МОДЕЛИРОВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ИЕРАРХИЧЕСКИХ ГИПЕРСЕТЕЙ И СЕТЕЙ ПЕТРИ

Бочков М. В.[1], Васинев Д. А.[2],

DOI: 10.21681/2311-3456-2024-1-108-115

Цель исследования: *моделирование объектов критической информационной инфраструктуры (КИИ) на основе математического аппарата гиперсетей и сетей Петри.*

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

Результат исследования: *предлагаемый способ построения математических моделей позволяет разработать параметрический точные имитационные модели для исследования свойств защищенности и устойчивости объектов КИИ, моделировать воздействия на них компьютерных атак (КА). В частности, предлагаемый способ имитационного моделирования позволяет учитывать конфигурационные и коммуникационные особенности построения и функционирования, динамику воздействия нарушителя на объекты КИИ, существующую политику безопасности, моделирование функциональных и структурных свойств устойчивости, исследования степени влияния этих элементов на защищенность объекта КИИ. Это обеспечивает возможность осуществлять оценку защищенности, обеспечение ИБ объектов КИИ с учетом конфигурационных и коммуникационных параметров объекта КИИ, уменьшить зависимость от экспертных оценок.*

Научная новизна: *заключается в развитии теории информационной безопасности в области оценки защищенности с учетом устойчивости и живучести объектов КИИ на основе математического аппарата иерархический гиперсетей, сетей Петри.*

Практическая ценность *заключается в получении параметрически точных моделей объекта КИИ. Возможности получения оценок защищенности на основании коммуникационных, инфраструктурных параметров самого объекта. Моделировании известных воздействий из банка данных угроз безопасности для проверки политики безопасности объекта КИИ в полученной модели. Моделировании воздействия на объект КИИ неизвестных ранее угроз.*

Ключевые слова: *информационная безопасность, коммуникационная инфраструктура, конфигурационная инфраструктура, моделирование математическое, моделирование имитационное, оценка защищенности, устойчивость, протокольные блоки данных.*

MODELING THE STABILITY OF CRITICAL INFORMATION INFRASTRUCTURE BASED ON HIERARCHICAL HYPERNETS AND PETRI NETS

Bochkov M. V.[3], Vasinev D. A.[4]

Research objective: *modeling of critical information infrastructure (CII) objects based on the mathematical apparatus of hypernets and Petri nets. The proposed method of building mathematical models allows to develop parametric accurate simulation models to study the properties of security and stability of CII objects, to simulate the impact of computer attacks (CA) on them.*

Research methods: *mathematical methods of systems theory and systems analysis methods of graph theory, methods of simulation modeling.*

Research result: *the proposed method of simulation modeling allows to take into account the configuration and communication features of construction and operation, the dynamics of the impact of the intruder on CII*

1 Бочков Максим Вадимович, доктор технических наук, профессор, ЧОУ ДПО «Центр предпринимательских рисков», г. Санкт-Петербург, Россия. E-mail: mvboch@cprspb.ru

2 Васинев Дмитрий Александрович, кандидат технических наук, сотрудник Академии ФСО России, г. Орёл, Россия. E mail: vda33@academ.msk.rsnet.ru

3 Maxim V. Bochkov, Dr. Sc., Professor, Center for entrepreneurial risks, Saint Petersburg, Russia. E mail: mvboch@yandex.ru

4 Dmitriy A. Vasinev, Ph.D., employee Academy FSO Russia, Orel, Russia. E mail: vda33@academ.msk.rsnet.ru

objects, the existing security policy, modeling of functional and structural properties of stability, research into the degree of influence of these elements on the security of the CII object. This makes it possible to assess the security, to ensure the IS of CII objects taking into account the configuration and communication parameters of the CII object, to reduce the dependence on expert assessments.

Keywords: *information security, communication infrastructure, configuration infrastructure, mathematical modeling, simulation modeling, hypernets, security assessment, stability, protocol data blocks.*

Введение

Актуальность вопросов обеспечения информационной безопасности для информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления (АСУТП) критических информационных инфраструктур (КИИ), функционирующих в критически важных отраслях деятельности государства в медицине, образовании, промышленности, энергетике поясняется отраслевой принадлежностью объектов атак, что говорит о продолжающемся информационном противоборстве. 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 КИИ [5,6,7].

В качестве составных элементов КИИ выступают распределенные фрагменты сетей, центры обработки данных (ЦОД), автоматизированные системы управления (АСУТП) объединенные в единую распределенную ИТС организации. Пример обобщённого представления распределенной КИИ представлен на рис. 1. Существующие особенности построения коммуникационной инфраструктуры технологически достаточно разнообразны, однако общими требованиями являются: применение технологий виртуальных частных сетей (VPN), резервирования, отказоустойчивости, обеспечение устойчивости в условиях воздействия компьютерных атак (КА)[8,9]. 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 исследования в области оценки защищенности и устойчивости КИИ в условиях воздействия на нее КА является актуальной задачей.

Воздействие нарушителя на распределенную ИТС, обусловлено инфраструктурными, коммуникационными особенностями организации каналов

5 РосТелекомм. Аналитический отчет об атаках на онлайн ресурсы компании за 2022г. [сайт]. URL:https:// https://rt-solar.ru/upload/iblock/34a/5w4h9o57axovdbv3ng7givrz271ykir3/Ataki-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf.

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

7 Бюллетени НКЦКИ: новые уязвимости ПО [сайт]. URL: https://safe-surf.ru/specialists/bulletins-nkcki/.

8 Запечников, С. В. Основы построения виртуальных частных сетей: учебное пособие для вузов/ Запечников, С.В., Милославская, Н. Г., Толстой, А. И. – 2-е изд. Москва: Горячая линия-Телеком, 2011, – 249. – ISBN 5-85582-119

9 Захватов, М. А. Построение виртуальных частных сетей на базе технологии MPLS / М. А. Захватов. – Москва: изд-во Cisco Systems, 2001 г.

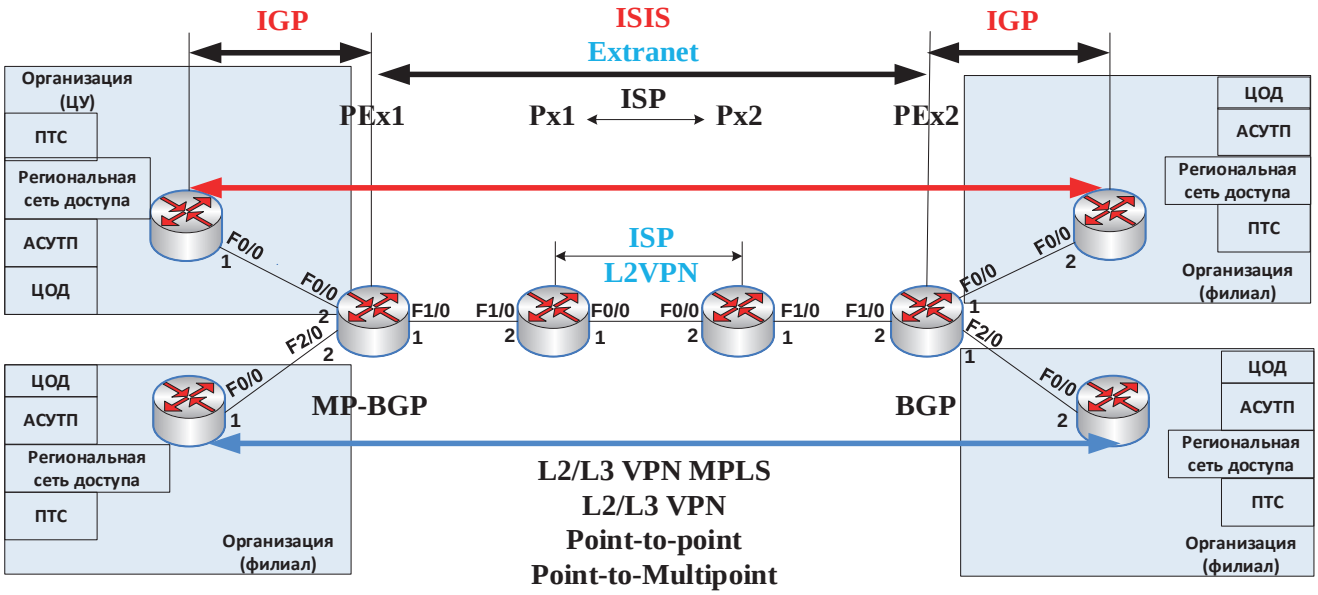

Рис. 1. Формирование распределенной инфраструктуры для объектов ИС, АСУТП, ИТС КИИ

связи, предлагаемых оператором связи, на основе которого осуществляется организация взаимодействия между распределенными филиалами телекоммуникационных объектов КИИ, представлено на рис. 2. Сетевые, транспортные и управляющие протоколы, которые применяются в коммуникационных инфраструктурах для передачи данных, управления, такие как (Ethernet, ICMP, IP, TCP, SNMP, Modbus, MMS, Goose). 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 неквалифицированных действий персонала в распределенных фрагментах ИТС.

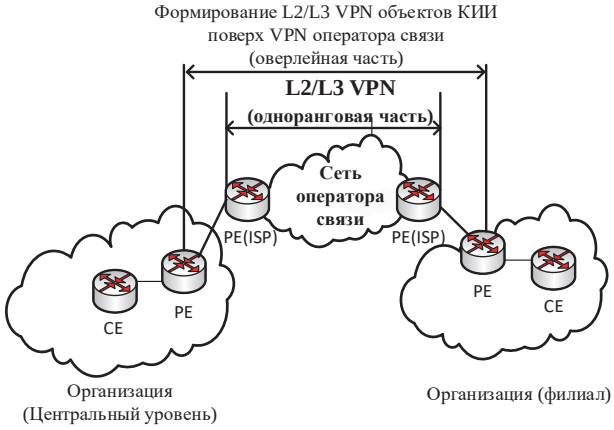

Рис. 2. Формирование распределенной инфраструктуры для ИС, АСУТП, ИТС

В настоящее время при обеспечении информационной безопасности (ИБ) объектов КИИ наряду со свойствами целостности, доступности, конфиденциальности, формируется понятие устойчивости КИ. Так, например, в нормативных документах[10,11,12] и известных исследованиях в области ИБ ряд авторов рассматривает свойство устойчивости объектов коммуникационной инфраструктуры от компьютерных атак [1–3] как свойство защищенности объекта, связанное с его способностью противостоять КА.

Решение задачи устойчивости функционирования КИИ в работах [1–3] связывается с возможностями противостоять компьютерным атакам методом резервирования на структурном – физическом уровне, как например в [4], на основе вероятностного расчета риска и нечетких множеств [5], вероятностных и Марковских методов оценки защищенности в работе [6]. Анализ вариантов оценок киберустойчивости объектов КИИ, представленные в работах [7–9], показывает, что в оценках киберустойчивости авторы применяют вероятностные методы, теорию нечетких множеств [7], основываются на экспертном методе при формировании алгоритмов оценки киберустойчивости в работе [8]. Авторы [9] предлагают применять описательные и концептуальные модели динамики обеспечения киберустойчивости объекта КИИ. Таким образом, при оценках киберустойчивости выделенные методы теории рисков, теории вероятностей, нечетких множеств, экспертные методы не учитывают иерархические и параметрические особенности построения и функционирования объектов КИИ, а также иерархические и параметрические особенности воздействия нарушителя. Как при оценке защищенности, так и при оценках киберустойчивости применяют обобщенные или абстрактные показатели, характеризующие защищённость, осуществляют свертку таких показателей в обобщенный показатель, характеризующий защищенность объекта. В рамках исследования делается предположение о возможностях получения оценок защищенности на основе иерархических особенностей построения объекта КИИ, параметров ее конфигурации, параметров воздействия нарушителя. На основе выделенных параметрических особенностей предлагается способ обеспечения устойчивости объектов КИИ при противодействии КА в логических каналах методом динамического изменения характеристик функционирования, что соответствует функциональному варианту обеспечения устойчивости. Примером логического резервирования могут быть параметры самого логического канала, типы применяемых виртуальных частных сетей (VPN), топология соединения, маршрутная информация, скорость передачи, качество обслуживания. Все это связано с технологическими особенностями построения, применимыми технологиями, иерархическими особенностями построения КИИ, вариант которой представлен на рис. 3.

Технологические особенности связаны с применением различных вариантов туннелирования (L2, L3 VPN), при формировании распределенной ИТС, а также с применением как физически зарезервированных каналов, так и логического резервирования на основе следующих технологий и протоколов (Rapid spanning tree protocol (RSTP), Virtual router redundancy protocol (VRRP), Bidirectional forwarding detection (BFD), Routing, MPLS Fast reroute FastRR) [6, 7].

10 Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03 февраля 2012 г., № 803). Режим доступа: https://fstec.ru/component/attachments/download/1906.

11 О безопасности Критической информационной инфраструктуры Российской Федерации: Федеральный закон ред. от. 19.07.2017г. №187 // ФСТЭК: [сайт]. – URL: https://fstec.ru/component/attachments/download/1906/.

12 Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России № 239 от 25.12.2017 // ФСТЭК: [сайт]. – URL: https://fstec.ru/dokumenty/vse-okumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239/.

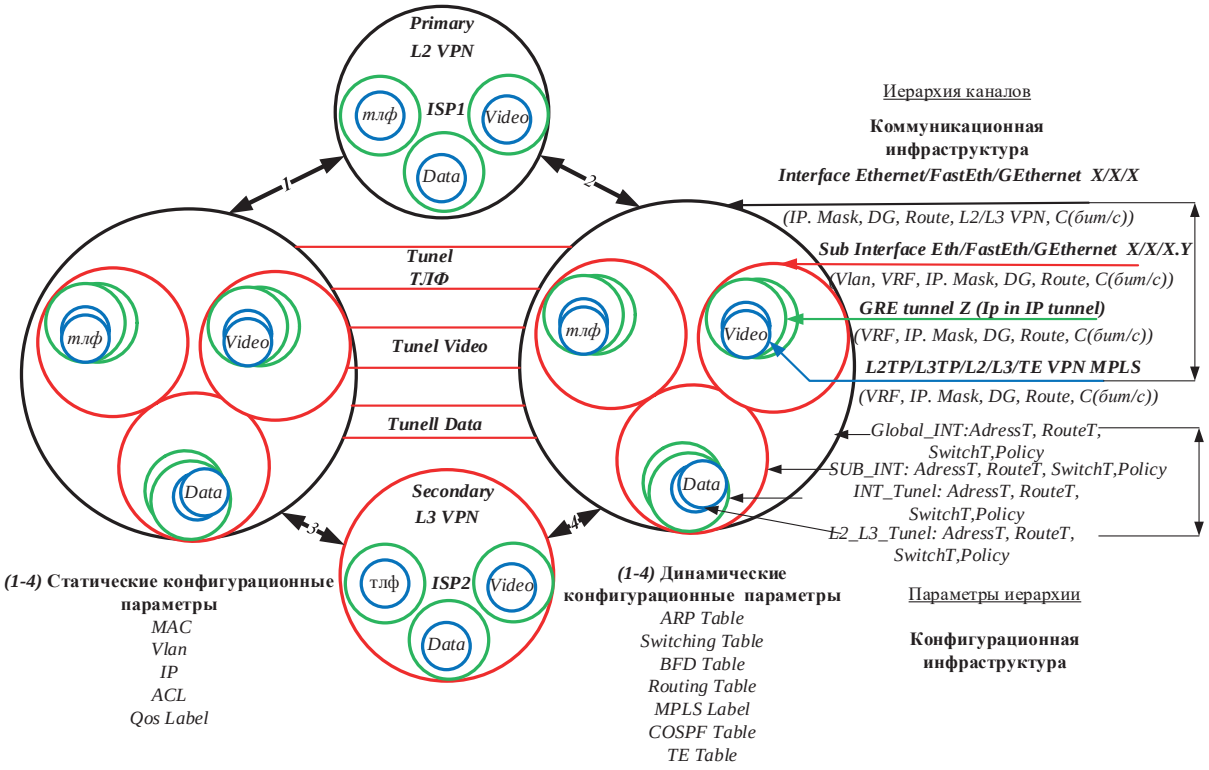

Рис.3. Вариант иерархической, вложенной коммуникационной инфраструктуры для моделирования распределенной инфраструктуры ИС, АСУТП, ИТС, объектов КИИ

Очевидно, что логическая структура каналов связи для КИИ имеет иерархическую особенность построения, обусловленную применением коммуникационных и конфигурационных параметров в КИИ рассматриваемых объектов (ИС, АСУТП, ИТС), функционирующих в единой распределенной сети организации.

Для оценки защищенности объектов (ИС, АСУТП, ИТС) а также исследования свойств устойчивости, с учетом иерархических особенностей КИИ предлагается применять математические модели основаны на теории гиперграфов[13] и [12]. При этом отличительная особенность предлагаемого решения на основе гиперграфов является учет не только иерархических особенностей построения объектов КИИ, но и их конфигурационных и коммуникационных особенностей функционирования, а также воздействий нарушителя как на логическую (коммуникационную и конфигурационную), так и на физическую составляющую объекта КИИ.

Моделирование объектов критической информационной инфраструктуры

Моделированию устойчивости объектов КИИ посвящены работы [10,11], однако не учитываются параметрические особенности моделирования протокольных единиц данных, иерархические особенности их построения и функционирования. Математическая модель на основе иерархических гиперграфов, позволяет наиболее полно отразить характеристики моделируемого объекта, связанные с иерархичностью и вложенностью протекающих процессов[14,15] и [12–14]. Развитие теории гиперграфов в области информационной безопасности связано с оценкой защищенности АСУТП на основе наиболее вероятной угрозы [15]. Предлагаемое решение заключается в учете конфигурационных и коммуникационных возможностей, а также конфликтности, связанной с воздействием нарушителя на выделенные структурные элементы КИИ в гиперграфе.

Математическая модель КИИ, учитывающая иерархические, вложенные инфраструктурные, конфигурационные компоненты, на основе теории s-гиперсетей представлена выражением (1)

$$H = (G_0, G_1, \ldots, G_m, G_{ИБ}, G_V), \quad (1)$$

где: G_0 – граф первичной физическая топология; $G_{1\ldots m}$ – графы инфраструктурных компонентов (технологий, протоколов, виртуальных туннелей), конфигураций;

13 Зыков А. А. Гиперграфы / Успехи математических наук, 11974. Т.9, выпуск 6, 89–154 // Общероссийский математический портал Math-Net.Ru [сайт] – URL:https://www.mathnet.ru/links/6ebfd77a48733caf850ac105bc7eaac6/rm4449.pdf.

14 Конин М. В. Применение S–гиперсетей для автоматизированного проектирования инженерной инфраструктуры предприятия /М. В. Конин, Э. Ю. Лепнер, Г. В. Попков / Информационные технологии в системах автоматизации. 2013. – №5 (24). [сайт]. – URL: https://www.elibrary.ru/download/elibrary_28906854_84188973.pdf

15 Лепнер Э. Ю. Разработка операций над S-гиперсетями: дис. на соиск. учен. магистра / Лепнер Эдуард Юрьевич: Новосибирский национальный исследовательский государственный университет. – Новосибирск – 2013: [сайт]. – URL: https://www.elibrary.ru/download/elibrary_28906854_84188973.pdf.

$G_{ИБ}$ – гиперграф политик информационной безопасности; G_V – гиперграф воздействия нарушителя.

На основании анализа работ по теории s-гиперсетей [12,13] и [12–15], а также руководствуясь возможностями математического моделирования на основе теории иерархических s-гиперсетей установлено, что исследование на таких моделях динамики функционирования объекта КИИ, а также конфигурация s-гиперсетей и исследования защищенности, моделирование динамики воздействия нарушителя имеет ограничения, связанные со сложностью задания выделенных объектов динамическими матрицами смежности или инцидентности, а также динамического преобразования исходного гиперграфа к необходимому виду.

Для устранения выделенных недостатков на данном этапе работы осуществлялось применение функционального аппарата раскрашенных вложенных сетей Петри, позволяющего моделировать и исследовать динамику функционирования КИИ (изменчивость гиперграфа в различных условиях). Примерами динамики изменения гиперграфа могут быть воздействия нарушителя, связанные с изменением коммуникационной и конфигурационной компонент гиперграфа, в условиях функционирования как объекта КИИ, так средств обеспечения ИБ (существующих политик ИБ), которые учтены в модели, представленной выражением (2)

$$S = (\{P_Д, P_{ИБ}, P_V\},\{T_Д, T_{ИБ}, T_V\},\{E_Д, E_{ИБ}, E_V\}, M_0), \quad (2)$$

где $P_Д$ – конечное множество допустимых позиций КИИ УК; $P_{ИБ}$ – конечное множество позиций политик ИБ; P_V – конечное множество воздействий нарушителя; $T_Д$ – конечное множество допустимых переходов (событий); $T_{ИБ}$ – конечное множество переходов (событий) политик информационной безопасности; T_V – конечное множество воздействий нарушителя; $E_Д$ – конечное множество дуг допустимых переходов (событий); $E_{ИБ}$ – конечное множество дуг событий политик ИБ; E_V – конечное множество дуг событий воздействия нарушителя; M_0 – начальное состояние сети.

Пример моделирования объектов коммуникационной инфраструктуры иерархическими s-гиперсетями представлен на рис. 4–8. Диаграмма вложений протоколов формирующих КИИ гиперграфов в s-гиперсети для ИТС КИИ представлена на рис. 4. Гиперграф первичной сети рис. 4, формирует первичную топологию ИТС КИИ с ее основными коммуникационными элементами – узлами, физическими каналами связи – ребрами гиперграфа.

Графы второго и последующих уровней вложения (рис. 5–8) определяются вершинами и рёбрами, участвующими во взаимодействии протоколов соответствующего уровня.

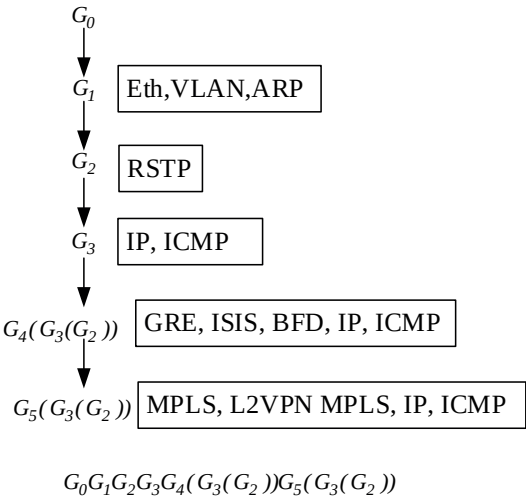

Рис. 4. Диаграмма вложений гиперграфов в s-гиперсети

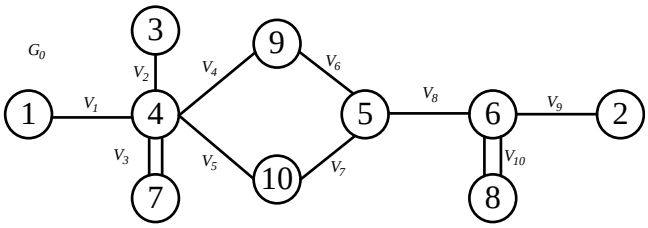

Рис. 5. Топология первичного графа G0 для ИТС объекта КИИ

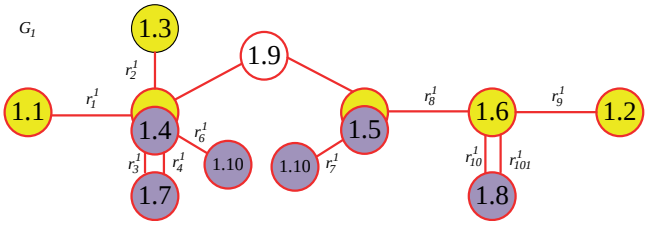

Рис. 6. Топология графа G1 (VLAN, ARP) для КИИ

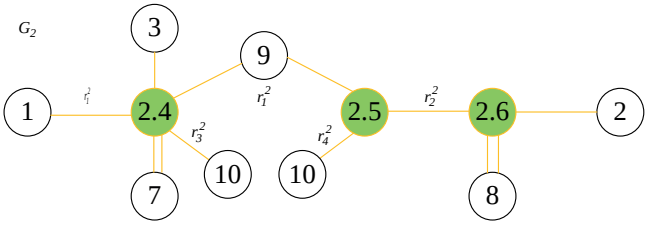

Рис. 7. Топология графа G2 (RSTP) для КИИ

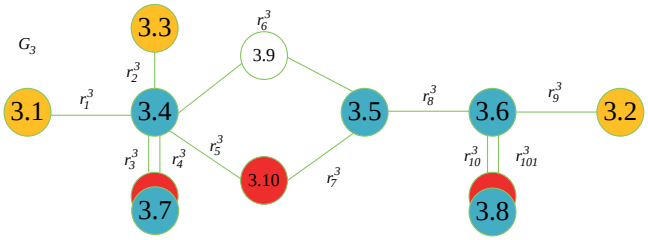

Рис. 8. Топология графа G3 (IP, ICMP) для КИИ

На рис. 4 представлена первичная топология – G0 объекта КИИ, узлы: 1, 2, 3 – оконечное оборудование (автоматизированные системы, АСУТП);

4, 5, 6 – коммутационное оборудование класса L2; 7, 8 маршрутизирующее оборудование L3; 9, 10 – оборудование L2, L3; оператора связи.

Вершины гиперграфа в сети Петри – это протокольные блоки данных, функционирующие на различных уровнях модели взаимодействия открытых систем (рис. 9–10), обладающие строго формализованными функциональными свойствами. При этом основная причина выбора имитационного моделирования заключается в сложности процесса формирования протокольного блока данных, взаимосвязи его с другими иерархическими элементами, размерности параметрического пространства состояний, что усложняет на данном этапе работы применение s-гиперсетей. Переход от гиперграфового подхода к формированию узлов графа в виде матриц смежности или инцидентности – к заданию вершин гиперграфа протокольными блоками данных в сети Петри, позволяет устранить выявленные на данном этапе работы недостатки в области масштабирования моделей, динамики смены состояний параллельных и асинхронных процессов, которые характерны для ИС, АСУТП, ИТС объектов КИИ.

Имитационное моделирование позволяет разработать универсальные способы построения имитационных протокольных блоков данных, для различных типов протоколов, учесть коммуникационные и конфигурационные особенности их функционирования (рис. 9–10).

Примеры моделирования вариантов конструкций протокольных блоков данных и особенностей их объединения, представлены на рис. 11–14.

Способ формирование кадров различной структуры параметрически полно отражающих существующие коммуникационные особенности объектов КИИ в процессе отправки, получения, обработки, представлен на рис. 11.

Учет полноты моделируемых параметров, позволяет сформировать многообразие пространства состояний протокольных блоков данных, что с одной стороны усложняет решение задачи оценки защищенности, а с другой позволяет задать точнее ограничения на пространстве состояний, учесть динамику воздействия нарушителя, проверять работоспособность политики безопасности.

Пример объединения различных типов кадров (кадр Ethernet, arp – запрос, arp – ответ) в едином канале обработки данных представлен на рис. 12, а демультиплексирования кадров – выбора из единого канала кадров заданного формата для дальнейшей их обработки на рис. 13.

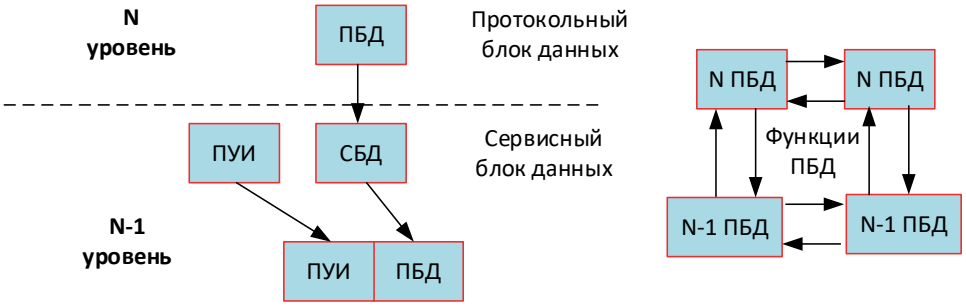

Рис. 9. Методы, способы взаимодействия ПБД в соответствии с моделью OSI (7498), X.200, ГОСТ Р ИСО/МЭК 7498-1-99

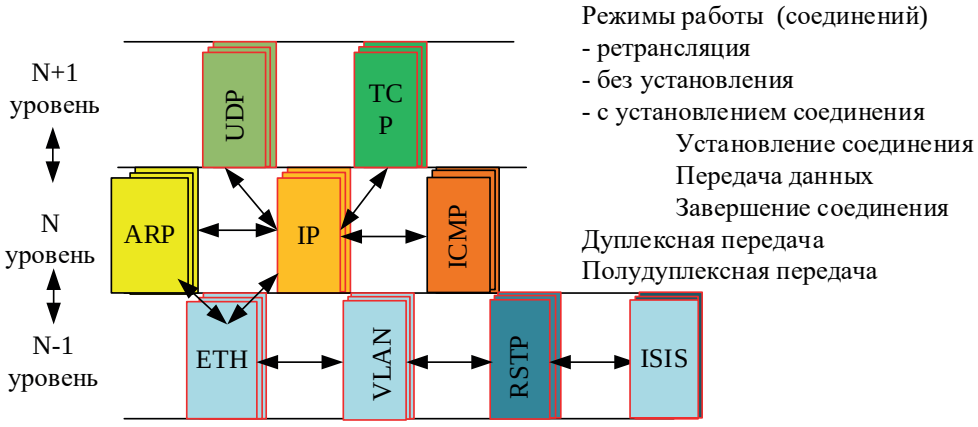

Рис.10. Вариант взаимодействия объектов различных уровней в соответствии с моделью OSI (7498), X.200, ГОСТ Р ИСО/МЭК 7498-1-99

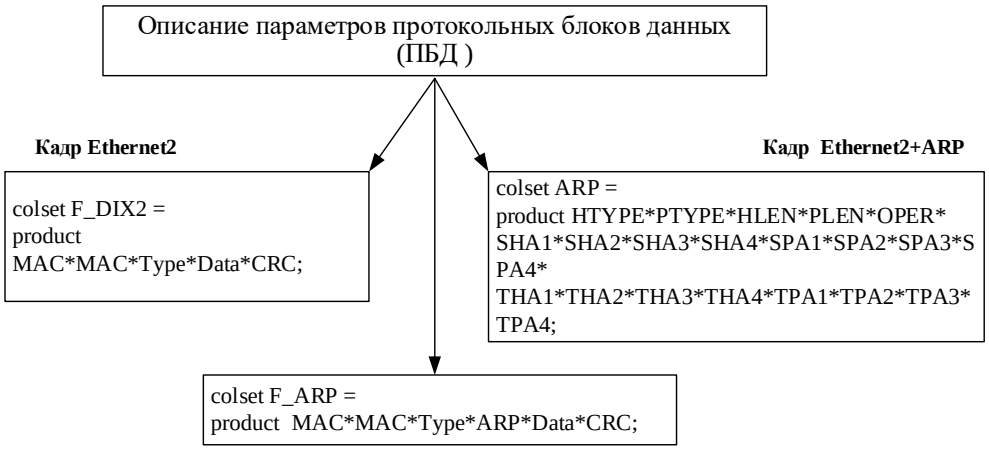

Рис. 11. Формирование иерархии цветов (типов) для кадра Ethernet, протокола ARP

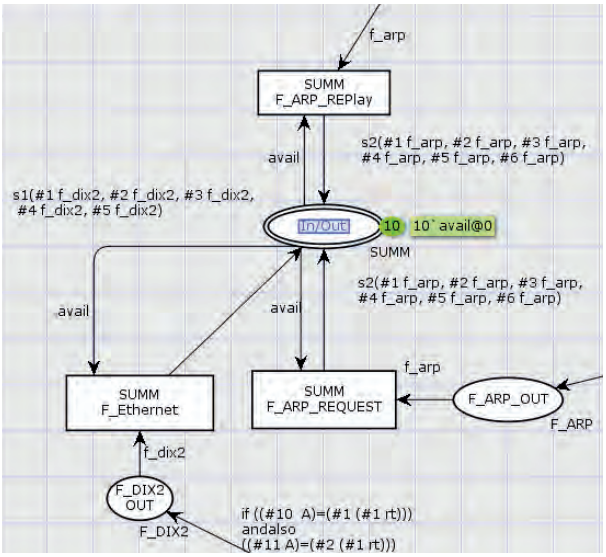

Рис. 12. Мультиплексирование объединение кадров с различным содержимым классов (F_DIX2, f_arp – запрос, f_arp – ответ) в структуры S1, S2 для передачи в канал

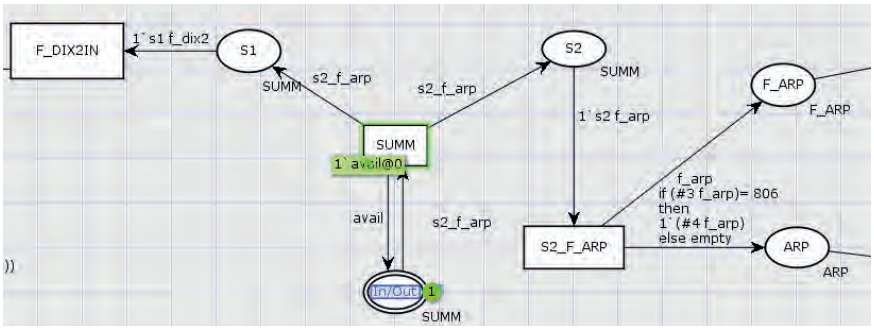

Рис. 13. Расщепление из единого потока S1, S2, кадров Ethernet с данными (F_DIX2), кадров протокола ARP (f_arp), пакетов протокола ARP (F_DIX2, f_arp – запрос, f_arp – ответ) в структуры S1, S2

Пример моделирования единой иерархической коммуникационной инфраструктуры на примере взаимодействия Ethernet, ARP представлен на рис. 14.

Заключение

Таким образом, моделирование фрагментов КИИ (ИС, АСУТП, ИТС) на основе математического аппарата иерархических s-гиперсетей и сетей Петри позволяет расширить прикладной аспект теории информационной безопасности в направлении моделирования и оценки защищенности объектов КИИ с учетом ее устойчивости в условиях воздействия КА. Моделирование на основе сетей Петри позволяет исследовать влияние протокольных особенностей построения объектов КИИ (ИС, АСУТП, ИТС) на свойства

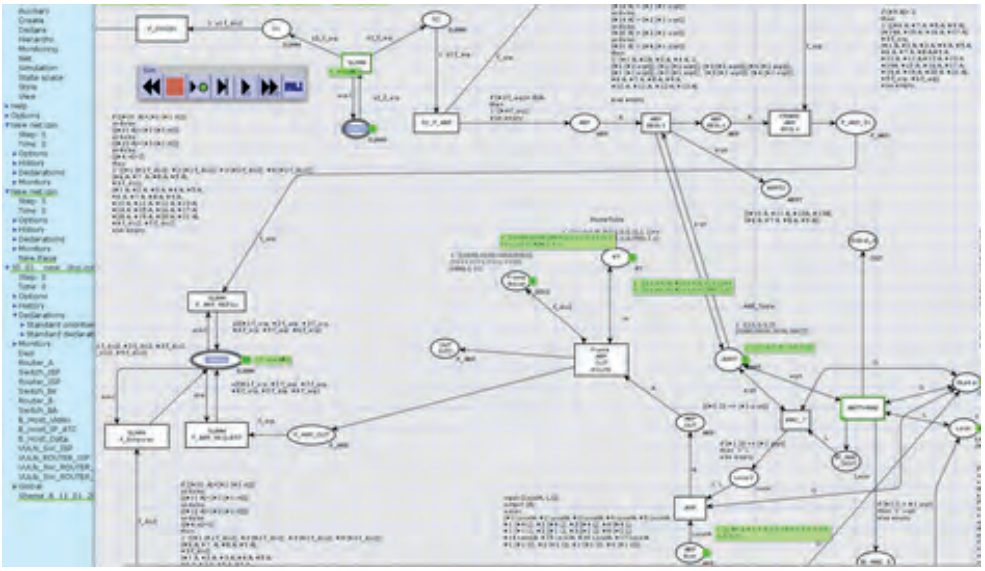

Рис. 14. Пример представления протокола ARP в имитационной модели

устойчивости и доступности объектов КИИ, и оценивать на основе этого их защищенность. Формирование параметрически точных моделей КИИ как аналитических, так и имитационных, 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 получать в том числе и количественные показатели оценки защищенности объектов КИИ в условиях воздействия нарушителя и исследовать влияние на них различных типов компьютерных атак.

Литература

1. *Зегжда Д. П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – Москва: Горячая линия – Телеком. 2023. – 500с. – ISBN 978-5-9912-0827-7.*
2. *Петренко С. А. Киберустойчивость цифровой индустрии 4.0: научная монография / С. А.Петренко. – Санкт-Петербург: Издательский Дом «Афина», 2020, – 256 с.*
3. *Петренко С. А. Управление киберустойчивостью. Постановка задачи // Защита информации. Инсайд. 2019. № 3(87). С. 16–24.*
4. *Штыркина А. А. Обеспечение устойчивости киберфизических систем на основе теории графов. Проблемы информационной безопасности // Компьютерные системы. 2021. № 2. С. 145–150.*
5. *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*
6. *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*
7. *Гурина Л. А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС // Вопросы кибербезопасности, 2022. № 3(48), С.18–26. DOI: 10.21681/2311-3456-2022-3-23-31*
8. *Чиркова Н. Е. Анализ существующих подходов к оценке киберустойчивости гетерогенных систем // Сборник материалов Международной научно-практической конференции: Техника и безопасность объектов уголовно-исполнительной системы Иваново. 2022. С. 408–410.*
9. *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.*
10. *Минаев М. В., Бондарь К. М., Дунин В. С. Моделирование киберустойчивости информационной инфраструктуры МВД России // Криминологический журнал. 2021. № 3. С. 123–128.*
11. *Осипенко А. А., Чирушкин К. А., Скоробогатов С. Ю., Жданова И. М., Корчевной 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.*
12. *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.*
13. *Величко В. В. Модели и методы повышения живучести современных систем связи / В. В. Величко, Г. В. Попков, В. К. Попков. – Москва: Горячая линия – Телеком, 2017. – 270 с. ISBN 978-5-94876-090-2.*
14. *Попков Г. В. Математические основы моделирования сетей связи / В. В. Величко, Г. В. Попков, В. К. Попков. – Москва: Горячая линия – Телеком, 2018.–182 с. ISBN 978-5-9912-0266-4.*
15. *Barrere M., Hankin C., Nicolaou N. // Journal of Information Security and Application. 2020. №52. DOI: 10.1016/jisa.2020.102471 [сайт]. – URL: https://www.sciencedirect.com/science/article/pii/S2214212619311342?via%3Dihub(дата обращения 10.11.2023).*