Научный центр информационных технологий и искусственного интеллекта
Center for Information Technologies and Artificial Intelligence

Университет Сириус

МОДЕЛЬ ЛОГИЧЕСКОГО ВЫВОДА ДЛЯ СТРУКТУРНО-ПАРАМЕТРИЧЕСКОГО СИНТЕЗА КОНСТРУКТИВНОЙ ЗАЩИТЫ

LOGICAL INFERENCE MODEL FOR THE STRUCTURAL-PARAMETRIC SYNTHESIS OF CONSTRUCTIVE PROTECTION

д.т.н. Сундеев Павел Викторович
Pavel V. Sundeev Doctor of Technical Sciences

The results were obtained with the financial support of the project “Technologies for countering previously unknown quantum cyber threats”, implemented within the framework of the state program of the “Sirius” Federal Territory “Scientific and technological development of the “Sirius” Federal Territory (Agreement No. 23-03 dated September 27, 2024)

© д.т.н. Сундеев П.В.

Университет Сириус

УРОВНИ, МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
LEVELS, MODELS, AND METHODS OF INFORMATION PROTECTION

УРОВНИ ЗАЩИТЫ PROTECTION LEVELS	МЕТОДЫ И МОДЕЛИ ЗАЩИТЫ METHODS AND MODELS OF PROTECTION
РИСКИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ **INFORMATION SECURITY RISKS**	Экспертные методы оценки рисков безопасности информации **Expert methods for assessing information security risks**
ПОЛИТИКА УПРАВЛЕНИЯ ДОСТУПОМ **ACCESS CONTROL POLICY (ACP)**	Формальные модели разграничения (управления) доступа **Formal access control models**
АРХИТЕКТУРА СИСТЕМЫ **SYSTEM ARCHITECTURE**	Модель архитектуры с недостатками реализации ACP (модель угроз) **The architecture model with the disadvantages of implementing the ACP**
СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ **INFORMATION PROTECTION SYSTEM**	Модели и методы анализа и синтеза защиты информации (модель защиты) **Models and methods of information protection analysis and synthesis**
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ **INFORMATION PROTECTION TOOLS**	Формальные методы оценки эффективности средств защиты **Formal methods for evaluating the effectiveness of protection tools**

Университет Сириус

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ КВАНТОВЫМ УГРОЗАМ
TECHNOLOGY FOR COUNTERING QUANTUM THREATS

КРИПТОГРАФИЯ И ДЕЦЕНТРАЗИЛАЦИЯ - ОСНОВА КОНСТРУКТИВНОЙ ЗАЩИТЫ DLT
CRYPTOGRAPHY AND DECENTRALIZATION ARE THE BASIS FOR CONSTRUCTIVE DLT PROTECTION

Синтез безопасной архитектуры
Synthesis of a secure architecture

КВАНТОВЫЕ ТЕХНОЛОГИИ СОЗДАЮТ УГРОЗУ КОМПРОМЕТАЦИИ КРИПТОГРАФИИ
QUANTUM TECHNOLOGIES POSE A THREAT TO COMPROMISE CRYPTOGRAPHY

Информация с горизонтом секретности 5-10 лет уже в зоне риска компрометации
Information with a security horizon of 5-10 years is already at risk of compromise

Анализ конструктивной защиты
Constructive protection analysis

РАЗРАБОТАТЬ ТЕХНОЛОГИЮ ЗАЩИТЫ АРХИТЕКТУРЫ С НОВОЙ КРИПТОГРАФИЕЙ
TO DEVELOP AN ARCHITECTURE PROTECTION TECHNOLOGY WITH NEW CRYPTOGRAPHY

Технология должна обеспечить формальный анализ и синтез конструктивной защиты систем
The technology should provide a formal analysis and synthesis of constructive protection systems

ФОРМАЛЬНАЯ МОДЕЛЬ И МЕТОД АНАЛИЗА И СИНТЕЗА КОНСТРУКТИВНОЙ ЗАЩИТЫ
FORMAL MODEL AND METHOD OF ANALYSIS AND SYNTHESIS OF CONSTRUCTIVE PROTECTION

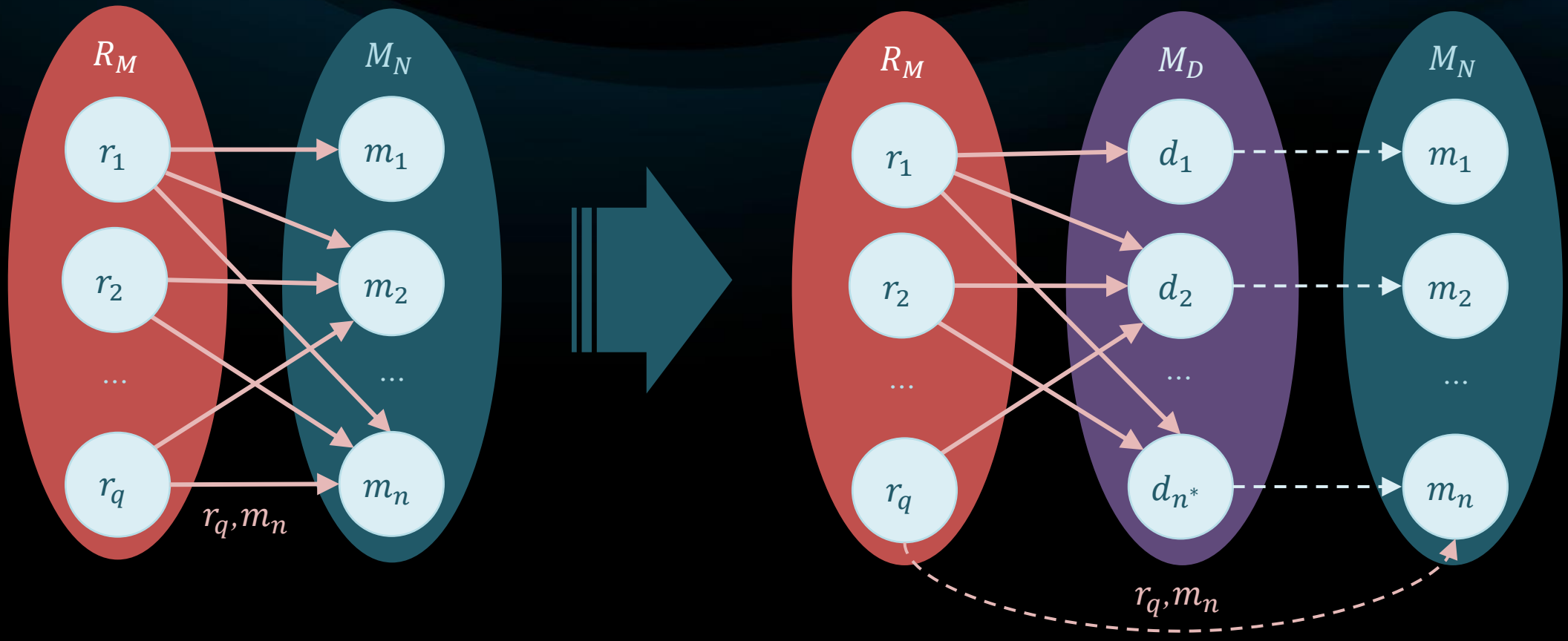
МЕТОД МОДИФИКАЦИИ ПОСТКВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ
A METHOD FOR MODIFYING POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

Новые криптографические алгоритмы
New cryptographic algorithms

Университет Сириус

МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ

A FULL-OVERLAP INFORMATION PROTECTION MODEL



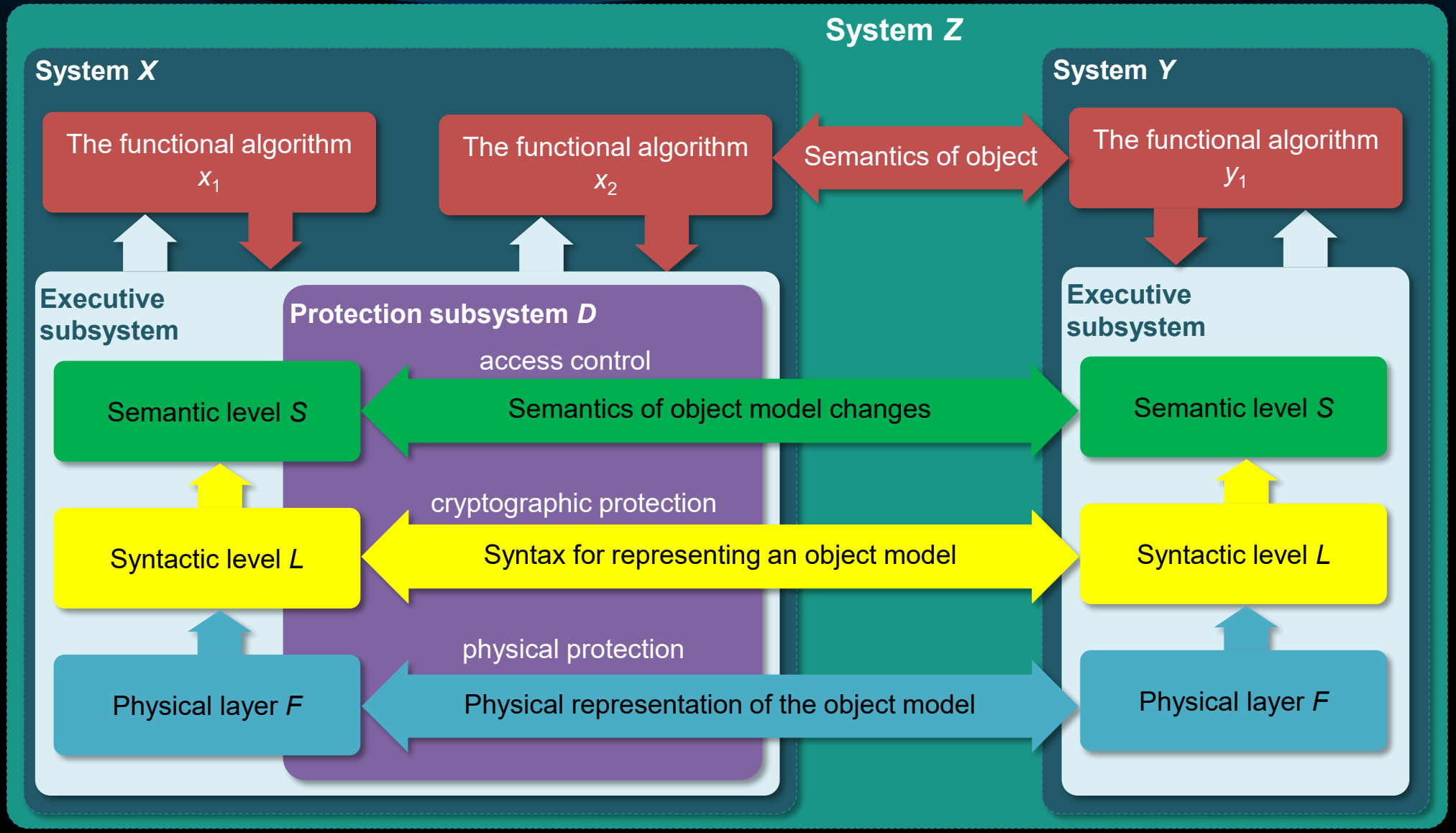
Модель защиты с полным перекрытием:
Отображение множества взаимодействий R_M на множество модулей M_N через множество средств защиты информации M_D

Full-overlap protection model:
Mapping multiple R_M interactions to multiple M_N modules through multiple M_D information security tools

© к.т.н. Сундеев П.В.

Университет Сириус

МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ
THE INFORMATION INTERACTION MODEL

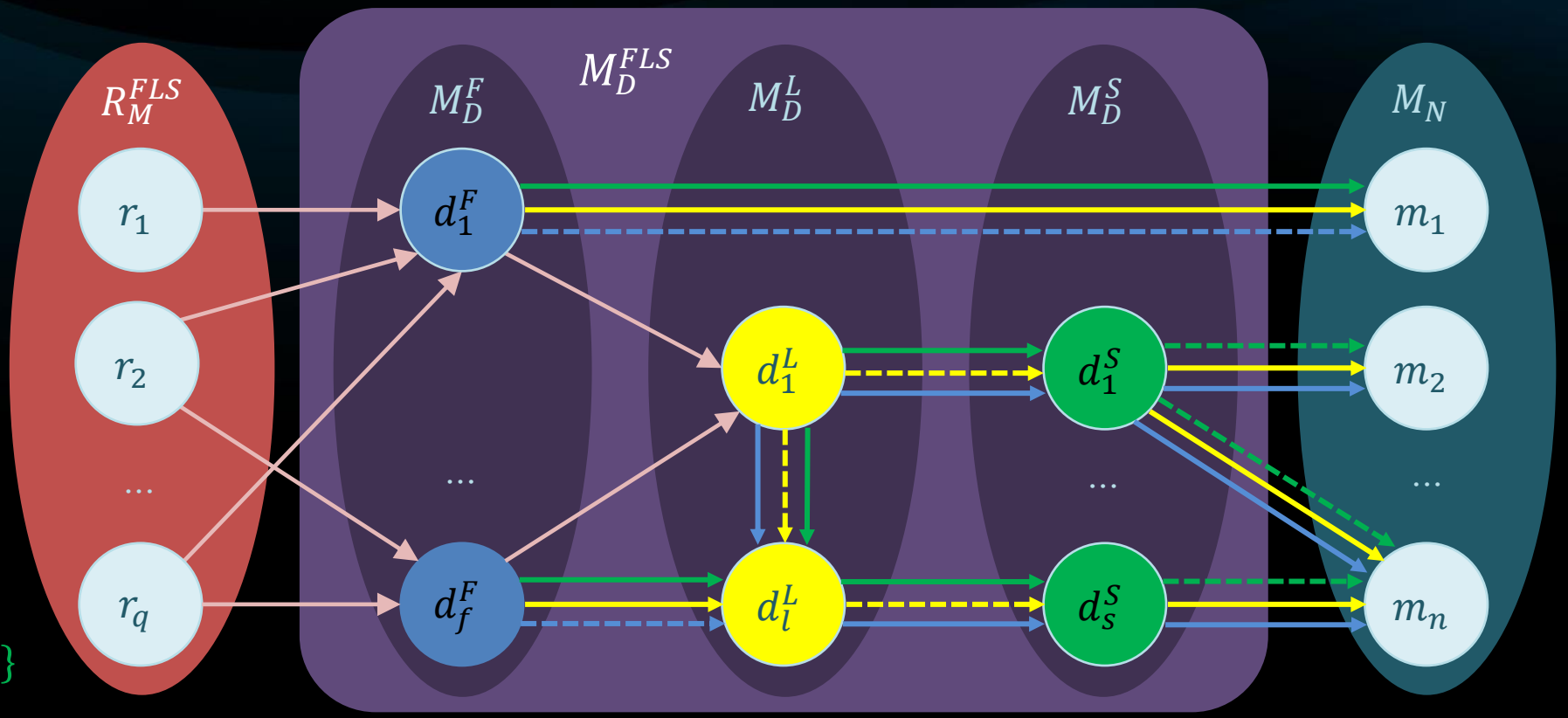


© д.т.н. Сундеев П.В.

Университет Сириус

FLS-МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ

A FULL-OVERLAP INFORMATION PROTECTION FLS-MODEL



$$R_M^{FLS} \subseteq \{R^F \cup R^L \cup R^S\}$$
$$R^F = \{r_f^F\}, R^L = \{r_l^L\}, R^S = \{r_s^S\}$$

Расширенная модель защиты с полным перекрытием

Отображение множества информационных взаимодействий R_M^{FLS} на множество модулей M_N через множество M_D^{FLS} средств защиты

Extended protection model with full overlap

Displaying multiple information interactions R_M^{FLS} many modules M_N through many M_D^{FLS} means of protection

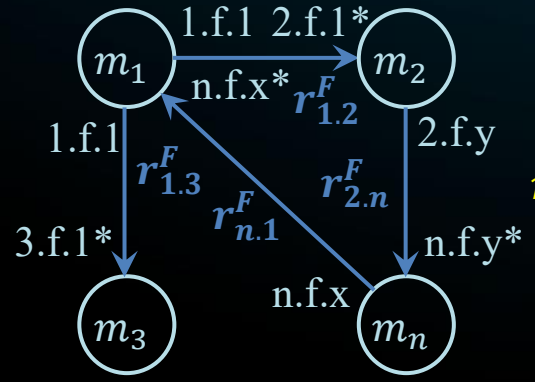
© к.т.н. Сундеев П.В.

Университет Сириус

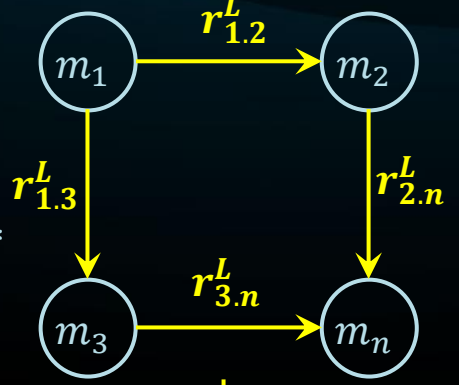
FLS-МУЛЬТИГРАФ ИНФОРМАЦИОННОЙ СИСТЕМЫ

FLS-MULTIGRAPH OF AN INFORMATION SYSTEM

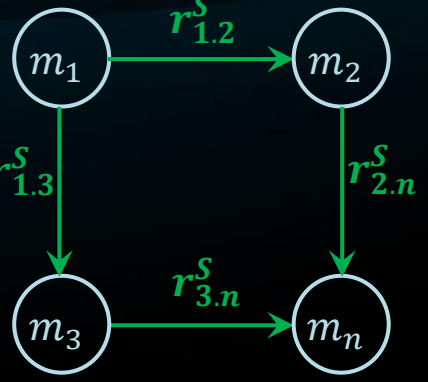
F-subgraph



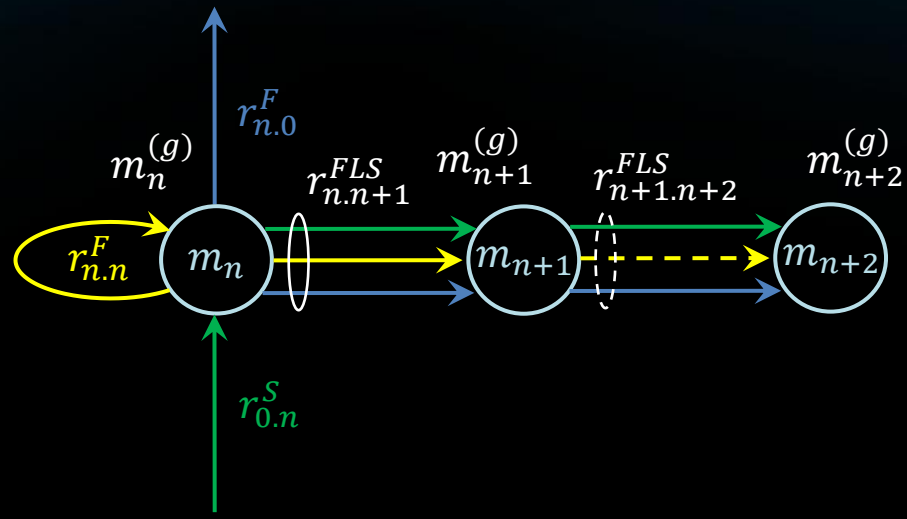
L-subgraph

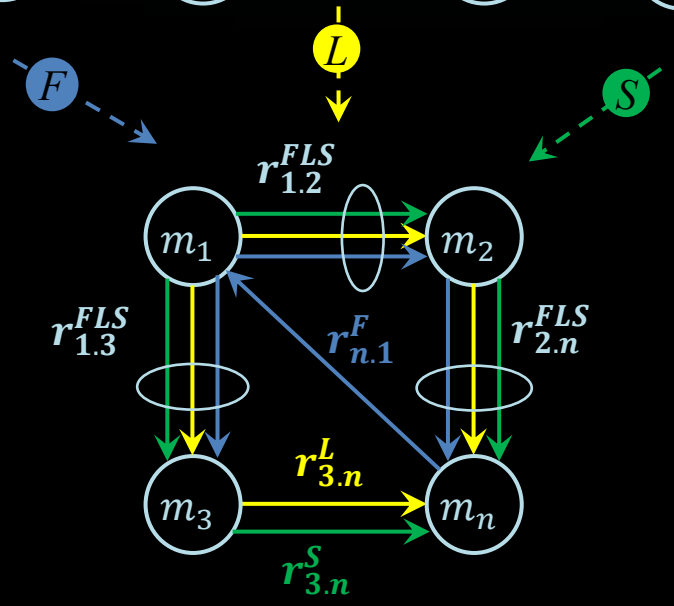


S-subgraph



Structural elements of the *FLS*-multigraph





Multigraph
$G^{FLS} = (M_N, R^{FLS}_M)$

$$\begin{cases} \forall A^F(i,j) = 1 \leftrightarrow \exists P^F(m_i, m_j) \\ \forall A^L(i,j) = 1 \leftrightarrow \exists P^F(m_i, m_j) \wedge \exists P^L(m_i, m_j) \\ \forall A^S(i,j) = 1 \leftrightarrow \exists P^F(m_i, m_j) \wedge \exists P^L(m_i, m_j) \wedge \exists P^S(m_i, m_j) \end{cases}$$

© д.т.н. Сундеев П.В.

Университет Сириус

ФОРМАЛЬНОЕ ОПРЕДЕЛЕНИЕ КЛАСТЕРНОЙ СТРУКТУРЫ
FORMAL DEFINITION OF THE CLUSTER STRUCTURE

Кластерная структура системы *Z* определяется на множестве модулей $M_N = \{M_x^X, M_y^Y, M_d^D\}$ информационной системы *X* и ее окружения *Y*, множествах *FLS*-отношений $R_M^{FLS} = \{R^F, R^L, R^S\}$ и кластеров $K^Z = \{K^X, K^Y, K^D\}$

The cluster structure of the Z system is defined on a set of modules $M_N = \{M_x^X, M_y^Y, M_d^D\}$ information system *X* and its environment *Y*, sets of *FLS*-relationships $R_M^{FLS} = \{R^F, R^L, R^S\}$ и кластеров $K^Z = \{K^X, K^Y, K^D\}$

$$G_Z^{FLS}(M_N, R_M^{FLS}) \equiv \begin{cases} M_N = \{M_x^X, M_y^Y, M_d^D\} | \{M_x^X \cap M_y^Y \cap M_d^D\} = \emptyset; \\ R_M^{FLS} = \{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}; \\ K^Z = \{K^X, K^Y, K^D\} | \{K^X \cap K^Y \cap K^D\} = \emptyset; \end{cases}$$

где $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ – подмножества полных внутренних $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}\}$ и внешних $\{R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ *FLS*-дуг кластеров $\{K^X, K^Y, K^D\}$

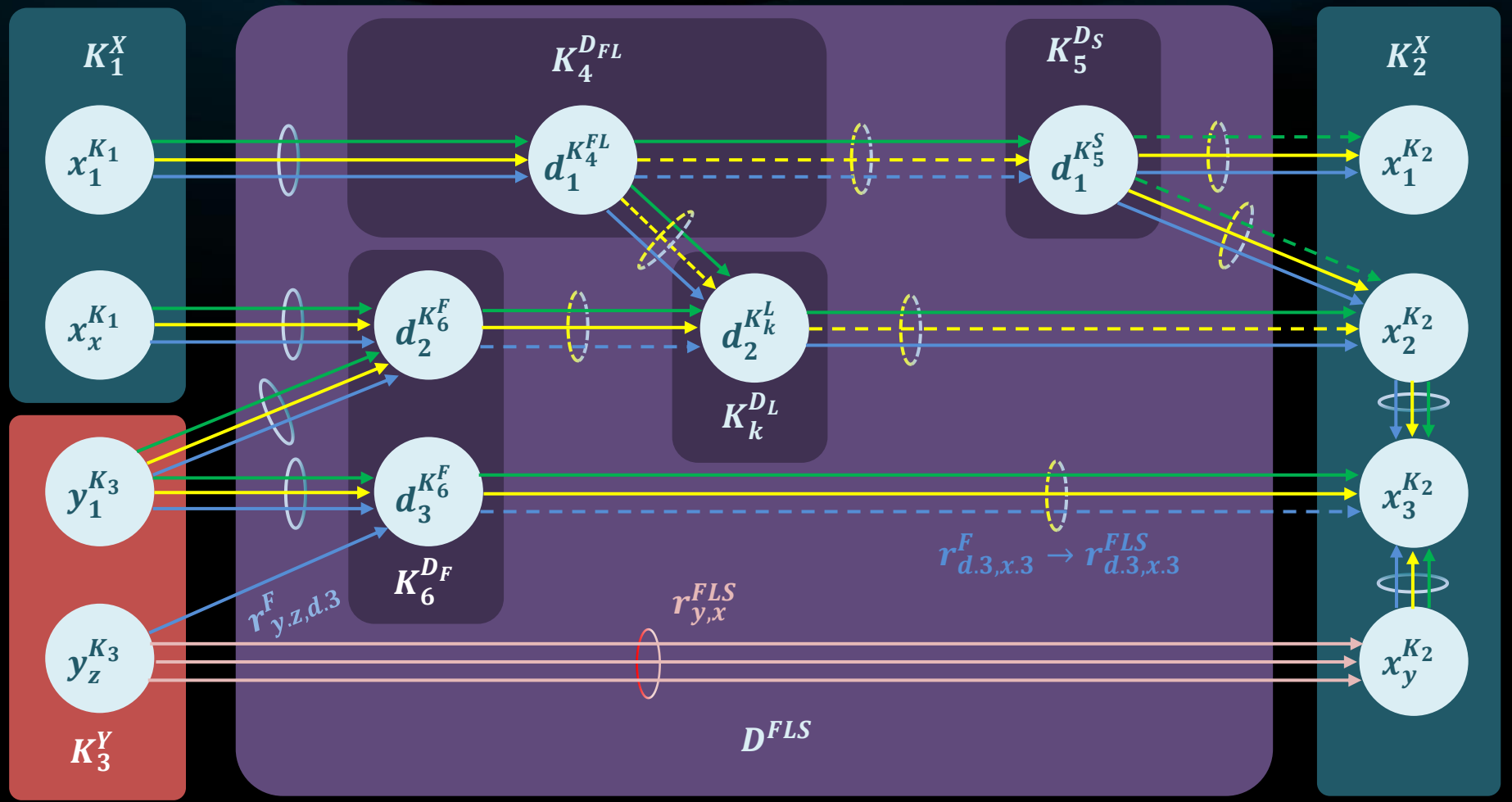
where $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ - subsets of complete internal $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}\}$ and external ones $\{R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ *FLS*-arcs of clusters $\{K^X, K^Y, K^D\}$

© д.т.н. Сундеев П.В.

Университет Сириус

КЛАСТЕРНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ

CLUSTER MODEL OF INFORMATION PROTECTION



© д.т.н. Сундеев П.В.

Университет Сириус

МОДЕЛЬ ЛОГИЧЕСКОГО ВЫВОДА С МАШИННЫМ ОБУЧЕНИЕМ

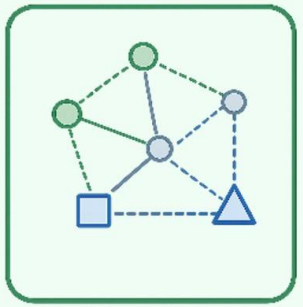
LOGICAL INFERENCE MODEL WITH MACHINE LEARNING

1 Initial data



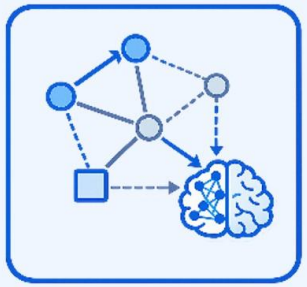
- modules and interfaces
- access policy
- protection criteria
- change log
- incidents

2 Formation of a heterogeneous *FLS*-multigraph



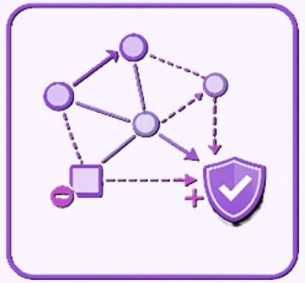
- nodes, arcs, attributes, clusters

3 Heterogeneous GNN



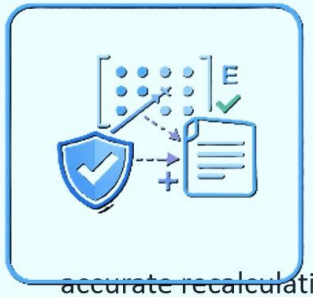
- risk-the speed of nodes / arcs / paths
- top-k candidates for modification
- assessment of

4 The candidate generator ΔG



- add/remove/redirect an arc, replace or add a protection node

5 The Formal Verification Unit (LIM)



- accurate recalculation of reachability **P**
- calculation of the matrix of dangerous conditions **E**
- verification of criteria **C**

6

$|P| > |C|$?

Have the protection criteria been met?

Yes

No

Additional training and adjustments

7 Counterexample



- A dangerous path
- Is the absence or non-compliance of a means of protection

8 Buffer of counterexamples



Teaching negative examples

9 Secure architecture and explicable solution



Accepted change of Δ*G* (modified *FLS*-multigraph) and formal proof of absence of dangerous conditions (**E**= 0) and fulfillment of protection criteria **C**

Университет Сириус

ГИБРИДНАЯ ML-МОДЕЛЬ СИНТЕЗА КОНСТРУКТИВНОЙ ЗАЩИТЫ
HYBRID ML MODEL FOR THE SYNTHESIS OF CONSTRUCTIVE PROTECTION

Hybrid model with machine learning

Structural-parametric synthesis is implemented using a hybrid model that automates the processing of large volumes of data and complex dependencies between features, employing ML, logical interpretation (explainability), and formal verification of compliance with protection criteria in a logical inference machine. The model can be retrained when access policies, protection requirements, and design protection criteria change. The ML model is limited by expert rules and classical algorithms to ensure reliability and interpretability. Logical rules prevent dangerous decisions that an ML algorithm might propose.

Graph neural network (GNN) with an attention mechanism (GAT) makes it possible to:

- formalize complex access rules in the form of a mathematical matrix
- automate the construction and updating of the reference cluster matrix
- take into account static rules (policies, norms) and dynamic criteria (weights, topology, clusters)
- scale the solution to large graphs through clustering and prediction at the cluster level

© д.т.н. Сундеев П.В.

Университет Сириус

ML-МОДЕЛЬ. РАЗМЕТКА ДАННЫХ
ML MODEL. DATA MARKUP

To build the initial information model of the architecture, the composition of modules (object-oriented objects and classes) and their characteristics is determined, as well as the cluster structure of the FLS multigraph. The task of module labeling is solved using ML based on logical rules

Module labeling formula

$$M_N^{XYD} = \{M_x^X, M_y^Y, M_d^D\} = \mathrm{ML}_{\mathrm{class}}(x_i) \cup \mathrm{Logic}_{\mathrm{rules}}(r_j),$$

where $\mathrm{ML}_{\mathrm{class}}$ — a machine learning classifier (Random Forest) that determines the type of module (F or L) based on features x_i

$\mathrm{Logic}_{\mathrm{rules}}$ — a set of logical rules clarifying the classification ("if the module has a physical embodiment, then M^F")

The interface markup formula defines the composition of the module's FLS interfaces

$$I^{FLS} = \bigcup_{k \in \{F,L,S\}} \left(\mathrm{ML}_{\mathrm{detect}}(f_k) \cap \mathrm{Logic}_{\mathrm{validate}}(v_k)\right),$$

where $\mathrm{ML}_{\mathrm{detect}}$ — interface type detection model (*F*, *L*, *S*)

$\mathrm{Logic}_{\mathrm{validate}}$ — checking the pairing of interfaces ("out." – "in.") and their compatibility

The formula for defining access policy markup to formalize the cluster structure of a multigraph

$$V = \{v_1, \dots, v_v\} = \mathrm{ML}_{\mathrm{policy}}(p) \cup \mathrm{Logic}_{\mathrm{access}}(a),$$

where $\mathrm{ML}_{\mathrm{class}}$ — A model for sampling access vectors v from textual descriptions of access policies

$\mathrm{Logic}_{\mathrm{access}}$ — formal access rules (for example, RBAC or ABAC)

© д.т.н. Сундеев П.В.

Университет Сириус

ML-МОДЕЛЬ. ОПТИМИЗАЦИЯ ЗАЩИТЫ
ML MODEL. OPTIMIZATION OF PROTECTION

Multigraph optimization

Objective function

$$\min_{G^{FLS}} \left(\alpha \cdot \text{Cost}(G^{FLS}) + \beta \cdot \text{Risk}(G^{FLS}) + \gamma \cdot \text{Comlexity}(G^{FLS}) \right)$$

where Cost — implementation cost (number of modules, arcs)

Risk — risk of violating access policy ($\sum e_{ij}$)

Complexity — the complexity of the architecture (number of clusters, connections)

α, β, γ — weighting coefficients

Limitations

- Compliance with access policy

$$\forall i,j: r_{ij} = 1 \Rightarrow c_{ij} = 1 \vee \exists m_k \in P_{ij}: m_k \in M_d^D$$

- Structural protection

$$\sum_{m_k \in M_d^D} g(m_k) \geq G_{\min}$$

where $g(m_k)$ — the weight of the protection module, $G_{\min}$ — the minimum required level of protection.Кластерная целостность

$$K^Z = K^X \cup K^Y \cup K^D, K^X \cap K^Y \cap K^D = \emptyset$$

- The condition for the existence of arcs

$$\forall r_{ij}^{FLS}: a_{ij}^F = a_{ij}^L = a_{ij}^S = 1$$

© д.т.н. Сундеев П.В.

Университет Сириус

ВЫВОДЫ
CONCLUSIONS

The logical inference model automates the process of synthesizing the structural protection of information systems by optimizing data markup, predicting dangerous conditions, and generating protection using machine learning. The ML model allows you to automate the analysis of the multigraph structure, identify dangerous conditions and generate candidates for architectural changes while maintaining the formal verifiability of the result in LIM. The inference model provides a formal proof of architecture security, which is essential for critical applications. The structural-parametric synthesis is provided by a formal description of the requirements in terms of the cluster protection model represented by the FLS-multigraph. The accuracy of the model is achieved by formally describing the criteria for information protection by multigraph clusters and decomposing information links into interaction levels through which information processing and protection functions are implemented, as well as by formally assessing the compliance of the architecture with the protection criteria in the inference machine.

The hybrid model can be used to automate the process of structurally parametric synthesis of constructive protection of distributed resources, national platforms and other critical information systems, taking into account the declared access policy, requirements of regulatory documents and standards for constructive protection with evidence of their implementation and optimization according to the criteria of constructive protection.

© д.т.н. Сундеев П.В.

01001001 00100000 01110111 01100001 01101110 01110100 00100000 01110100 01101111 00100000 01110011 01100101 01100101 00100000 01110111 01101000 01100001 01110100 00100111 01110011 00100000 01101001 01101110 01110011 01101001 01100100 01100101 00100000 01111001 01101111 01110101

