

Научная статья

УДК 004.056.5

<https://doi.org/10.31854/1813-324X-2025-11-1-70-83>

EDN:QOBBRA



Метод моделирования коммуникационной инфраструктуры на основе средств имитационного и полунатурного моделирования

Дмитрий Александрович Васинев, vda33@academ.msk.rsnet.ru

Академия Федеральной службы охраны Российской Федерации,
Орел, 302015, Российская Федерация

Аннотация

Актуальность исследования объясняется сложившимся противоречием предметной области, которое заключается в динамически меняющейся в процессе функционирования коммуникационной инфраструктуры объекта критической информационной инфраструктуры (КИИ), а также методах воздействия нарушителя на объект КИИ, создающих предпосылки для снижения уровня информационной безопасности, и возможностями существующих методов оценки защищенности объекта на основе сигнатур, экспертного подхода, а также методов и средств обеспечения информационной безопасности, не позволяющих учитывать такую динамику изменения уровня информационной безопасности объекта.

Цель исследования: обеспечение информационной безопасности коммуникационной инфраструктуры объектов КИИ за счет учета коммуникационных и конфигурационных параметров, динамики взаимодействующих субъектов.

Методы исследования: математические методы теории систем и системного анализа, теории вероятностей, методы теории графов, методы имитационного моделирования.

Результаты. В статье представлен метод моделирования коммуникационной инфраструктуры, который позволяет формировать параметрически точные имитационные модели объекта КИИ для исследования свойств защищенности и устойчивости, моделировать воздействия нарушителя на объект КИИ.

Новизна. Разработан метод моделирования коммуникационной инфраструктуры на основе конфигурационных и коммуникационных параметров объекта КИИ, учитывающий динамику взаимодействия коммуникационной инфраструктуры, политики его информационной безопасности и действия нарушителя.

Теоретическая значимость. Развитие методов информационной безопасности в области моделирования коммуникационной инфраструктуры объектов КИИ на основе гиперграфов, вложенных раскрашенных сетей Петри, позволяющих учитывать динамику взаимодействующих субъектов (коммуникационную и конфигурационную инфраструктуру, политику информационной безопасности, воздействие нарушителя).

Практическая значимость. Метод моделирования позволяет учитывать конфигурационные и коммуникационные особенности построения и функционирования объекта КИИ, параметры воздействия нарушителя на объект КИИ, существующую политику безопасности, моделировать свойство устойчивости, проводить исследование влияния взаимодействующих субъектов на защищенность объекта КИИ, уменьшить зависимость от экспертных оценок, получать параметрически обоснованные оценки защищенности коммуникационной инфраструктуры объекта КИИ.

Ключевые слова: критическая информационная инфраструктура, коммуникационная инфраструктура, конфигурационная инфраструктура, метод моделирования, метод оценки защищенности, киберустойчивость, протокольные блоки данных


Ссылка для цитирования: Васинев Д.А. Метод моделирования коммуникационной инфраструктуры на основе средств имитационного и полунатурного моделирования // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 70–83. DOI:10.31854/1813-324X-2025-11-1-70-83. EDN:QOBBRA

Original research

<https://doi.org/10.31854/1813-324X-2025-11-1-70-83>

EDN:QOBBRA

Method of Communication Infrastructure Modeling Based on Simulation and Semi-Natural Modeling

 Dmitry A. Vasinev, vda33@academ.msk.rsnet.ru

Academy of the Russian Federal Guard Service,
Orel, 302015, Russian Federation

Annotation

The relevance of the research is explained by the existing contradiction of the subject area, which consists in the communication infrastructure of the critical information infrastructure (CII) object dynamically changing in the process of functioning, as well as the methods of the intruder's impact on the CII object, as well as the methods of the intruder's impact on the CII object, which create preconditions for reducing the level of information security and the capabilities of the existing methods of assessing the object's security based on signatures, expert approach, as well as methods and means of ensuring information security, which do not allow taking into account such dynamics of changes in the level of information security of the object.

Purpose of the research. Provision of information security of communication infrastructure of CII objects by taking into account communication and configuration parameters, dynamics of interacting subjects.

Research methods. Mathematical methods of systems theory and system analysis of probability theory, methods of graph theory, methods of simulation modeling.

Results. The article presents a method of modeling of communication infrastructure that allows to form parametric accurate simulation models of the CII object to study the properties of security and stability, to simulate the impact of an intruder on the CII object.

Novelty. A method of modeling the communication infrastructure based on configuration and communication parameters of the CII object has been developed, taking into account the dynamics of communication infrastructure interaction, its information security policy and intruder actions.

Theoretical significance. Development of information security methods in the field of modeling the communication infrastructure of CII objects on the basis of hypergraphs, nested colored Petri nets, allowing to take into account the dynamics of interacting subjects (communication and configuration infrastructure, information security policy, the impact of the intruder).

Practical significance. The modeling method allows to take into account configuration and communication peculiarities of construction and functioning of the CII object, parameters of the intruder's impact on the CII object, the existing security policy, to model the stability property, to conduct research of the influence of interacting subjects on the security of the CII object, to reduce the dependence on expert assessments, to receive parametrically justified assessments of the security of the communication infrastructure of the CII object.

Keywords: critical information infrastructure, communication infrastructure, configuration infrastructure, modeling method, security assessment method, cyber resilience, protocol data blocks

For citation: Vasinev D.A. Method of Communication Infrastructure Modeling Based on Simulation and Semi-Natural Modeling. *Proceedings of Telecommunication Universities*. 2025;11(1):70–83. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-70-83. EDN:QOBBRA

Введение

Продолжающееся информационное противоборство делает актуальными вопросы обеспечения информационной безопасности (ИБ) для информаци-

онных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления (АСУТП) критических информационных инфраструктур (далее КИИ), функциони-

рующих в критически важных отраслях деятельности государства (в медицине, образовании, промышленности, энергетике поясняется отраслевой принадлежностью объектов атак). Среди прочих, целью нарушителя являются объекты КИИ. При этом уровень деструктивных действий нарушителя на коммуникационную инфраструктуру говорит о сетевых угрозах преимущественно высокого и критического уровней воздействия нарушителя, проявляющихся в атаках на КИИ¹²³. В качестве составных элементов КИИ выступают распределенные фрагменты сетей, центры обработки данных (ЦОД), АСУТП, объединенные в единую распределенную ИТС организации. Пример обобщенного представления распределенной КИИ представлен на рисунке 1.

Существующие особенности построения коммуникационной инфраструктуры технологически достаточно разнообразны [1, 2]. Общими моментами являются применение технологий виртуальных частных сетей (VPN, от англ. Virtual Private Network), резервирования, отказоустойчивости,

обеспечение киберустойчивости в условиях воздействия компьютерных атак (КА) [3–6]. Кроме того, современные условия функционирования технических систем предполагают применение отечественного коммуникационного оборудования, средств защиты для проектирования новых и импортозамещения существующих фрагментов КИИ. В этих условиях исследование в области оценки защищенности и устойчивости КИИ при воздействии на нее КА с учетом параметрических особенностей объекта, самого воздействия, является актуальной задачей [3, 7].

Воздействие нарушителя на распределенную инфраструктуру объекта КИИ обусловлено инфраструктурными, коммуникационными особенностями организации каналов связи, предлагаемых оператором, на основе которых осуществляется организация взаимодействия между распределенными филиалами телекоммуникационных объектов КИИ (см. рисунок 1). Сетевые, транспортные и управляющие протоколы (Ethernet, ICMP, IP, TCP, UDP, SNMP) применяются в коммуникационных инфраструктурах для передачи данных, управления.

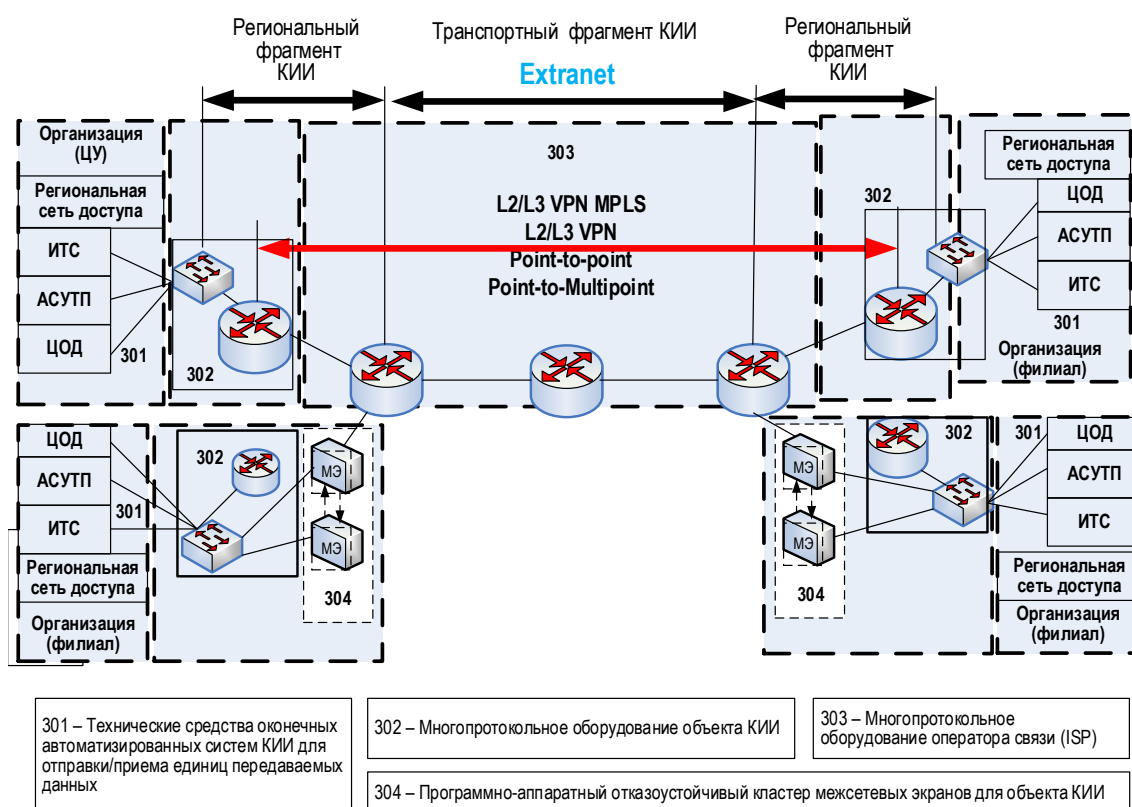


Рис. 1. Формирование распределенной инфраструктуры: для объектов ИС, АСУТП, ИТС КИИ

Fig. 1. Formation of Distributed Infrastructure: for Information System (IS), Automated Process Control Systems Information-Telecommunication System (ITS) of Critical Information Infrastructure (CII) Objects

¹ РосТелеком. Аналитический отчет об атаках на онлайн ресурсы компании за 2022 г. URL: https://rt-solar.ru/upload/iblock/34a/5w4h9e57axovdbv3ng7givrz271ykir3/Ataki-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf

² ТрансТелеКом. Аналитический отчет по сервису «Защита от DDoS-атак» 1 квартал 2023. URL: https://ttk.ru/upload/doc/business/ddos_1_2023.pdf

³ Бюллетени НКЦКИ: новые уязвимости ПО. URL: <https://safe-surf.ru/specialists/bulletins-nkcki>

Для выделенных протоколов помимо иерархических – коммуникационных особенностей – можно выделить конфигурационные компоненты формирования инфраструктур, которые также могут быть причиной снижения защищенности объекта (в связи с воздействием нарушителя, или некавалифицированными действиями персонала в распределенных фрагментах ИТС).

Очевидно, что логическая структура каналов связи для объектов КИИ имеет иерархическую особенность построения, обусловленную применением коммуникационных и конфигурационных параметров в КИИ рассматриваемых подсистем (ИС, АСУТП, ИТС), функционирующих в единой распределенной сети организации. Для моделирования и оценки защищенности таких подсистем, а также исследования свойств устойчивости [6, 8, 9], с учетом иерархических особенностей формирования объектов КИИ, предлагается применять совокупность имитационных и полунатурных моделей [7]. При этом отличительным признаком данного решения на основе имитационных моделей сетей Петри является учет не только иерархии построения объектов КИИ, но и их конфигурационных и коммуникационных особенностей функционирования, а также воздействия нарушителя как на логическую (коммуникационную и конфигурационную), так и на физическую составляющую объекта КИИ [9–12, 13, 18].

В сложившихся условиях при воздействии на коммуникационную инфраструктуру объекта КИИ, сетевых воздействиях нарушителя существующие методы оценки защищенности основаны на знании сигнатур угроз и сводятся к методам оценки защищенности на основе ранее известных угроз, например, баз данных угроз (БДУ) ФСТЭК [14–17], что представлено на рисунке 2.

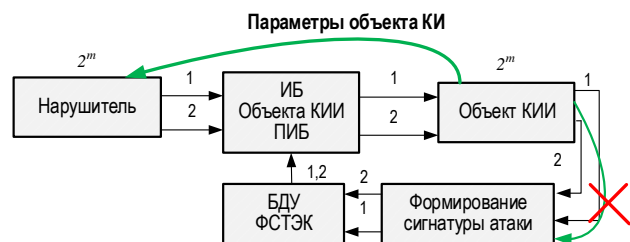


Рис. 2. Существующий подход к оценке защищенности объектов КИИ

Fig. 2. Existing Approach to Assessing the Security of Critical Information Infrastructure (CII) Facilities

В таких условиях нарушитель, работающий в известном пространстве состояний объекта КИИ, обладает сведениями о 2^m параметрах функционирования объекта КИИ. Эти же параметры являются основой для формирования воздействия нарушителя на объект КИИ. Такие возможности нарушителя позволяют изменять сигнатуры, формировать

новые, ранее не известные воздействия 1 и 2 (см. рисунок 2). При этом методы обеспечения защищенности объекта КИИ на основе сигнатурных средств всегда отстают по времени от воздействия нарушителя, что создает предпосылки нахождения объекта КИИ в незащищенных состояниях 1, 2 (см. рисунок 2).

Формирование сигнатур на основе существующих БД сигнатур методами машинного обучения является перспективным направлением, требовательным к исходным данным о состоянии объекта. Причем применение для этого знаний о параметрах функционирования самого объекта КИИ является ключевым фактором, учитываемым в разрабатываемых моделях. Решением сложившегося противоречия между многообразием воздействия нарушителя и существующими возможностями методов и средств обеспечения ИБ является учет параметров объекта КИИ в формировании его политики ИБ, обозначенной на рисунке 3 как ПИБ.

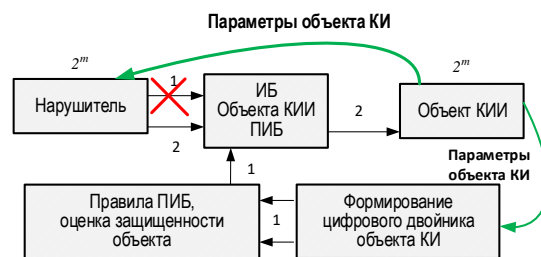


Рис. 3. Предлагаемый метод оценки защищенности объектов КИИ

Fig. 3. Proposed Method for Assessing the Security CII Facility

В основе предлагаемого метода оценки защищенности – разработанная на основе конфигурационных и коммуникационных параметров функционирования взаимосвязанная система имитационных моделей. Имитационные модели коммуникационной инфраструктуры позволяют формализовать в заданных правилах параметры коммуникационной инфраструктуры, политику ИБ, сформировать основанную на параметрах систему тестов для верификации политики ИБ. Предлагаемый метод позволяет получать параметрически точные модели коммуникационной инфраструктуры – цифрового двойника объекта КИИ, в динамике исследовать влияние на политику ИБ действий нарушителя. В основе цифрового двойника – имитационные модели на основе вложенных раскрашенных сетей Петри, верификация которых осуществляется полунатурными моделями. Комплекс моделей цифрового двойника включает в себя модель коммуникационной инфраструктуры объекта КИИ, модели каналов связи, комплекс взаимоувязанных моделей, связанных с формированием политики ИБ, анализом защищенности и действиями нарушителя [2].

Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

Моделирование многоуровневых коммуникационных инфраструктур связано с особенностями их построения (рисунок 4 из [7]). На основе анализа существующих методов моделирования и оценки защищенности [8, 9, 12, 15, 17, 19–23], а также сформулированных ранее предположений о необходимости учета параметров объекта КИИ [7], разработан метод моделирования иерархически сложных телекоммуникационных объектов и метод оценки защищенности объектов КИИ на основе конфигурационных и коммуникационных параметров функционирования объекта КИИ.

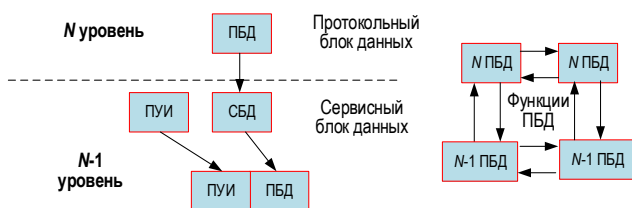


Рис. 4. Методы и способы взаимодействия протокольных блоков данных в соответствии с моделью OSI (7498), X.200 (ГОСТ Р ИСО/МЭК 7498-1-99)

Fig. 4. Methods and Ways of Interaction of PBDs in Accordance with the Following OSI Model (7498), X.200 (GOST R ISO/IEC 7498-1-99)

Основными особенностями, которые легли в основу универсальных масштабируемых модулей для имитационного и полунатурного моделирования, является внутриуровневое и межуровневое взаимодействие протокольных блоков данных, обозначенных на рисунке 4 как ПБД.

В связи с необходимостью моделировать множество протоколов, разработана концептуальная модель протокольного блока данных для реализации концепции вертикального и горизонтального взаимодействия протокольных блоков данных (рису-

нок 5), учитывающая наиболее важные подсистемы взаимодействия [7]. Для реализации разнотипных протокольных блоков данных, функционирующих в объектах КИИ, предлагается обобщенное концептуальное представление протокольного блока данных. В его основе – протокол с множеством параметров протокола π_l на l -м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, с множеством $\Theta_{l,\pi}$ – множество функциональных связей между алгоритмами $A_{l,\pi}$ в протоколе π_l на l -м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, $R_{l,\pi}$ – ресурсом на l -м уровне функционирования в коммуникационной инфраструктуре объекта КИИ, применяемым для функционирования протокола π_l коммуникационной инфраструктуры, множеством показателей качества обслуживания ($Qos_{l,\pi}$), характеризующих функциональное состояние коммуникационной инфраструктуры объекта КИИ. Для протокола π_l на l -м уровне функционирования входными / выходными параметрами являются $X_{l,\pi}$; формируется множество параметров политики информационной безопасности ($PIB_{l,\pi}$). Протокол имеет предварительно заданное множество параметров конфигураций ($CNF_{l,\pi}$). Для протокола, а также политики ИБ для протокола π_l l -го уровня предусмотрено множество параметров деструктивных воздействий ($VIB_{l,\pi}$) нарушителя на алгоритмы функционирующих в коммуникационной инфраструктуре объекта КИИ протоколов [8].

Предлагаемое обобщенное представление протокольных блоков данных позволяет объединять похожие по функциональному назначению элементы (алгоритмы работы протокола, ресурс протокола, его конфигурации, политику ИБ, воздействие нарушителя) для построения универсальных имитационных моделей на основе вложенных раскрашенных сетей Петри [7].

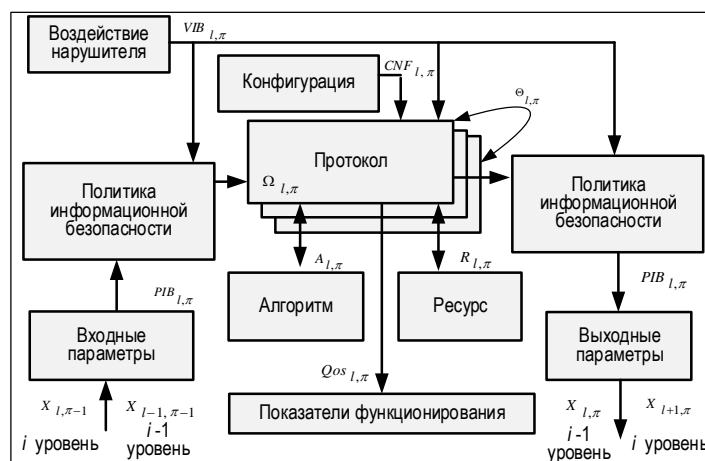


Рис. 5. Концептуальная модель протокольного блока данных

Fig. 5. Conceptual Model of the Protocol Data Unit (PDU)

Применение имитационного моделирования позволяет разработать универсальный метод построения блоков данных для различных типов протоколов, учесть коммуникационные и конфигурационные особенности их функционирования, осуществить перенос конфигурации с физического объекта в имитационные модели, являющиеся основой метода сквозного моделирования коммуникационной инфраструктуры объектов КИИ (рисунок 6).

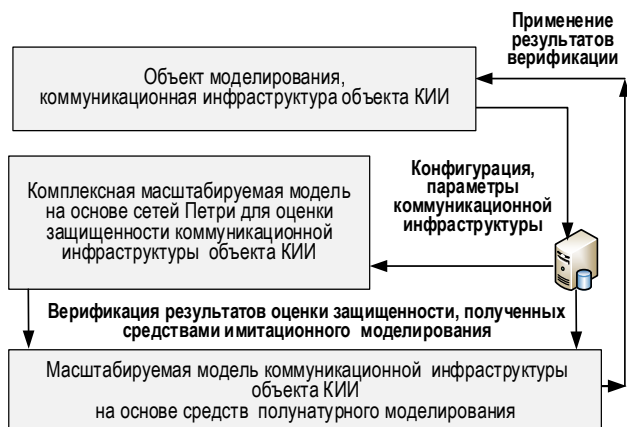


Рис. 6. Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

Fig. 6. End-to-End Modeling Method of CII Objects Based on Simulation and Semi-Natural Modeling

Суть предлагаемого метода заключается во взаимосвязи конфигураций (параметров) объекта КИИ с полунатурными и имитационными моделями, а также возможностями переноса конфигурации как с физического объекта на имитационные и

полунатурные модели, так и с имитационных и полунатурных моделей в физический объект. Представленная структурная взаимосвязь моделей в методе позволяет исследовать значимые свойства информационной безопасности физического объекта на имитационных и полунатурных моделях и переносить значимые результаты (оценки защищенности, результаты верификации политик ИБ), на физические объекты.

Объекты, представленные на рисунке 6, объединены единой логической составляющей – конфигурационными и коммуникационными параметрами. На физическом объекте эти параметры переносятся в полунатурные модели. Для применения в средствах имитационного моделирования необходимы дополнительные преобразования, позволяющие из разнообразных типов конфигураций получать параметры для имитационной модели. Основной задачей решаемой в методе моделирования коммуникационной инфраструктуры является получение универсальных масштабируемых имитационных и полунатурных моделей, пригодных для моделирования многоуровневых распределенных коммуникационных инфраструктур различных объектов КИИ. Структура комплекса имитационных моделей и возможные области их конфликтного взаимодействия для моделирования коммуникационной инфраструктуры объекта КИИ подсистем ИБ и действий нарушителя представлены на рисунке 7.

Пример реализации комплексной имитационной модели, учитывающей конфигурационные и коммуникационные параметры, методы обеспечения ИБ и воздействия нарушителя, представлен на рисунке 8.

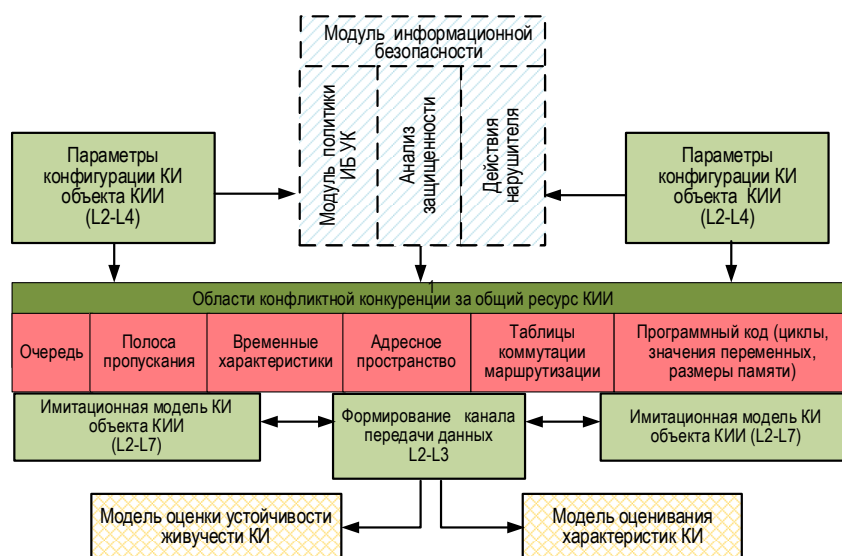


Рис. 7. Области конфликтного взаимодействия в модели оценки защищенности коммуникационной объекта КИИ

Fig. 7. Areas of Conflict Interaction in the Security Assessment Model of CII Communication Facility

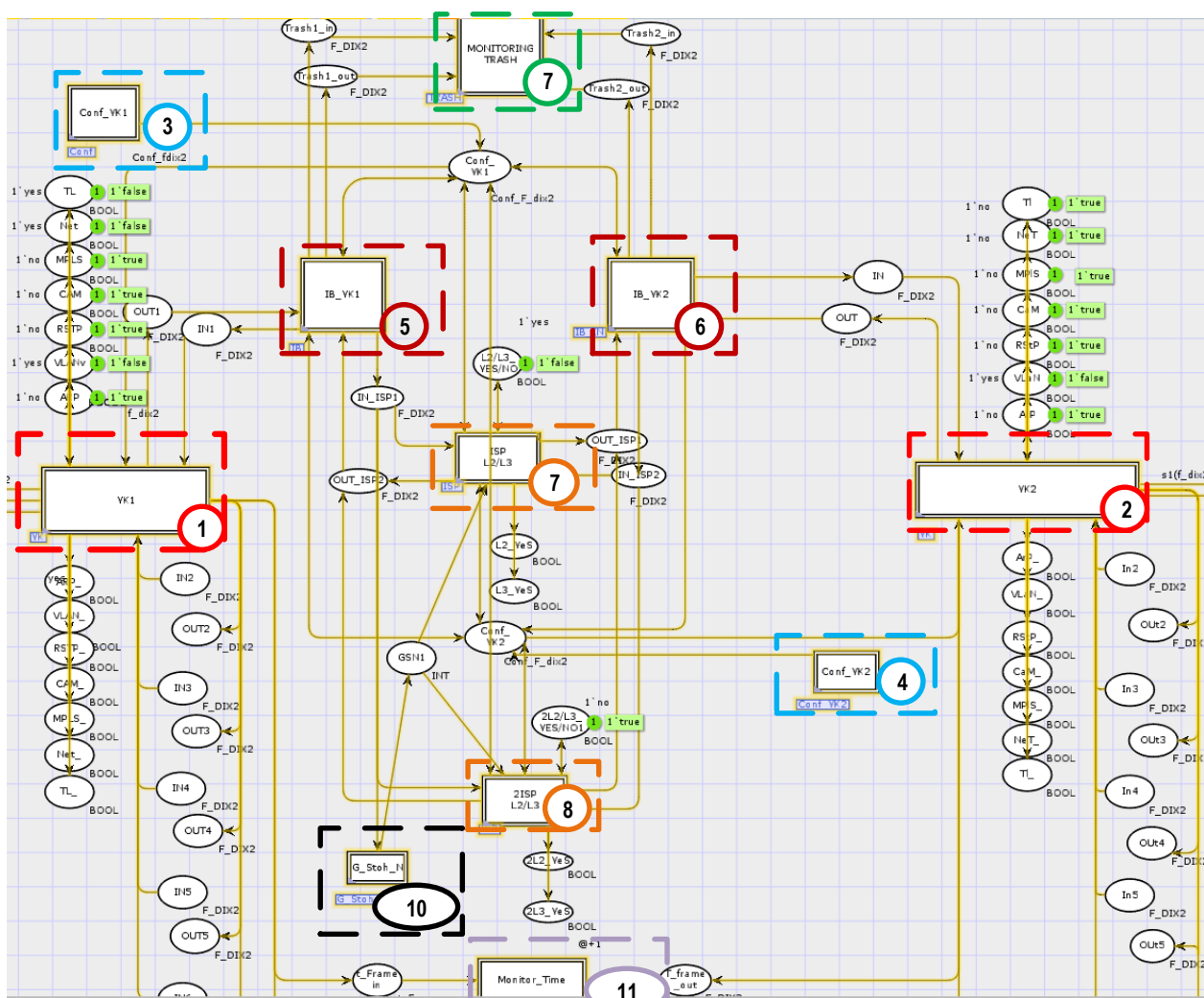


Рис. 8. Комплексная имитационная модель коммуникационной инфраструктуры с учетом функционирования методов и средств обеспечения ИБ, а также конфликтности взаимодействия

Fig. 8. Comprehensive Simulation Model of Communication Infrastructure Taking into Account the Functioning of Information Security Methods and Tools, and the Conflict of Interaction

Модель (см. рисунок 8) объединяет основные взаимодействующие субъекты, коммуникационную инфраструктуру, методы обеспечения ИБ, в том числе и воздействия нарушителя, что позволяет моделировать конфликтное поведение взаимодействующих субъектов. Имитационная модель позволяет исследовать влияние новых конфигураций, иерархических транспортных конструкций на защищенность объекта КИИ, проверять функциональность политики безопасности на потенциально возможные воздействия нарушителя, известные из БДУ ФСТЭК.

Основными составными элементами комплексной имитационной модели являются:

1, 2 – универсальные масштабируемые модели коммуникационной инфраструктуры объекта КИИ;
3, 4 – модели ввода конфигураций, коммуникационной инфраструктуры, задания сервисов;

5, 6 – универсальные масштабируемые модели ИБ для коммуникационной инфраструктуры объекта КИИ;

7 – результирующее множество регистрируемых угроз и их параметров для политики ИБ коммуникационной инфраструктуры объекта КИИ;

8, 9 – универсальные масштабируемые модели каналов оператора связи для коммуникационной инфраструктуры объекта КИИ;

10 – блок оценки устойчивости / живучести для коммуникационной инфраструктуры объекта КИИ;

11 – блок оценки характеристик устойчивости / живучести для коммуникационной инфраструктуры объекта КИИ.

Запуск имитационной модели осуществляется на основе конфигурационных данных, получаемых от физического объекта. Концепция построения функции конфигурации в имитационной модели представлен на рисунке 9.

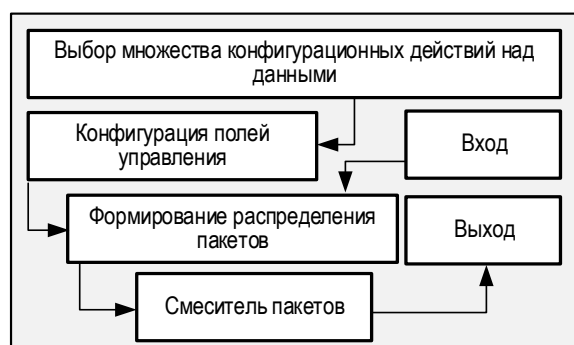


Рис. 9. Концепция построения функции конфигурации универсального протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 9. Building Concept the Configuration Function of the Universal Protocol Data Block of CII Communication Facility Object

На основе поступающих на вход протокольных блоков данных различного размера формируется детерминированные или стохастические посылки протокольных блоков данных, объединяемые в смесителе, после которого поступают на выход конфигурационного блока. Блок конфигурации имитационной модели представлен на рисунке 10, является основой для работы моделей узла коммутации, а также запуска модуля ИБ и расчета тестовых конструкций для проверки политики ИБ.

Коммуникационная инфраструктура объекта КИИ обладает иерархичностью, вложенностью в соответствии с моделью взаимодействия открытых систем OSI (7498), X.200 (ГОСТ Р ИСО/МЭК 7498-1-99). Для учета иерархических и вложенных протокольных конструкций объекта КИИ разработана структура и функционал модуля коммутации в имитационной модели, обладающего свойством масштабируемости (рисунок 11).

Формируя единый универсальный модуль коммутации на основе рисунка 11, появляется возможность формировать и наращивать функциональные свойства модуля имитационной модели, моделировать функционал сервера, рабочей станции, коммутатора, маршрутизатора, других объектов коммуникационной инфраструктуры объекта КИИ. Пример реализации модуля в имитационной модели представлен на рисунке 12. Такое решение дает возможность наращивать функционал единого модуля коммутации, применять его при моделировании различных наборов протоколов, изменяя его при необходимости.

Основным элементом имитационной модели является модуль обеспечения ИБ, концепция построения которого для входящего и исходящего информационного направления представлена на рисунке 13. Для входящего и исходящего направления структура блока обеспечения ИБ содержит:

- модуль приема конфигурации протокола в форме $|m|$ параметров коммуникационной инфраструктуры;

- модель формирования политики ИБ (ее формализация в виде команд имитационной модели);
- модуль анализа защищенности для политики безопасности на основе $2 \times |m|$ тестовых параметров;
- модуль формирования действий нарушителя политики безопасности коммуникационной инфраструктуры на основе $2 \times |m \pm \Delta|$ (методом стохастического случайного поиска в заданном пространстве состояний параметров $|m|$) (Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети: приказ ФСТЭК № 33 от 07.03.2024 г.).

Реализация представленной на рисунке 13 концепции построения модуля ИБ в имитационной модели на основе вложенных раскрашенных сетей Петри представлена на рисунке 14. Ключевым фактором является учет всех параметров $|m|$ коммуникационной инфраструктуры объекта КИИ, на основе которых осуществляется расчет тестовых комбинаций для анализа защищенности $2 \times |m|$, а также вторичная верификация в пространстве случайных состояний $2 \times |m \pm \Delta|$.

Предлагаемая структурно-функциональная схема построения блока обеспечения ИБ позволяет осуществлять оценку защищенности как для канала связи целиком, так и для каждого информационного направления, кроме того, – получать оценки защищенности как для входящего, так и исходящего направления. Имитационная модель позволяет формировать и детерминированные, и стохастические вектора атак, а также исследовать их влияние на политику ИБ объекта КИИ, исследовать известные угрозы из БДУ ФСТЭК и их влияние на политику ИБ.

Верификация политики ИБ множеством тестовых запросов в полунатурной модели коммуникационной инфраструктуры объекта КИИ, структура программно-аппаратного комплекса, представленного на рисунке 15, позволяет проверить работоспособность политики ИБ относительно тестов на основе параметров объекта – $|m|$.

С целью верификации политики ИБ формируется программно-аппаратный комплекс на основе полунатурных моделей, например, UNL/EVE или на основе средств виртуализации – операционных систем с открытым исходным кодом [24]. В полунатурную модель подключаются средства измерения, такие как программно-аппаратные датчики М-716, или программные средства измерения на основе программного средства iperf. Реализация тестовых протокольных конструкций осуществляется на основе программного средства Scapy, а также разработанного программно-аппаратного комплекса тестирования телекоммуникационного и оконечного оборудования объектов КИИ [25, 26].

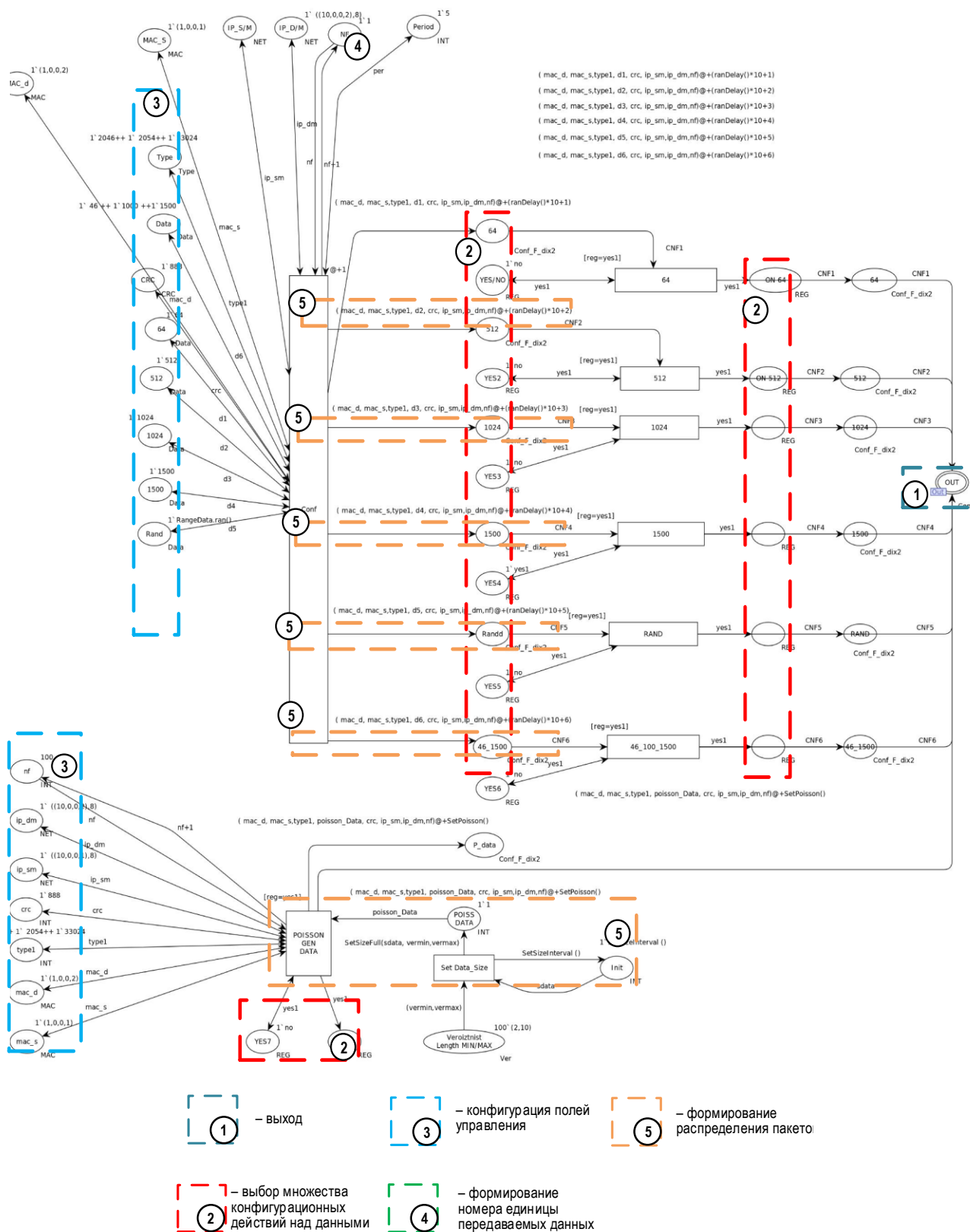


Рис. 10. Пример реализации функции конфигурации универсального протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 10. Example of Implementation of the Universal Protocol Data Block of CII Communication Facility Object

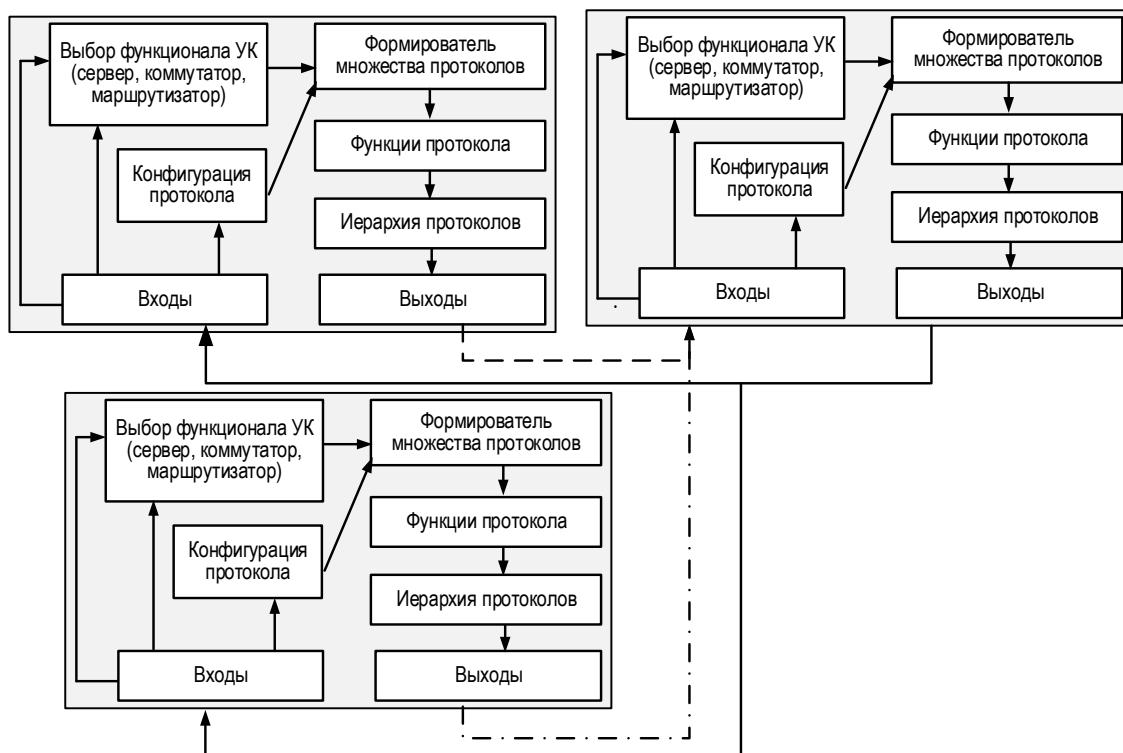


Рис. 11. Концепция иерархического построения горизонтальных и вертикальных связей протокольного блока данных коммуникационной инфраструктуры объекта КИИ

Fig. 11. Concept of Hierarchical Construction of Horizontal and Vertical Connections of Protocol Data Block of CII Communication Facility Object

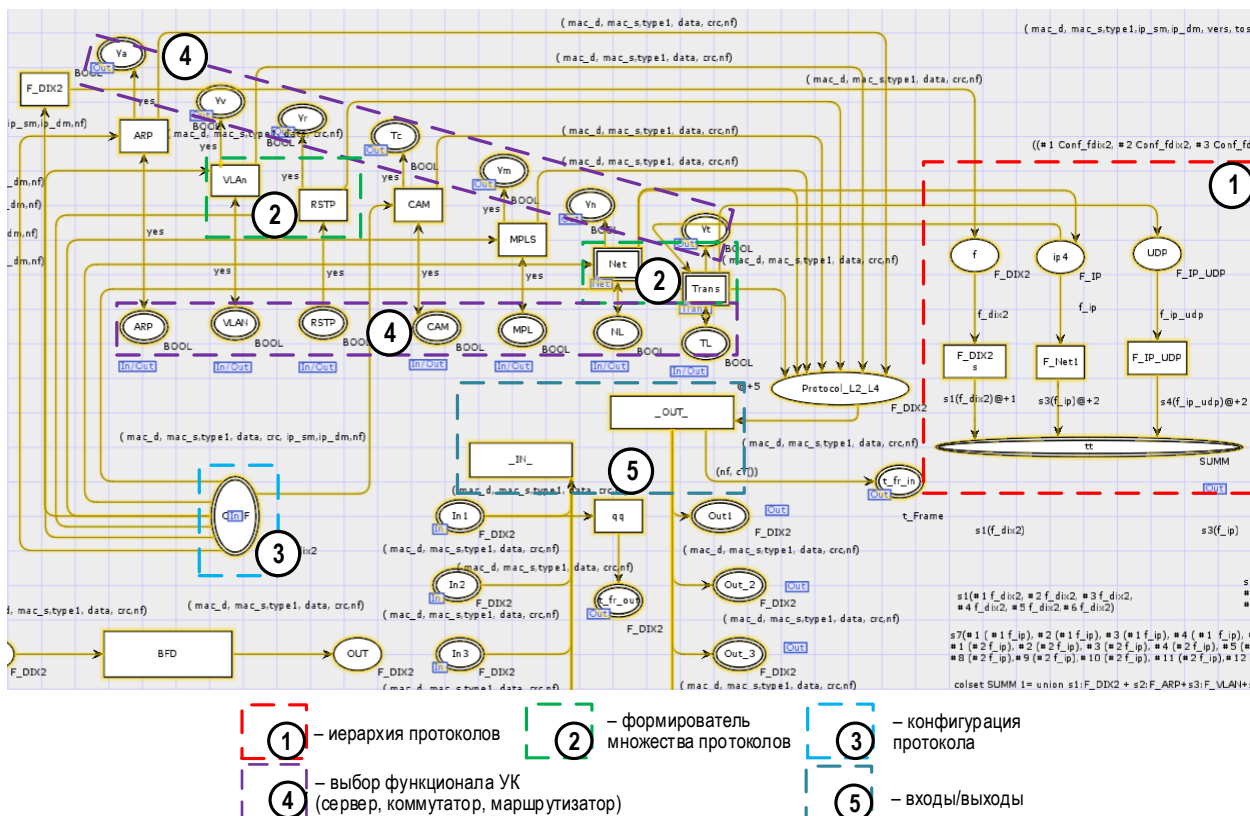


Рис. 12. Пример построения универсального протокольного блока данных для моделирования коммуникационной инфраструктуры объекта КИИ

Fig. 12. Example of Building a Universal Protocol Data Block for Modeling of CII Communication Facility Object

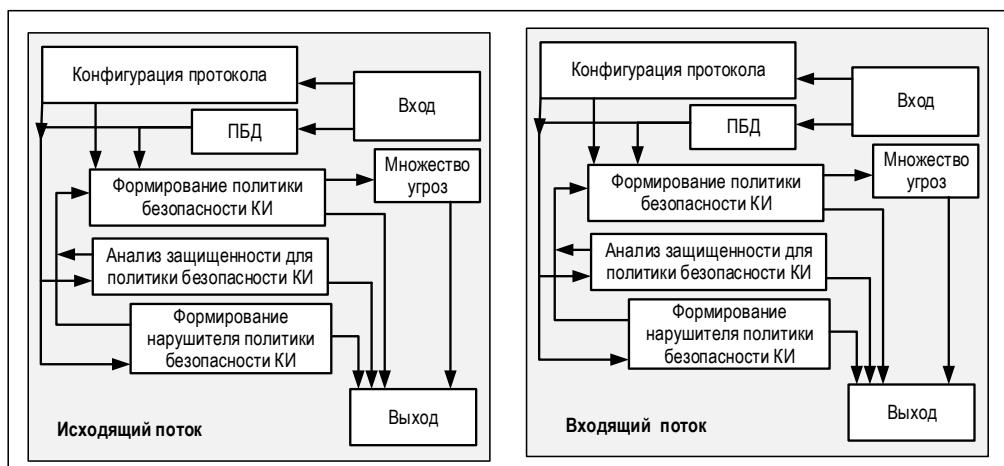


Рис. 13. Концепция построения модуля ИБ для моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в коммуникационной инфраструктуре объекта КИИ

Fig. 13. Concept of Building an Information Security Module for Modeling the Information Security Policy, Security Analysis, Formation of the Intruder Model in the CII Communication Facility

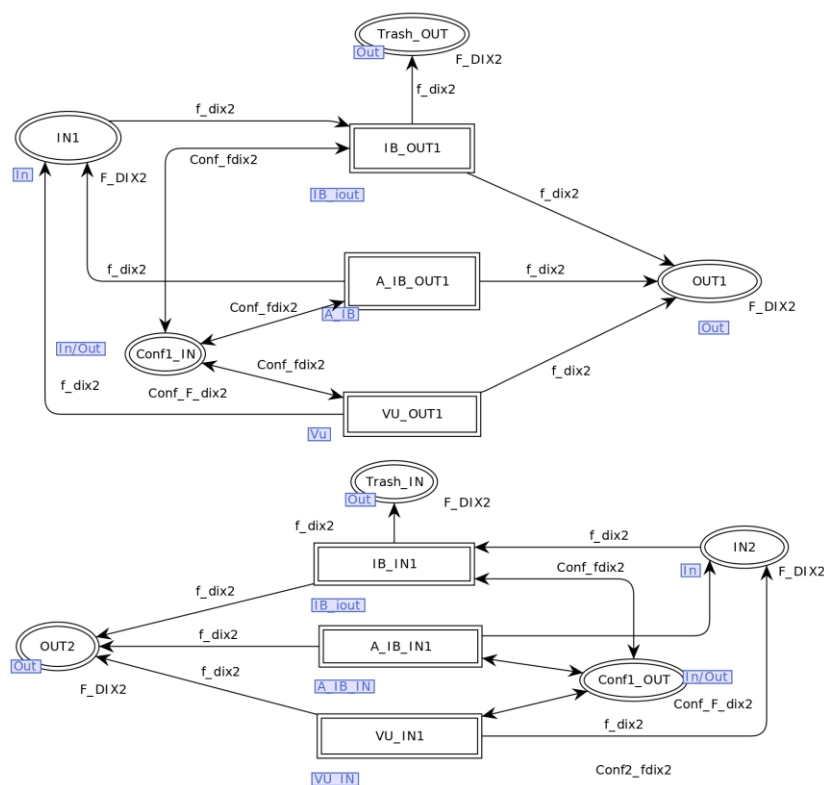


Рис. 14. Пример моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в коммуникационной инфраструктуре объекта КИИ на основе вложенных, раскрашенных сетей Петри для входящего и исходящего направления

Fig. 14. Example of Modeling of Information Security Policy, Security Analysis, and Formation of Intruder Model in the CII Communication Facility Object Based on Nested, Colored Petri Nets for Incoming and Outgoing Directions

Предлагаемый метод формирования моделей коммуникационной инфраструктуры, верификация результатов имитационного моделирования позволяет формировать параметрически точные модели, учитывающие существующие конфигурации коммуникационной инфраструктуры объекта

КИИ, параметры его политики ИБ, моделировать параметрическим способом действия нарушителя и исследовать влияние выделенных подсистем на защищенность объекта КИИ в динамике их взаимодействия. Верификация результатов имитационного моделирования предусмотрена полунатур-

ными моделями, аналитическими методами, сравнением функциональных характеристик (формирование и фильтрация протокольных блоков данных) с физическим объектом.

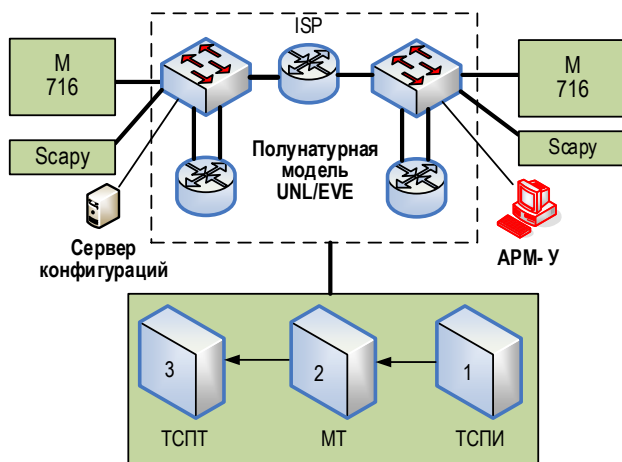


Рис. 15. Пример варианта программно-аппаратной реализации коммуникационной инфраструктуры в средствах полунатурного моделирования

Fig. 15. An Example of Variant of Software and Hardware Implementation of Communication Facility in Semi-Natural Modeling Tools

Заключение

Таким образом, предлагаемый метод моделирования коммуникационной инфраструктуры объектов КИИ (ИС, АСУТП, ИТС) на основе иерархических, раскрашенных сетей Петри позволяет расширить прикладной аспект теории ИБ в направлении развития методов моделирования: учета иерархичности и вложенности объектов проверяемой теорией гиперграфов и реализации этих принципов вложенными, раскрашенными сетями Петри. Моделирование на основе сетей Петри позволяет исследовать влияние протокольных особенностей построения рассматриваемых объектов КИИ (ИС, АСУТП, ИТС) на свойства устойчивости и доступности, и оценивать на основе этого их защищенность. Формирование параметрически точных моделей КИИ позволяет строить цифровые двойники объектов коммуникационной инфраструктуры и в динамике исследовать функционирование такого объекта с учетом изменения конфигурации, воздействия нарушителя, формирования физических или логических резервных направлений связи. Полученные результаты позволяют разрабатывать в том числе и количественные параметрически обоснованные показатели оценки защищенности объектов КИИ.

Список источников

1. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: учебное пособие для вузов. М.: Горячая линия – Телеком, 2011. 249 с.
2. Захватов М.А. Построение виртуальных частных сетей на базе технологии MPLS. М.: Изд-во Cisco Systems, 2001.
3. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия – Телеком, 2023. 500 с.
4. Петренко С.А. Киберустойчивость цифровой индустрии 4.0. СПб.: Издательский Дом «Афина», 2020. 256 с.
5. Петренко С.А. Управление киберустойчивостью: постановка задачи // Защита информации. Инсайд. 2019. № 3(87). С. 16–24. EDN:HNJVJNX
6. Штыркина А.А. Обеспечение устойчивости киберфизических систем на основе теории графов // Проблемы информационной безопасности. Компьютерные системы. 2021. № 2. С. 145–150. EDN:HACNAD
7. Бочков М.В., Васинев Д.А. Моделирование устойчивости критической информационной инфраструктуры на основе иерархических гиперсетей и сетей Петри // Вопросы кибербезопасности. 2024. № 1(59). С. 108–151. DOI:10.21681/2311-3456-2024-1-108-115. EDN:KWFIOY
8. Минаев М.В., Бондарь К.М., Дунин В.С. Моделирование киберустойчивости информационной инфраструктуры МВД России // Криминологический журнал. 2021. № 3. С. 123–128. DOI:10.24412/2687-0185-2021-3-123-128. EDN:EAKMQK
9. Осиленко А.А., Чирушкин К.А., Скоробогатов С.Ю., Жданова И.М., Корчевой П.П. Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей // Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281. DOI:10.24412/2071-6168-2023-2-274-281. EDN:VNGXMX
10. Ванг Л., Егорова Л.К., Мокряков А.В. Развитие теории Гиперграфов // Известия РАН. Теория и системы управления. 2018. № 1. С. 111–116. DOI:10.7868/S00023388180110. EDN:YSTDTE
11. Величко В.В., Попков В.К. Модели и методы повышения живучести современных систем связи. М.: Горячая линия – Телеком, 2017. 270 с.
12. Попков Г.В., Попков В.К. Математические основы моделирования сетей связи. М.: Горячая линия – Телеком, 2018. 182 с.
13. Колосок И.Н., Гурина Л.А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей // Вопросы кибербезопасности. 2021. № 6(46). С. 2–11. DOI:10.21681/2311-3456-2021-6-2-11. EDN:IJWNV
14. Гурина Л.А. Повышение киберустойчивости SCADA и WAMS при кибератаках на информационно-коммуникационную подсистему ЭЭС // Вопросы кибербезопасности. 2022. № 2(48). С. 18–26. DOI:10.21681/2311-3456-2022-2-18-26. EDN:QITQLA
15. Гурина Л.А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС // Вопросы

кибербезопасности. 2022. № 3(49). С. 23–31. DOI:10.21681/2311-3456-2022-3-23-31. EDN:SAPIYH

16. Чиркова Н.Е. Анализ существующих подходов к оценке киберустойчивости гетерогенных систем // Международная научно-практическая конференция «Техника и безопасность объектов уголовно-исполнительной системы» (Воронеж, Российская Федерация, 18–19 мая 2022 г.). Иваново: ИПК "ПресСто", Воронежский институт ФСИН России, 2022. С. 408–410. EDN:CPZRPV

17. Макаренко С.И. Динамическая модель системы связи в условиях функционально-разноразовного информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122–185. DOI:10.24411/2410-9916-2015-10307. EDN:UKSPAV

18. Бобров В.Н., Захарченко Р.И., Бухаров Е.О., Калач А.В. Системный анализ и обоснование выбора моделей обеспечения киберустойчивого функционирования объектов критической информационной инфраструктуры // Вестник Воронежского института ФСИН России. 2019. № 4. С. 31–43. EDN:DPJCN

19. Левшун Д.С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 105–115. DOI:10.31854/1813-324X-2023-9-1-105-115. EDN:QCZRIH

20. Костогрызов А.И., Нистратов А.А., Голосов П.Е. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 2. Моделирование с использованием «Черных ящиков» // Вопросы кибербезопасности. 2024. № 6(64). С. 2–27. DOI:10.21681/2311-3456-2024-6-2-27. EDN:ELOIDW

21. Язов Ю.К., Панфилов А.П. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз информационной безопасности // Вопросы кибербезопасности. 2024. № 2(60). С. 53–65. DOI:10.21681/2311-3456-2024-2-53-65. EDN:TEJAVM

22. Водопьянов А.С. Использование цифровых двойников с целью обеспечения информационной безопасности киберфизических систем // Вопросы кибербезопасности. 2024. № 4(62). С. 140–144. DOI:10.21681/2311-3456-2024-4-140-144. EDN:XTJILH

23. Скрыль С.В., Ицкова А.А., Ушаков К.Е. О возможности совершенствования процедур количественной оценки защищенности информации объектов критической информационной инфраструктуры от угроз несанкционированного доступа // Безопасность информационных технологий. 2024. Т. 31. № 3. С. 94–104. DOI:10.26583/bit.2024.204. EDN:CZFYR

24. Васинев Д.А. Применение операционных систем с открытым исходным кодом в коммуникационном оборудовании для сетей с коммутацией пакетов // Вопросы кибербезопасности. 2016. № 4(17). С. 36–44. DOI:10.21681/2311-3456-2016-4-36-44. EDN:XCMVAV

25. Васинев Д.А., Соловьев М.В. Предложения по построению универсального фаззера протоколов // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 59–67. DOI:10.31854/1813-324X-2023-9-6-59-67. EDN:AABMEE

26. Васинев Д.А., Бочков М.В., Кирьянов А.В., Андреев С.Ю., Полехин А.А., Сенотрусов И.А. и др. Способ и программно-аппаратный комплекс для оценки защищенности телекоммуникационного оконечного оборудования критической информационной инфраструктуры. Патент на изобретение № RU 2831928 C1. Оpubл. 16.12.2024.

References

1. Zapechnikov S.V., Miloslavskaya N.G., Tolstoj A.I. *Basics of Building Virtual Private Networks*. Moscow: Goryachaya liniya – Telekom Publ.; 2011. 249 p. (in Russ.)
2. Zahvatov M.A. *Building Virtual Private Networks Based on MPLS Technology*. Moscow: Cisco Systems Publ.; 2001. (in Russ.)
3. Zegzhda D.P. *Cybersecurity of the Digital Industry. Theory and Practice of Functional Resistance to Cyberattacks*. Moscow: Goryachaya liniya – Telekom Publ.; 2023. 500 p. (in Russ.)
4. Petrenko S.A. *Cyber Resilience of Digital Industry 4.0*. Saint Petersburg: Afina Publ.; 2020. 256 p. (in Russ.)
5. Petrenko S.A. Cyber Resilience Management: Problem Statement. *Zašita informacii. Inside*. 2019;3(87):16–24. (in Russ.) EDN:HHVJNX
6. Shtyrkina A.A. Cyber-Physical Systems Sustainability Based on Graph Theory. *Information Security Problems. Computer Systems*. 2021;2:145–150. (in Russ.) EDN:HACNAD
7. Bochkov M.V., Vasinev D.A. Modeling the Stability of Critical Information Infrastructure Based on Hierarchical Hypernets and Petri Nets. *Voprosy kiberbezopasnosti*. 2024;1(59):108–151. (in Russ.) DOI:10.21681/2311-3456-2024-1-108-115. EDN:KWFIOY
8. Minaev M.V., Bondar K.M., Dunin V.S. Modeling of Cyber Resilience Information Infrastructure of the Internal Affairs Ministry of Russia. *Kriminologicheskij zhurnal*. 2021;3:123–128. (in Russ.) DOI:10.24412/2687-0185-2021-3-123-128. EDN:EAKMQK
9. Osipenko A.A., Chirushkin K.A., Skorobogatov S.Yu., Zhdanova I.M., Korchevnoj P.P. Simulation of Computer Attacks on Software-Configured Networks Based on Stochastic Networks Transformation. *Izvestiya Tula State University. Technical Sciences*. 2023;2:274–281. (in Russ.) DOI:10.24412/2071-6168-2023-2-274-281. EDN:VNGXMX
10. Vang L., Egorova L.K., Mokryakov A.V. Development of Hypergraph Theory. *Journal of Computer and Systems Sciences International*. 2018;57(1):109–114. DOI:10.1134/S1064230718010136. EDN:XXVAJV
11. Velichko V.V., Popkov V.K. *Models and Methods for Increasing the Survivability of Modern Communication Systems*. Moscow: Goryachaya liniya – Telekom Publ.; 2017. 270 p. (in Russ.)
12. Popkov G.V., Popkov V.K. *Mathematical Foundations of Communication Network Modeling*. Moscow: Goryachaya liniya – Telekom Publ.; 2018. 182 p. (in Russ.)
13. Kolosok I.N., Gurina L.A. Assessment of Cyber Resilience Indices of Information Collection and Processing Systems in Electric Power Systems Based on Semi-Markov Models. *Voprosy kiberbezopasnosti*. 2021;6(46):2–11. (in Russ.) DOI:10.21681/

2311-3456-2021-6-2-11. EDN:IJWNV

14. Gurina L.A. Increasing Cyber Resilience of SCADA and WAMS in the Event of Cyber Attacks on the Information and Communication Subsystem of the Electric Power System. *Voprosy kiberbezopasnosti*. 2022;2(48):18–26. (in Russ.) DOI:10.21681/2311-3456-2022-2-18-26

15. Gurina L.A. Assessment of Cyber Resilience of Operational Dispatch Control System of EPS. *Voprosy kiberbezopasnosti*. 2022;3(49):23–31. (in Russ.) DOI:10.21681/2311-3456-2022-3-23-31. EDN:SAPIYH

16. Chirkova N.E. Analysis of Existing Approaches to Assessing the Cyber Resilience of Heterogeneous Systems. *Proceedings of the International Scientific and Practical Conference on Technology and Security of Penal System Facilities, 18–19 May 2022, Voronezh, Russian Federation*. Ivanovo: PressTo Publ.; Voronezh Institute of the Federal Penitentiary Service of Russia Publ.; 2022. p.408–410. (in Russ.) EDN:CPZRPV

17. Makarenko S.I. Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression. *Systems of Control, Communication and Security*. 2015;3:122–186. (in Russ.) DOI:10.24411/2410-9916-2015-10307. EDN:UKSPAV

18. Bobrov V.N., Zaharchenko R.I., Buharov E.O., Kalach A.V. System Analysis and Justification of Selection of Models for Ensuring Cyber-Stable Functioning of Critical Information Infrastructure Facilities. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*. 2019;4:31–43. (in Russ.) EDN:DPJJCN

19. Levshun D. Hierarchical Model for the Design of Microcontroller-Based Systems Protected from Cyber-Physical Attacks. *Proceedings of Telecommunication Universities*. 2023;9(1):105–115. (in Russ.) DOI:10.31854/1813-324X-2023-9-1-105-115. EDN:QCZRIH

20. Kostogryzov A.I., Nistratov A.A., Golosov P.E. Methodological Provisions on Probabilistic Prediction of Information Systems Operation Quality. Part 2. Modeling Using “Black Boxes”. *Voprosy kiberbezopasnosti*. 2024;6(64):2–27. (in Russ.) DOI:10.21681/2311-3456-2024-6-2-27. EDN:ELOIDW

21. Yazov Yu.K., Panfilov A.P. Composite Petri-Markov Networks With Special Construction Conditions for Modeling Information Security Threats. *Voprosy kiberbezopasnosti*. 2024;2(60):53–65. (in Russ.) DOI:10.21681/2311-3456-2024-2-53-65. EDN:TEJAVM

22. Vodopyanov A.S. Using Digital Twins to Ensuring Information Security of Cyberphysical Systems. *Voprosy kiberbezopasnosti*. 2024;4(62):140–144. (in Russ.) DOI:10.21681/2311-3456-2024-4-140-144. EDN:XTJILH

23. Skryl S.V., Iczkova A.A., Ushakov K.E. On the Possibility of Improving the Procedures for Quantifying Information Protection of Critical Information Infrastructure Objects from Threats of Unauthorized Access. *IT Security*. 2024;31(3):94–104. (in Russ.) DOI:10.26583/bit.2024.204. EDN:CZFY

24. Vasinev D.A. Application of Operating Systems with Open Source Code in of Communication Equipment for Networks with Commutation of Packages. *Voprosy kiberbezopasnosti*. 2016;4(17):36–44. (in Russ.) DOI:10.21681/2311-3456-2016-4-36-44. EDN:XCMVAV

25. Vasinev D., Solovov M. Proposals for Universal Protocol Fuzzer Construction. *Proceedings of Telecommunication Universities*. 2023;9(6):59–67. (in Russ.) DOI:10.31854/1813-324X-2023-9-6-59-67. EDN:AABMEE

26. Vasinev D.A., Bochkov M.V., Kirianov A.V., Andreev S.Iu., Polekhin A.A., Senotrusov I.A., et al. *Method and Software and Hardware System for Assessing Security of Telecommunication and Terminal Equipment of Critical Information Infrastructure*. Patent RF, no. 2831928 C1, 16.12.2024. (in Russ.)


Статья поступила в редакцию 24.12.2024; одобрена после рецензирования 12.02.2025; принята к публикации 20.02.2025.

The article was submitted 24.12.2024 approved after reviewing 12.02.2025; accepted for publication 20.02.2025.

Информация об авторе:

ВАСИНЕВ
Дмитрий Александрович

кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации

 <https://orcid.org/0009-0004-7030-5421>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.