МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Бочков М. В.[1], Васинев Д. А.[2]

DOI: 10.21681/2311-3456-2025-4-17-29

Цель исследования: *разработка метода оценки защищенности критической информационной инфраструктуры (КИИ) на основе средств полунатурного и имитационного моделирования. Предлагаемый метод позволяет разработать параметрически точные имитационные модели объекта КИИ для исследования свойств защищенности и устойчивости, моделировать воздействия на объекты компьютерных атак (КА).*

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

Результат исследования: *предлагаемый метод оценки защищенности позволяет учитывать конфигурационные и коммуникационные особенности построения и функционирования объектов КИИ, динамику и параметры воздействия нарушителя на объекты КИИ, существующую политику безопасности, моделировать свойство устойчивости, проводить исследования степени влияния составных элементов на защищенность объекта КИИ. Разработанный метод моделирования позволяет осуществлять оценку защищенности объектов КИИ с учетом конфигурационных и коммуникационных параметров объекта КИИ, уменьшить зависимость от экспертных оценок, получать параметрически обоснованные оценки защищенности.*

Научная новизна: *заключается в развитии методов теории информационной безопасности в области оценки защищенности объектов КИИ за счет учета вложенности и иерархичности объектов методами теории гиперграфов и их реализации методами вложенных раскрашенных сетей Петри. В этом случае учитываются конфигурационные и коммуникационные параметры объектов КИИ, позволяющие получать параметрически точные имитационные модели на основе математического аппарата сетей Петри и осуществлять верификацию полученных результатов на полунатурных моделях. Практическая ценность заключается в получении оценок защищенности, основанных на известных параметрах объекта КИИ, возможности получения оценок защищенности на основании коммуникационных, инфраструктурных параметров самого объекта, возможности моделирования известных воздействий из банка данных угроз для проверки политики безопасности объекта КИИ в полученной модели.*

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

Введение

Продолжающееся информационное противоборство делает актуальными вопросы 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. 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[4,5,6].

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 объединяющими моментами являются применение технологий виртуальных частных сетей (VPN), резервирования, отказоустойчивости, обеспечение киберустойчивости в условиях воздействия компьютерных атак (КА)[7,8]. Кроме того, современные условия функционирования технических систем предполагают применение отечественного коммуникационного оборудования, средств

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

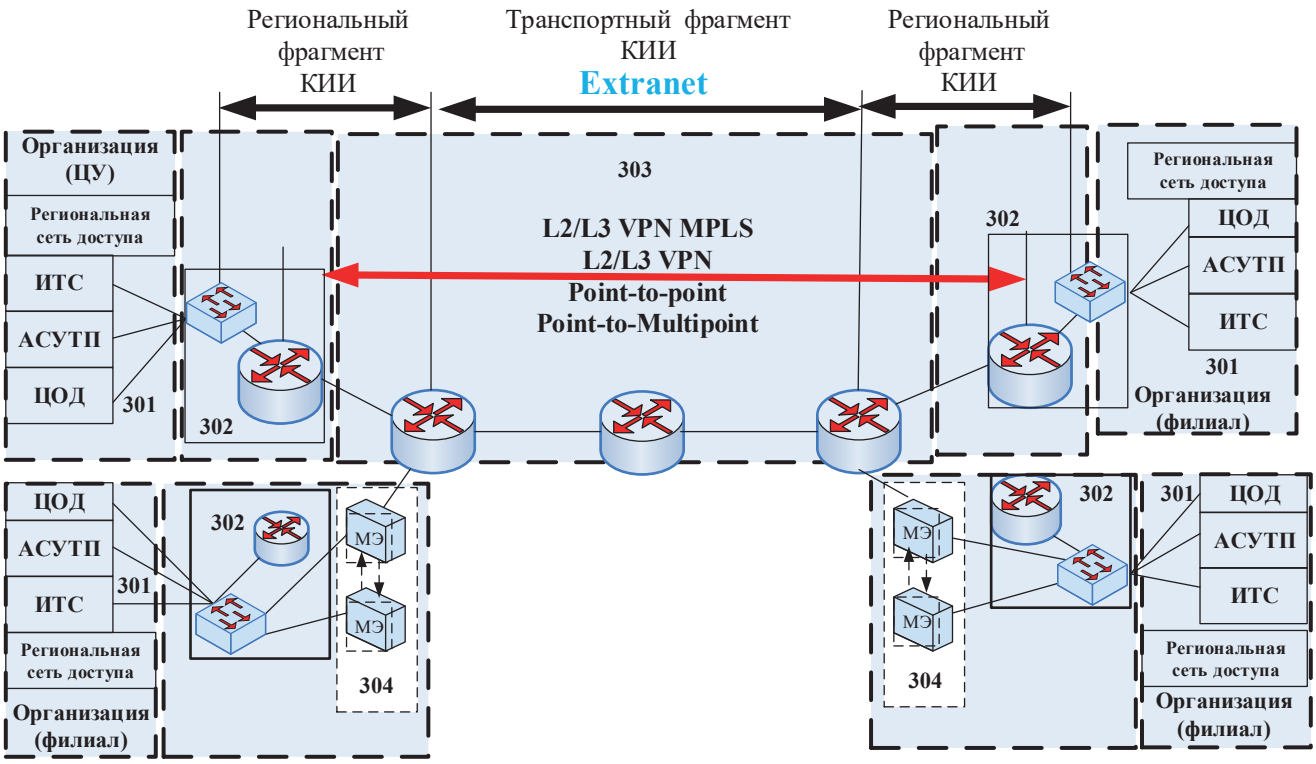
3 РосТелекомм. Аналитический отчет об атаках на онлайн ресурсы компании за 2022г. [сайт]. URL:https:// https://rt-solar.ru/upload/iblock/34a/5w4h9o57axovdbv3ng7givrz271ykir3/Ataki-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf.

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

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

6 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.

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



301. – Технические средства оконечных автоматизированных систем КИИ для отправки/приема единиц передаваемых данных	302. – Многопротокольное оборудование объекта КИИ.	303. – Многопротокольное оборудование оператора связи (ISP).
	304. – Программно-аппаратный отказоустойчивый кластер межсетевых экранов для объекта КИИ	

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

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 с учетом параметрических особенностей объекта воздействия является актуальной задачей [1–4].

Воздействие нарушителя на распределенную ИТС обусловлено инфраструктурными, коммуникационными особенностями организации каналов связи, предлагаемых оператором связи, на основе которого осуществляется организация взаимодействия между распределенными филиалами телекоммуникационных объектов КИИ, представлено на (рис. 1). Сетевые, транспортные и управляющие протоколы, которые применяются в коммуникационных инфраструктурах для передачи данных, управления, такие как Ethernet, ICMP, IP, TCP, UDP, SNMP. 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 неквалифицированными действиями персонала в распределенных фрагментах ИТС.

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 моделирования и оценки защищенности таких объектов (ИС, АСУТП, ИТС) а также исследования свойств устойчивости [1–4], с учетом иерархических особенностей формирования объектов КИИ предлагается применять совокупность имитационных и полунатурных моделей. При этом отличительной особенностью предлагаемого решения на основе имитационных моделей сетей Петри 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. [5]

В сложившихся условиях при сетевых воздействиях нарушителя на коммуникационную инфраструктуру (КИ) объекта КИИ существующие методы оценки защищенности, основанные на знании сигнатуры угрозы, сводятся к методам оценки защищенности от известных угроз, например, зарегистрированных в БДУ ФСТЭК. На рисунке 2 представлен процесс оценки защищенности объекта КИ на основе известных сигнатур угроз. [6–10]

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 неизвестные воздействия 1 и 2, представленные на рисунке 2. При этом методы обеспечения защищенности объекта КИИ на основе сигнатурных средств всегда отстают по времени от воздействия нарушителя, что создает предпосылки к нахождению объекта КИИ в незащищенных состояниях 1, 2 рисунок 2.

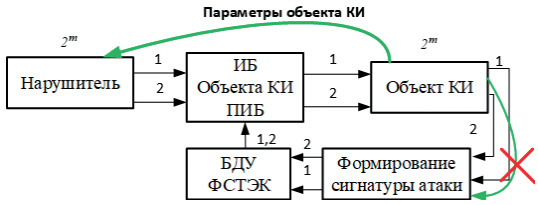


Рис. 2. Существующий подход к оценке защищенности объектов КИИ

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, требующим учета в разрабатываемых моделях.

Решением сложившегося противоречия между многообразием воздействия нарушителя и существующими возможностями методов и средств обеспечения информационной безопасности является учет параметров объекта КИИ в формировании политики информационной безопасности объекта. На рисунке 3 представлен процесс формирования оценок защищённости на основе учета m параметров объекта КИИ, формализации их в модели цифрового двойника (имитационной модели), расчет на ее основе оценок защищенности, учетm параметров в политике ИБ объекта КИИ.

В основе предлагаемого метода оценки защищенности – формирование на основе конфигурационных

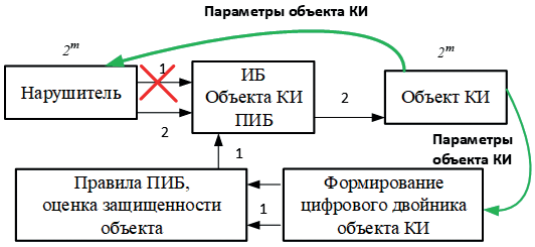


Рис. 3. Предлагаемый метод оценки защищенности объекта КИИ

и коммуникационных параметров функционирования объекта КИИ, его политики безопасности, моделей коммуникационной инфраструктуры, ее политики информационной безопасности, воздействия на нее нарушителя. Предлагаемый метод позволяет получать параметрически точные модели коммуникационной инфраструктуры – цифрового двойника объекта КИИ, в динамике исследовать влияние на политику информационной безопасности 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 взаимосвязанных моделей, связанных с формированием политики ИБ, анализом защищенности и действиями нарушителя [5].

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

Моделирование многоуровневых коммуникационных инфраструктур связано с особенностями их построения (рисунок 4) [5]. На основе анализа существующих методов моделирования и оценки защищенности [12–16], сформулированных ранее предположений о необходимости учета параметров объекта КИИ [5] разработан метод моделирования иерархически сложных телекоммуникационных объектов и метод оценки защищенности объектов КИИ на основе конфигурационных и коммуникационных параметров функционирования объекта КИИ.

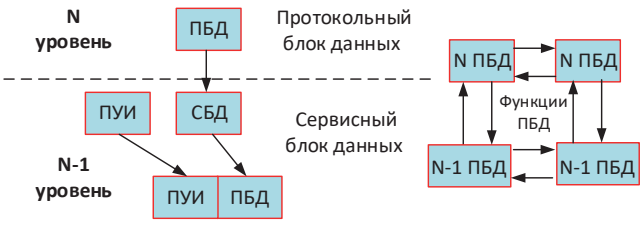


Рис. 4. Методы, способы взаимодействия ПБД в соответствии с моделью OSI (7498), X.200, ГОСТ Р ИСО/МЭК 7498-1-99

Основными особенностями, которые легли в основу универсальных масштабируемых модулей для имитационного и полунатурного моделирования, является внутриуровневое и межуровневое взаимодействие протокольных блоков данных, представленных на рисунке 4. В связи с необходимостью моделировать множество протоколов разработана концептуальная модель протокольного блока данных для реализации концепции вертикального и горизонтального взаимодействия протокольных блоков данных, учитывающая наиболее важные подсистемы взаимодействия, представлена на рисунке 5 [11].

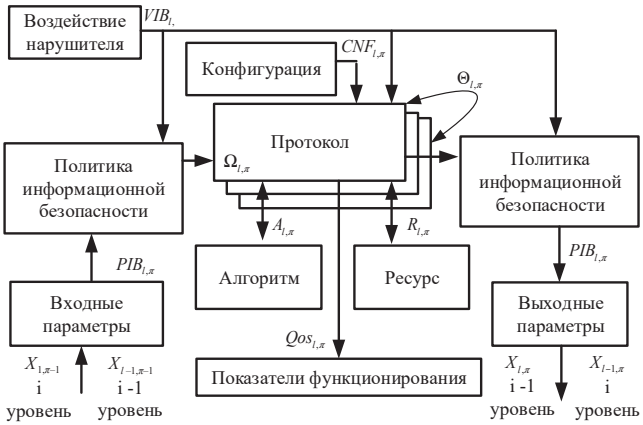


Рис. 5. Концептуальная модель протокольного блока данных

Для реализации разнотипных протокольных блоков данных, функционирующих в объектах КИИ, предлагается обобщенное концептуальное представление протокольного блока данных, представленного на рисунке 5. В основе его – протокол с множеством параметров π_l-го протокола на l-ом 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-ом уровне функционирования в коммуникационной инфраструктуре объекта КИИ, $R_{l,\pi}$ – ресурсом на l-ом уровне функционирования в коммуникационной инфраструктуре объекта КИИ, применяемого для функционирования π_l-го протокола в коммуникационной инфраструктуре, множеством показателей качества обслуживания – $Qos_{l,\pi}$, характеризующих функциональное состояние коммуникационной инфраструктуры объекта КИИ. Для π_l протокола на l-ом уровне функционирования входными/выходными параметрами являются $-X_{l,\pi}$. Для π_l протокола на l-ом уровне функционирования формируется множество параметров политики информационной безопасности – $PIB_{l,\pi}$ для входящего/исходящего направления π_l-го протокола на l-ом уровне функционирования в коммуникационной инфраструктуре объекта КИИ. Протокол имеет предварительно заданное множество параметров конфигураций – $CNF_{l,\pi}$ для π протоколов l-ого уровня функционирования в коммуникационной инфраструктуре объекта КИИ. Для протокола, а также политики информационной безопасности для π-го протокола l-ого уровня предусмотрено множество параметров деструктивных воздействий $VIB_{l,\pi}$ нарушителя для алгоритмов, функционирующих в коммуникационной инфраструктуре объекта КИИ [11].

Предлагаемое обобщенное представление протокольных блоков данных позволяет объединять похожие по функциональному назначению блоки (алгоритмов функционирования протокола, ресурса протокола, конфигураций, политики информационной безопасности, воздействия нарушителя) для построения универсальных имитационных моделей на основе вложенных раскрашенных сетей Петри [5].

Применение имитационного моделирования позволяет разработать универсальный метод построения имитационных протокольных блоков данных для различных типов протоколов, учесть коммуникационные и конфигурационные особенности их функционирования, являющиеся основой метода сквозного моделирования сетей, узлов и комплексов специальной связи. Данный метод представлен на рисунке 6.

Суть предлагаемого метода заключается во взаимосвязи конфигураций (параметров) объекта КИ (рисунок 6) с полунатурными и имитационными моделями и возможностями переноса конфигурации как с физического объекта на имитационные (рисунок 8) и полунатурные модели (рисунок 9), так и с имитационных, полунатурных моделей в физический объект. Представленная структурная взаимосвязь моделей в методе позволяет исследовать значимые свойства физического объекта на имитационных и полунатурных моделях и переносить значимые результаты их на физические объекты.

Объекты, представленные на рисунке 6, объединены единой логической составляющей – конфигурационными и коммуникационными параметрами. С физического объекта – конфигурационные и коммуникационные параметры переносятся в полунатурные модели физического объекта с высокой степенью достоверности. 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 коммуникационных инфраструктур, является получение универсальных масштабируемых имитационных и полунатурных моделей, пригодных для моделирования многоуровневых распределенных коммуникационных инфраструктур различных объектов КИИ.

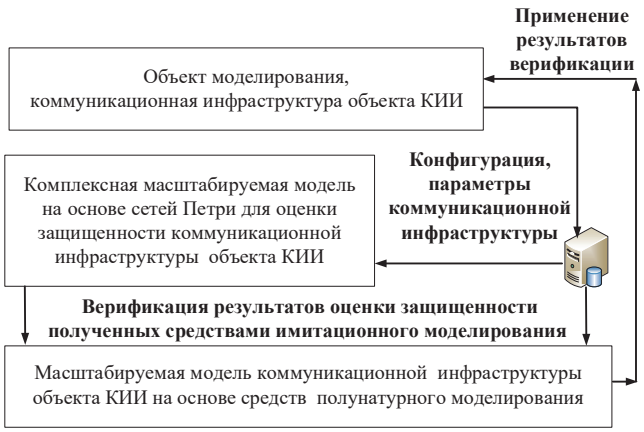


Рис. 6. Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

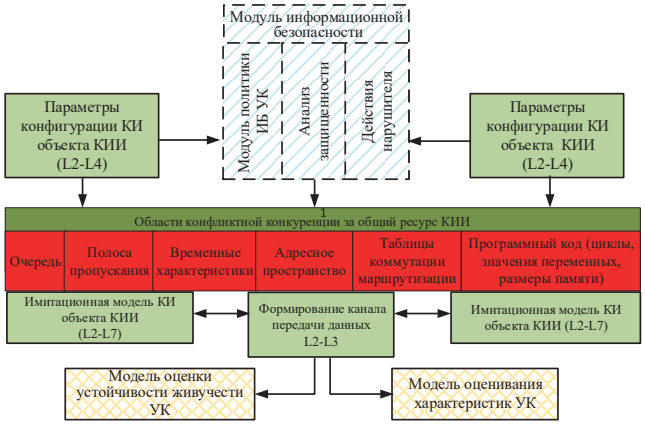


Рис. 7. Области конфликтного взаимодействия в модели оценки защищенности КИ объекта КИИ

Структура комплекса имитационных моделей для моделирования узла коммутации, подсистем информационной безопасности, области их конфликтного взаимодействия представлены на рисунке 7.

Пример реализации комплексной имитационной модели, учитывающей конфигурационные и коммуникационные параметры, методы обеспечения информационной безопасности, методы воздействия нарушителя, представлен на рис. 8. Модель объединяет основные взаимодействующие субъекты, инфраструктуры, методы обеспечения информационной безопасности, что позволяет моделировать конфликтное поведение взаимодействующих субъектов.

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 коммуникационной инфраструктуры являются: 1,2 – универсальная масштабируемая модель коммуникационной инфраструктуры объекта КИИ; 3,4 – модель ввода конфигураций коммуникационной инфраструктуры, задания сервисов; 5,6 – универсальная масштабируемая модель информационной безопасности для коммуникационной инфраструктуры объекта КИИ; 7 – результирующее множество регистрируемых угроз и их параметров для политики информационной безопасности коммуникационной инфраструктуры объекта КИИ; 8,9 – универсальная масштабируемая модель 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.

Основным элементом имитационной модели является модуль обеспечения информационной безопасности, концепция построения которого для входящего и исходящего информационного направления представлена на рисунке 9. Для входящего и исходящего направления структура блока обеспечения информационной безопасности содержит: модуль формализации конфигурации протокола в форме $|m|$ параметров коммуникационной инфраструктуры; модель формирования политики информационной безопасности – формализация политики информационной безопасности объекта КИИ в форме команд имитационной модели; анализа защищенности для политики безопасности на основе $2\times|m|$ параметров, формирование нарушителя политики безопасности КИ – на основе $2\times|m \pm \Delta|$, методом стохастического случайного поиска в заданном пространстве состояний параметров $|m|$[8].

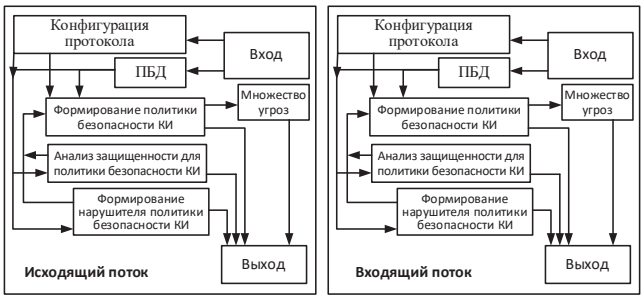


Рис. 9. Концепция построения модуля информационной безопасности для моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в КИ объекта КИИ

Реализация представленной на рисунке 9 концепции построения модуля информационной безопасности представлена на рисунке 10 вложенными раскрашенными сетями Петри.

8 Требования по безопасности информации, приказ ФСТЭК № 33 от 07.03.2024 г.

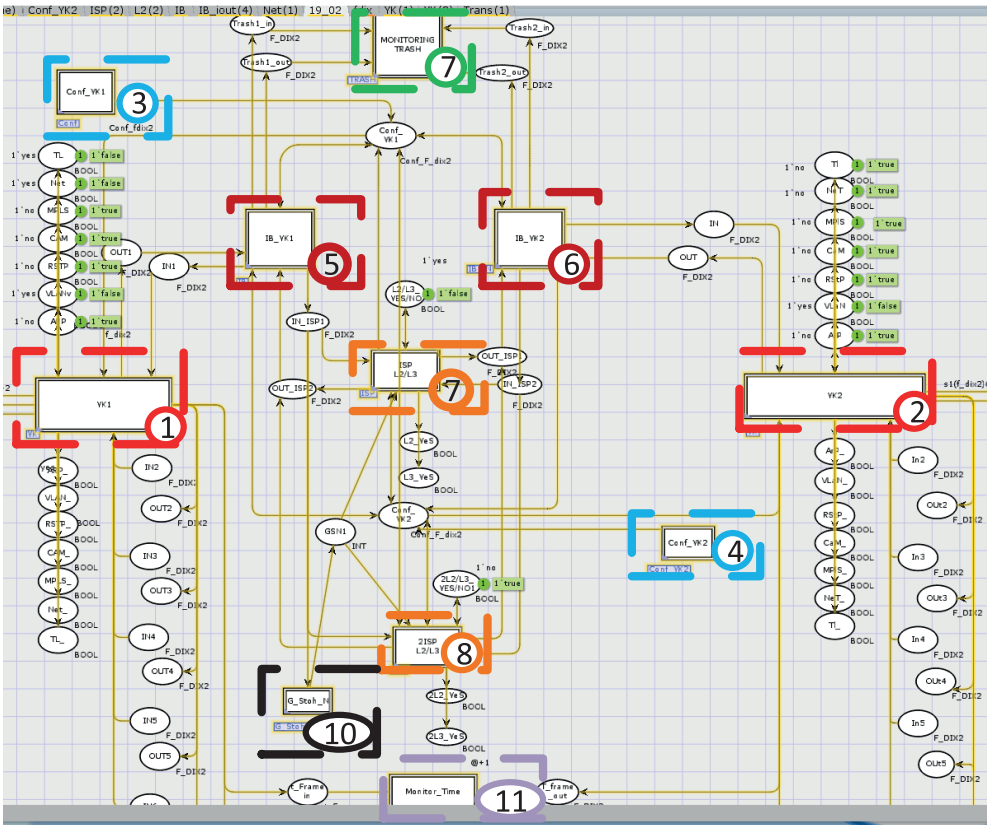


Рис. 8. Комплексная имитационная модель коммуникационной инфраструктуры, с учетом функционирования методов и средств обеспечения ИБ, а также конфликтности взаимодействия

Ключевым фактором является учет всех параметров объекта КИ объекта КИИ $|m|$, на основе которых осуществляется расчет тестовых комбинаций для анализа защищенности $2\times|m|$, а также вторичная верификация в пространстве случайных состояний $2\times|m \pm \Delta|$.

Верификация политики информационной безопасности множества тестовых запросов, происходящая в полунатурной модели коммуникационной инфраструктуры объекта КИИ, представлена на рисунке 11, позволяет проверить работоспособность политики информационной безопасности относительно тестов на основе множества параметров объекта – $|m|$.

С целью верификации политики информационной безопасности формируется программно-аппаратный комплекс на основе полунатурных моделей, например, UNL/EVE, или средств виртуализации на основе операционных систем с открытым исходным кодом. 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

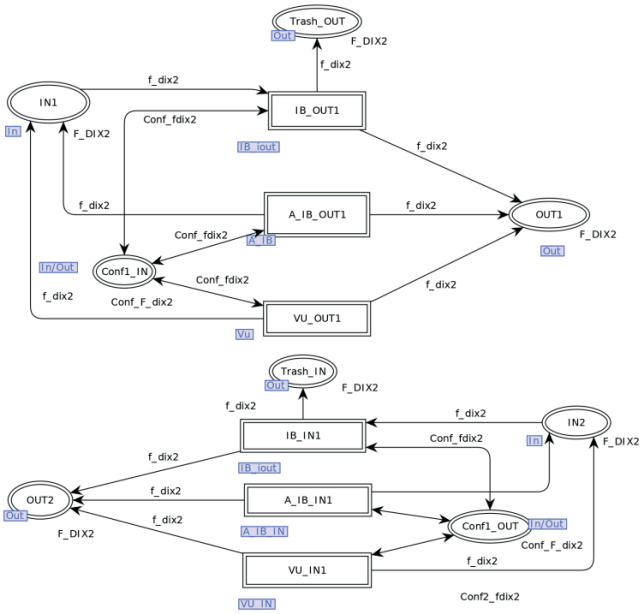


Рис. 10. Пример моделирования политики ИБ, анализа защищенности, формирования модели нарушителя в КИ объекта КИИ на основе вложенных, раскрашенных сетей Петри для входящего и исходящего направления

разработанного программно-аппаратного комплекса тестирования телекоммуникационного и оконечного оборудования объектов КИИ[9] [17].

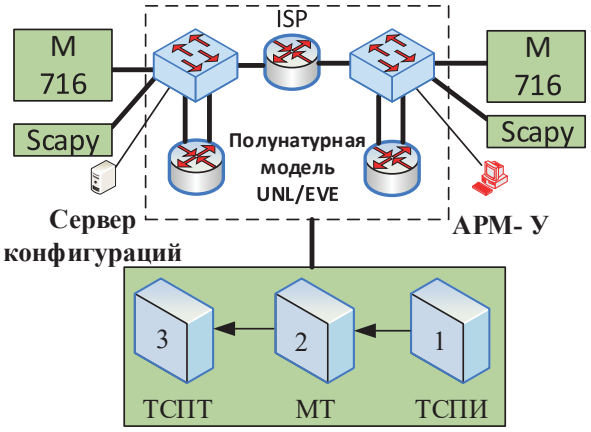


Рис. 11. Пример варианта программно-аппаратной реализации коммуникационной инфраструктуры в средствах полунатурного моделирования

Предлагаемый метод формирования моделей коммуникационной инфраструктуры и верификации результатов имитационного моделирования позволяет формировать параметрически точные модели, учитывающие существующие конфигурации объекта КИИ, параметры его политики информационной безопасности, моделировать параметрические действия нарушителя и исследовать влияние изменения выделенных подсистем на защищенность объекта КИИ в динамике взаимодействия объекта КИ политики его ИБ, действий нарушителя. Верификация результатов имитационного моделирования предусмотрена полунатурными моделями, аналитическими методами, сравнением функциональных характеристик (формирование и фильтрация протокольных блоков данных) с физическим объектом.

2. Метод оценки защищенности коммуникационной инфраструктуры объектов КИИ

Основные взаимосвязанные элементы метода, позволяющие решать задачу оценки защищенности на основе параметров конфигурации, представлены на рисунке 12, 13.

Формирование комплексной модели оценки защищенности на основе вложенных раскрашенных сетей Петри осуществляется в блоке 1 рисунка 12. Проводится формализация в правилах имитационной модели параметров коммуникационной инфраструктуры $|m|$, составляющих протокольную часть коммуникационной инфраструктуры объекта КИИ. Формализация в правила имитационной модели множества разрешающих правил *true*, политики информационной безопасности, с учетом $|m|$ параметров КИ. Формализация в правила имитационной модели множество запрещающих правил *false* на основе формирования тестовых последовательностей $2\times|m|$ и $2\times|m \pm \Delta|$ параметров коммуникационной инфраструктуры (блок 1).

На основе существующих параметров КИ $|m|$, осуществляют автоматическое (эталонное) построение политики информационной безопасности коммуникационной инфраструктуры объекта КИИ – множества разрешающих правил *true* – $rule_{MsIB} = |\{rule_{КИ,Конф,N}\{KI(H,P,CF,S)\} = rule_{КИ,Конф,N}\{MsIB\}\}| = |m|$ в блоке 2, а также формируют множество правил ИБ – $rule_{MsIB} = \{MsIB\}$, для существующей политики ИБ КИ объекта КИИ в блоке 3, рисунка 12.

Осуществляют проверку политики ИБ коммуникационной инфраструктуры объекта КИИ (блок 4) методом сопоставления множеств $truerule_{MsIB} = rule_{КИ,Конф,N}\{MsIB\}$ с формализованной политикой ИБ объекта КИИ множеством $\{rule_{MsIB}\}$, на основе которых в случае $\{rule_{КИ,Конф,N}\}\backslash\{rule_{MsIB}\} = \{Inc_{ib}\}$ – формируют множество угроз в блоке 14 рисунка 13.

В блоке 5 на основе параметров КИ множества – $|m|$, формируют тестовые последовательности для анализа защищенности множество *false* $\{VN(KI(H,P,CF,S),V)\} = \{m \pm \Delta\} = 2 \times |m|$. Далее осуществляют сопоставление множеств правил политики ИБ и множеств правил для анализа защищенности объекта КИИ, $\{rule_{MsIB}\}\backslash\{m \pm \Delta\} = \{\dashv\}$, на основе которых в случае $\{rule_{MsIB}\}\backslash\{m \pm \Delta\} = \{Inc\_A\_i\ b\}$ – формируют множество угроз в блоке 14.

Верификации политики ИБ КИ $\{rule_{MsIB}\}$ нарушителя методами стохастического случайного поиска на основе Марковской цепи, с модификацией параметров протокольных блоков данных генетическим алгоритмом осуществляется в блоках 6–10 рисунка 12. При этом множество $\{m \pm \Delta\}$ расширяется множеством на основе тестовых последовательностей $M = \{m_1 \ldots m_k\}$. Осуществляется вторичная верификации политики информационной безопасности методом сопоставления множества $M = \{m_1 \ldots m_k\}$ с формализованной политикой ИБ объекта КИИ $\{rule_{MsIB}\}$.

По результатам сравнения политики ИБ коммуникационной инфраструктуры объекта КИИ с тестовыми последовательностями множества *false* в элементах 111, 122, 133 тестовые запросы, неучтенные политикой информационной безопасности (блоках 11, 12, 13 рисунка 13), позволяют получить множество угроз для коммуникационной инфраструктуры объекта КИИ (блок 14 рисунка 13).

В блоке 14 формируется множество известных и неизвестных относительно функциональных возможностей средств обеспечения ИБ угроз, которое получено на основе имитационной модели и сделанных предположений о составе и структуре множества угроз ИБ КИ ($F = f_{true} \cup f_{false}$, блок 14, рисунка 13). Предположение заключается в том,

9 Свидетельство о регистрации программы для ЭВМ RU 20246115254 от 05.03.2024 г.

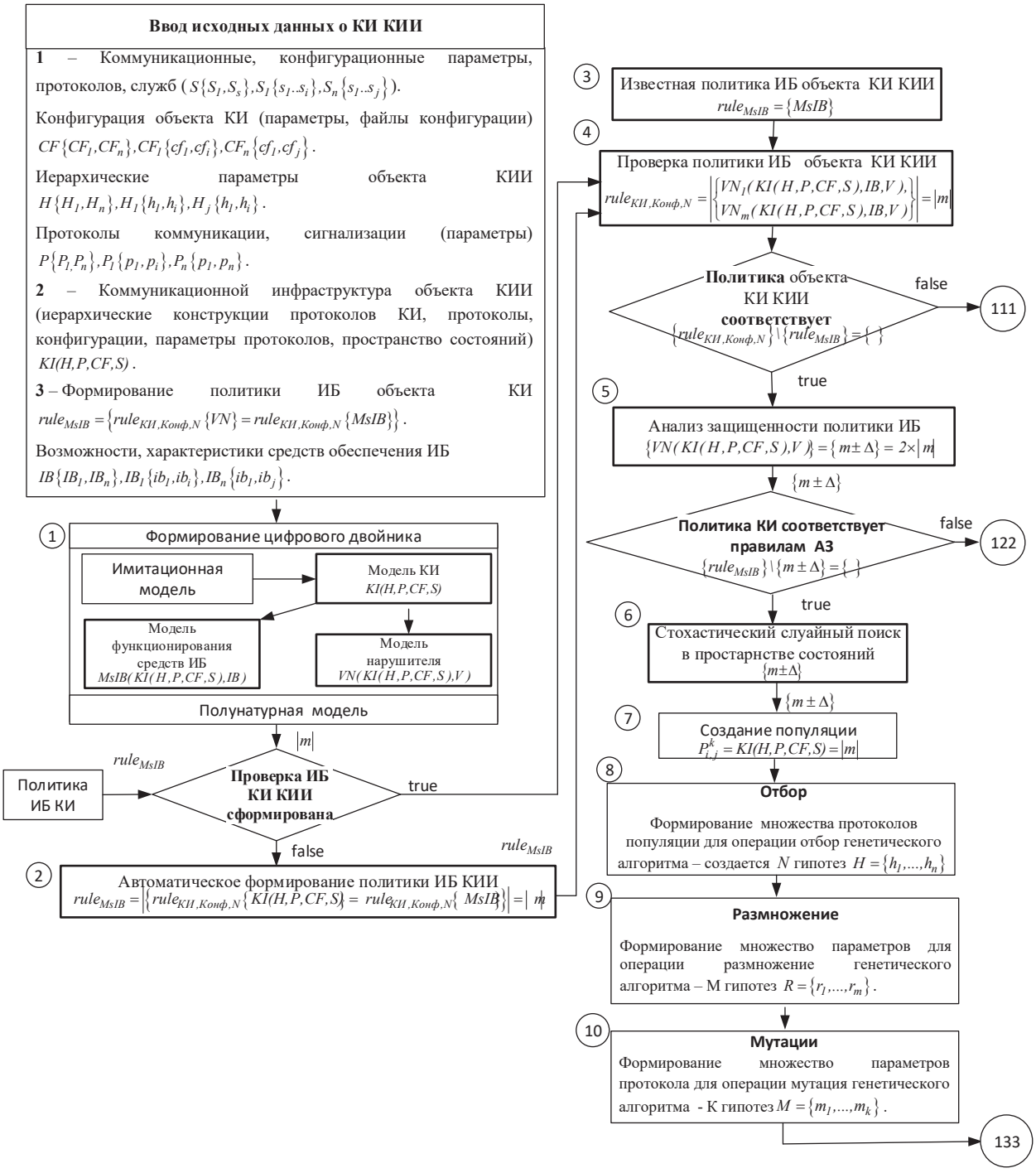


Рис. 12. Метод оценки защищенности КИ объектов КИИ (анализ защищенности)

что множество угроз $F = f_{true} \cup f_{false}$ КИ структурировано относительно параметров КИ – $|m|$, а также функциональных возможностей средств обеспечения ИБ объекта КИИ, влияющих на соотношение множеств f_{true} и f_{false}. Имитационная модель позволяет рассчитать эти соотношения. На основе множества неизвестных угроз f_{false} (блок 15) формируется множество известных f_{true} (блок 16) относительно политики ИБ объекта КИИ.

Для множества известных угроз реализуются алгоритмы обеспечения киберустойчивости на основе логического резерва КИ (блок 17), а для неизвестных угроз алгоритмы обеспечения киберживучести (блок 18) на основе логического, физического резерва КИ по заданным правилам.

Оценка защищенности УК осуществляется в блоке 20 на основе исходных данных 1, 2, 3, 4, позволяет оценивать защищенность, незащищенность,

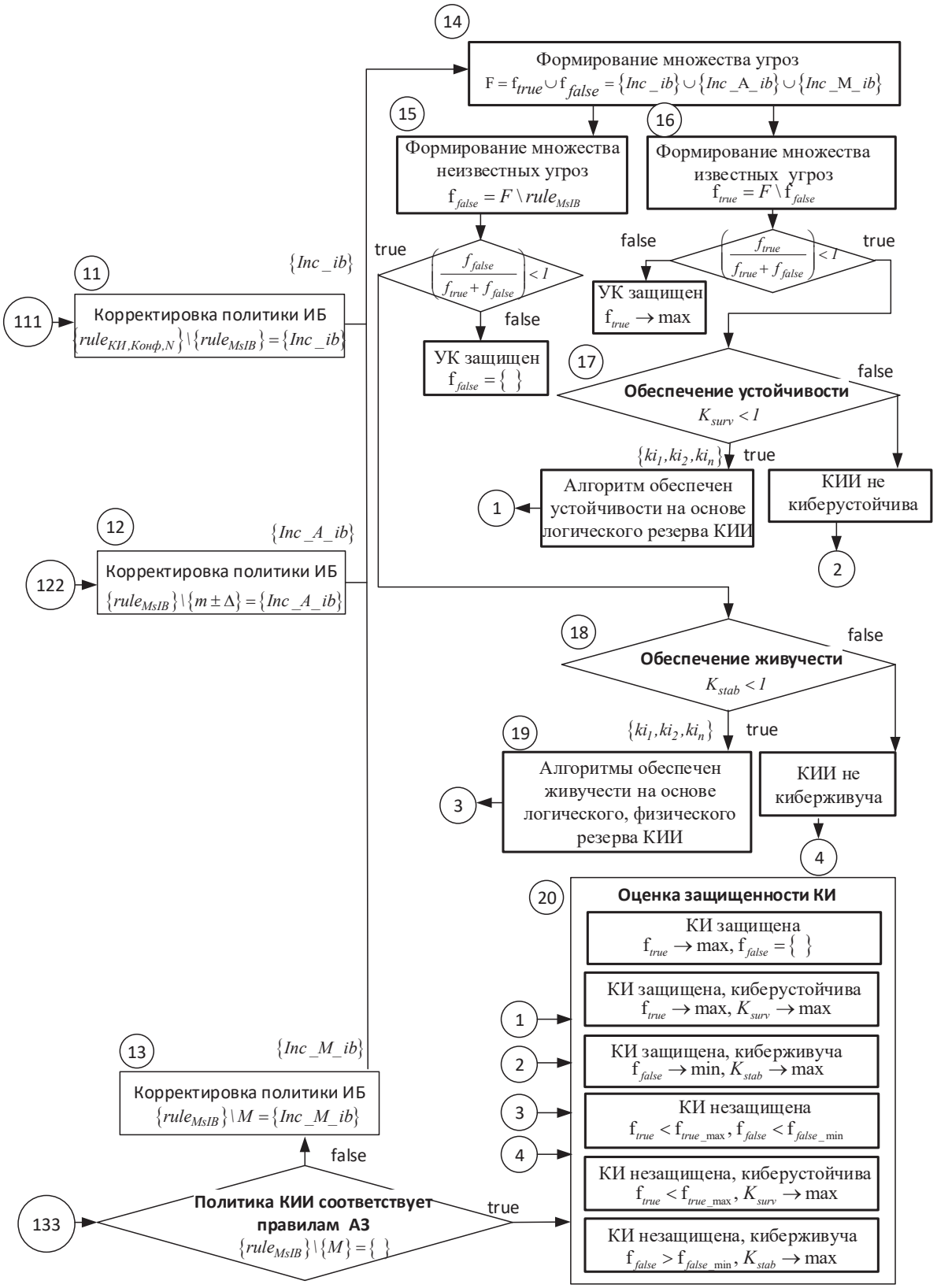


Рис. 13. Метод оценки защищенности КИ объектов КИИ (оценка защищенности)

киберустойчивость объектов относительно известных параметров объекта КИИ и возможностей средств обеспечения его ИБ.

Таким образом, на основе предлагаемого метода моделирования объектов КИИ получены параметрически точные модели объектов КИИ, осуществляется моделирование политики ИБ, проверка политики ИБ КИИ различными классами тестов – анализом защищенности, моделированием действий нарушителя. В предлагаемом методе параметры коммуникационной инфраструктуры являются исходными данными для функционирования модуля ИБ, на основе которого формируются тестовые проверочные конструкции различных типов.

Полученные результаты полунатурного и имитационного моделирования позволяют применять их для расчета защищенности объекта КИИ, верификации его политики безопасности относительно известных параметров, пример которой представлен в таблицах 1–4. Пример расчета основан на оценке защищенности протокола Ethernet для кадра DIX2, для размерности пространства состояний m. Известно, что для размера кадра Ethernet DIX2 l = 1518 бит, возможно 2^{1518} бит воздействий нарушителя, очевидно, что пространство состояний достаточно большое. На основе предложенного варианта снижения его размерности предлагается выделить параметры КИ объекта КИИ, участвующих во взаимодействии. Пусть исходные данные объекта КИИ заданы параметрами канального уровня. 00:00:00:00:00:02 – macD (адрес назначения), 00:00:00:00:00:01 – macS (адрес источника), 11:11:11:1:11:11 – широковещательный адрес; Etype(2): 0x0800 (2048) – Ipv4 (типа протокола); 0x8100 (33024)– 802.1q (тегированного кадра) – 5 параметров – значения m. Параметры коммуникационной инфраструктуры позволяют снизить размерность пространства состояний до 5 значений.

Пусть правила политики ИБ объекта КИИ содержат 2 правила по фильтрации кадров. Проверка работоспособности функционирования политики ИБ относительно параметров объекта КИИ осуществляется не более чем 5 тестовыми запросами, учитывающими m разрешенных параметров, запросы формируются разрешенные. Анализ защищенности осуществляется на основе $2 \cdot m$ параметров, позволяет проверить работоспособность политики ИБ по верхней и нижней границе относительно значения m. В этом случае $2 \cdot m$ тестовых запросов представляют собой тестовые деструктивные запросы для анализа защищенности. Значения тестовых множеств для рассматриваемого примера представлены в таблице 1.

В таблице 1 введены значения коммуникационных $N_i^{КИ}$ и конфигурационных N_i^{Cnf} параметров объекта КИИ в предположении, что они будут представлять отдельные непересекающиеся множества значений при учете всего множества параметров m.

На основе представленных параметров произведены расчеты на имитационной модели, результаты которых представлены в таблице 2.

При работе имитационной модели было сформировано 112 кадров, из которых, число деструктивных кадров – 50, среди которых 40 учитываются политикой ИБ объекта КИИ, а 10 политикой ИБ не учитываются по причине отсутствия функциональных возможностей оборудования, необходимостью модернизации самой политики ИБ.

Получение тестовых последовательностей P_i, множество пакетов воздействия нарушителя – угроз коммуникационной инфраструктуре, конфигурациям, неизвестные относительно возможностей средств информационной безопасности $(K_i(K_i^{КИ},Cnf_i^{КИ},N_i^{КИ}))$ – угрозы, не прошедшие политику ИБ. Выделенное множество угроз K_i содержит угрозы – $(K_{BHi}^{КИ},Cnf_{BHi}^{КИ})$, устранимые средствами политики ИБ за время $T_{УСТР}^{КИ} \le T_{доп}^{КИ}$, приемлемое время для функционирования коммуникационной инфраструктуры объектов КИИ, и угрозы – $N_i^{КИ}$, не устранимых средствами политики ИБ за время $T_{УСТР}^{N} \ge T_{доп}^{N}$ неприемлемое для функционирования коммуникационной инфраструктуры объектов КИИ, представлено в таблице 2.

Имитационная модель позволяет исследовать поведение объекта КИИ в условиях резервирования физических или логических элементов объекта КИИ, получая при этом оценки для случая функционирования КИ объекта КИИ в условиях известных угроз – обеспечения киберустойчивости, так и в условиях неизвестных угроз относительно политики информационной безопасности – обеспечение

Таблица 1.

Исходные данные для оценки защищенности объекта КИИ

Количество параметров (коммуникационных, конфигурационных)	**Количество правил политики ИБ объекта**	**Количество правил для проверки политики ИБ**	**Количество правил для анализа защищенности одного направления**	**Количество правил для анализа защищенности с учетом политики ИБ**
$N_i^{КИ}$, N_i^{Cnf}	$rule_i^{MsIB}$	$N_i^{КИ} + N_i^{Cnf}$	$2^{(K_{BH_i}^{КИ} + Cnf_{BHi}^{КИ})}$	$(2 \cdot m + \mathrm{m})$
5	2	5	10	15

Таблица 2.

Результаты расчета имитационной модели по тестированию политики ИБ

Количество пакетов, сформированные имитационной моделью	Количество пакетов, не соответствующие политике ИБ	Количество пакетов нарушителей КИ, потенциально устранимых средствами политики ИБ $T_{УСТР}^{КИ} \le T_{доп}^{КИ}$	Количество пакетов нарушителей КИ, неустранимых средствами политики ИБ за время $T_{УСТР}^{N} \ge T_{доп}^{N}$
P_i	$K_i(K_i^{КИ}, Cnf_i^{КИ}, N_i^{КИ})$	$K_{BH_i}^{КИ}, Cnf_{BHi}^{КИ}$	$N_i^{КИ}$
112	50	40	10

Таблица 3.

Расчет коэффициентов устойчивости на основе резервного ресурса логического и физического пространства состояний

Количество физических резервных направлений	Количество логических резервных направлений	Количество допустимых физических резервных направлений	Количество допустимых логических резервных направлений	Коэффициент устойчивости	Коэффициент живучести
$F_{факт}$	$L_{факт}$	$F_{доп}$	$L_{доп}$	$K_{stab} = \frac{L_{факт}}{L_{доп}}$	$K_{stab} = \frac{F_{факт}}{F_{доп}}$
2	2	6	10	0,2	0,33

киберживучести объекта. При этом под физическими элементами резервирования понимаются коммуникационное оборудование, каналы связи различного типа. Под логическим резервированием понимаются логические транспортные единицы формируемые в многопротокольном оборудовании (VLAN, VRF, Tunnel L2/L3, протоколы маршрутизации).

Результаты расчетов позволяют ограничить допустимые значения логического резерва – $L_{доп}$, а также допустимые значения физического резерва $F_{доп}$, с учетом имеющегося ресурса резервирования КИ рассчитать коэффициенты устойчивости и живучести, представленные в таблице 3.

Итоговый расчет защищенности как без учета резервирования, так и с учетом резервирования представлен в таблице 4.

Для заданных исходных данных, определяемых параметрами коммуникационной инфраструктуры, получены параметрически обоснованные и точные оценки защищенности объекта КИИ. При этом для полученных оценок очевидны причинно-следственные связи защищенности объекта КИИ с его параметрами. Выявленные недостатки средств обеспечения информационной безопасности позволяют определить направления дальнейшего совершенствования политики информационной безопасности. В случае обеспечения функционирования объекта КИИ в условиях компьютерных атак появляются как теоретические предположения, объясняющее этот процесс и поведение объекта КИИ в дальнейшем, так и практическое подтверждение расчета оценок его защищённости.

Таблица 4.

Оценка коэффициентов защищенности с учетом устойчивости, живучести на основе комплексной интегрированной модели оценки защищенности

Коэффициент защищенности	Коэффициент защищенности с учетом киберустойчивости и киберживучести
$K_n^{ИБ}$	$K_n^{Конф,КИ,N} = \frac{\left(\sum_{i=1}^{n} K_i^{КИ} + \sum_{i=1}^{n} K_i^{Конф}\right)}{\sum_{i=1}^{n} (K_n^{КИ} + K_n^{Конф} + K_n^{N})} K_{stab} + \frac{\sum_{i=1}^{n} N_i}{\sum_{i=1}^{n} (K_n^{КИ} + K_n^{Конф} + K_n^{N})} K_{surv}.$
$K_n^{ИБ} = 40/50 = 0,8$	$K_n^{Конф,КИ,N} = 40/50 \cdot 0,2 + 10/50 \cdot 0,33 = 0,8 \cdot 0,2 + 0,2 \cdot 0,33 = 0,226$

Заключение

Таким образом, предлагаемый метод оценки защищенности фрагментов КИ объектов КИИ (ИС, АСУТП, ИТС) на основе иерархических, раскрашенных сетей Петри позволяет расширить прикладной аспект теории информационной безопасности в направлении развития методов моделирования и методов оценки защищенности объектов КИИ на основе учета иерархичности и вложенности объектов учитываемой теорией гиперграфов ее реализации во вложенных раскрашенных сетях Петри. Моделирование на основе сетей Петри позволяет исследовать влияние протокольных особенностей построения объектов КИИ (ИС, АСУТП, ИТС) на свойства устойчивости и доступности объектов КИИ 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 получать в том числе и количественные параметрически обоснованные 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: монография / Александрова Е. Б., Калинин М. О., Марков А. С. [и др.]. – 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, – 255 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. Васинев Д. А., Бочков М. В. Моделирование устойчивости критической информационной инфраструктуры на основе иерархических гиперсетей и сетей Петри // Вопросы кибербезопасности, 2024, № 1(59), С. 108–115. DOI: 10.21681/2311-3456-2024-1-108-115.
6. Минаев М. В., Бондарь К. М., Дунин В. С. Моделирование киберустойчивости информационной инфраструктуры МВД России // Криминологический журнал. 2021. № 3. С. 123–128.
7. Осипенко А. А., Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей / Чирушкин К. А., Скоробогатов С. Ю., Жданова И. М., Корчевной П. П. //Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281.
8. 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.
9. 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.
10. 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.
11. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления //Системы управления, связи и безопасности. 2015. № 3. С. 122–186, УДК 623-624.
12. 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.
13. Гурина Л. А. Повышение киберустойчивости SCADA и WAMS при кибератаках на информационно-коммуникационную подсистему ЭЭС // Вопросы кибербезопасности. 2022. №2(48). С.23-31. DOI: 10.21681/2311-3456-2022-2-18-26
14. 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.
15. 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.
16. 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.
17. Васинев Д. А., Соловьев М. В., Предложения по построению универсального фаззера протоколов//Труды учебных заведений связи. 2023. № 9(6). С. 59–67. DOI: 10.31854/1813-324X-2023-9-6-59-67.

METHOD ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURE SECURITY ON THE BASIS OF SEMI-NATURAL AND SIMULATION MODELING TOOLS

Bochkov M. V.[10], Vasinev D. A.[11]

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

Research objective: *development of a method assessing the security of critical information infrastructure (CII) based on semi-natural and simulation modeling tools. The proposed method allows to develop parametric accurate simulation models of the CII object to investigate the properties of security and stability, to model the impact on the objects of computer attacks (CA).*

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

Research result: *the proposed modeling method allows to take into account the configuration and communication features of the construction and functioning of CII objects, the dynamics and parameters of the intruder's impact on the CII objects, the existing security policy, to model the stability property, to conduct research on the degree of influence of the constituent elements on the security of the CII object. The developed modeling method makes it possible to assess the security of KII objects taking into account the configuration and communication parameters of the KII object, to reduce the dependence on expert assessments, to obtain parametrically justified security assessments.*

References

1. Zegzhda D. P. Kiberbezopasnost' cifrovoj industrii. Teorija i praktika funkcional'noj ustojchivosti k kiberatakam / Pod redakciej professora RAN, doktora tehnicheskih nauk D.P. Zegzhdy. – Moskva: Gorjachaja linija – Telekom. 2023. – 500s. – ISBN 978-5-9912-0827-7.
2. Petrenko S. A. Kiberustojchivost' cifrovoj industrii 4.0: nauchnaja monografija / S. A.Petrenko. – Sankt-Peterburg: Izdatel'skij Dom «Afina», 2020, – 256 s.
3. Petrenko S. A. Upravlenie kiberustojchivost'ju. Postanovka zadachi // Zashhita informacii. Insajd. 2019. № 3(87). S. 16–24.
4. Shtyrkina A. A. Obespechenie ustojchivosti kiberfizicheskih sistem na osnove teorii grafov. Problemy informacionnoj bezopasnosti // Komp'juternye sistemy. 2021. № 2. S. 145–150.
5. Vasinev D. A., Bochkov M. V. Modelirovanie ustojchivosti kriticheskoj informacionnoj infrastruktury na osnove ierarhicheskih gipersetej i setej Petri // Voprosy kiberbezopasnosti, 2024, № 1(59), S. 108–151. DOI: 10.21681/2311-3456-2024-1-108-115.
6. Minaev M. V., Bondar' K. M., Dunin V. S. Modelirovanie kiberustojchivosti informacionnoj infrastruktury MVD Rossii // Kriminologicheskij zhurnal. 2021. № 3. S. 123–128.
7. Osipenko A. A., Chirushkin K. A., Skorobogatov S. Ju., Zhdanova I. M., Korchevnoj P. P. Modelirovanie komp'juternyh atak na programmno-konfiguriruemye seti na osnove preobrazovanija stohasticheskih setej // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2023. № 2. S. 274–281.
8. Vang L., Egorova L. K., Mokrjakov A. V., Razvitie teorii Gipergrafov // Izvestija RAN. Teorija i sistemy upravlenija. 2018. №1. S. 111–116. DOI: 10.7868/S00023388180110.
9. Velichko V. V. Modeli i metody povyshenija zhivuchesti sovremennyh sistem svjazi / V. V. Velichko, G. V. Popkov, V. K. Popkov – Moskva: Gorjachaja linija – Telekom, 2017.–270 s. ISBN 978-5-94876-090-2.
10. Popkov, G. V. Matematicheskie osnovy modelirovanija setej svjazi / V. V. Velichko, G. V. Popkov, V. K. Popkov – Moskva: Gorjachaja linija – Telekom, 2018.–182 s. ISBN 978-5-9912-0266-4.
11. Makarenko S. I. Dinamicheskaja model' sistemy svjazi v uslovijah funkcional'no-raznourovnevogo informacionnogo konflikta nabljudenija i podavlenija // Sistemy upravlenija, svjazi i bezopasnosti. 2015. № 3. S. 122–186, UDK 623–624.
12. Kolosok I. N., Gurina L. A. Ocenka pokazatelej kiberustojchivosti sistem sbora i obrabotki informacii v JeJeS na osnove polumarkovskih modelej // Voprosy kiberbezopasnosti, 2021, № 6(46), S. 2–11. DOI: 10.21681/2311-3456-2021-6-2-11.
13. Gurina L. A. Povyshenie kiberustojchivosti SCADA i WAMS pri kiberatakah na informacionno-kommunikacionnuju podsistemu JeJeS // Voprosy kiberbezopasnosti. 2022. №2(48). S. 18–26. DOI: 10.21681/2311-3456-2022-2-18-26.
14. Gurina L. A. Ocenka kiberustojchivosti sistemy operativno-dispetcherskogo upravlenija JeJeS // Voprosy kiberbezopasnosti, 2022. № 3(48), S. 18–26. DOI: 10.21681/2311-3456-2022-3-23-31.
15. Chirkova N. E. Analiz sushhestvujushhih podhodov k ocenke kiberustojchivosti geterogennyh sistem // Sbornik materialov Mezhdunarodnoj nauchno-prakticheskoj konferencii: Tehnika i bezopasnost' ob#ektov ugolovno-ispolnitel'noj sistemy Ivanovo. 2022. S. 408–410.
16. Bobrov V. N., Zaharchenko R. I., Buharov E. O., Kalach A. V. Sistemnyj analiz i obosnovanie vybora modelej obespechenija kiberustojchivogo funkcionirovanija ob#ektov kriticheskoj informacionnoj infrastruktury //Vestnik Voronezhskogo instituta FSIN Rossii. 2019. № 4. S. 31–43.
17. Vasinev D. A., Solov'ev M. V., Predlozhenija po postroeniju universal'nogo fazzera protokolov // Trudy uchebnyh zavedenij svjazi. 2023. №6. S. 59–67. DOI: 10.31854/1813-324X-2023-9-6-59-67.

10 Maxim V. Bochkov, Doctor of Technical Sciences, Professor, Center for Entrepreneurial Risks, St. Petersburg, Russia. E-mail: mvboch@cprspb.ru
11 Dmitry A. Vasinev, Ph.D. of Technical Sciences, Employee of the Academy of the Federal Guard Service of Russia, Orel, Russia. E-mail: vda33@academ.msk.rsnet.ru