyber security and security of information, the probability of their impact on the security of banking information resources.**

3. ***The method of estimating the generalized indicator of the level of security of banking information resources is developed, which provides the possibility of establishing interconnections between the elements*** of the hierarchical structure of the automated banking system, communication channels, information assets of banking information resources and threats to information security, cybersecurity, security of information to **achieve synergistic effect,** and definition of the level of security of banking information resources