Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет имени
первого Президента России Б.Н. Ельцина»

На правах рукописи

СИНАДСКИЙ Николай Игоревич

МЕТОДОЛОГИЯ СИНТЕЗА ИНТЕРАКТИВНОЙ СЕТЕВОЙ СРЕДЫ ДЛЯ КОМПЬЮТЕРНЫХ ПОЛИГОНОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
доктора технических наук

Екатеринбург – 2022

Работа выполнена в учебно-научном центре «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина».

Официальные оппоненты:

Козачок Александр Васильевич, доктор технических наук, доцент, ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», г. Орел, сотрудник Академии ФСО России;

Котенко Игорь Витальевич, доктор технических наук, профессор, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», г. Санкт-Петербург, главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности;

Лось Владимир Павлович, доктор военных наук, профессор, ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва, директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности

Защита состоится 27 декабря 2022 г. в 11:00 часов на заседании диссертационного совета УрФУ 2.3.12.13 по адресу: 620002, г. Екатеринбург, ул. Мира, 19, ауд. И-420 (зал Ученого совета).

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»,
https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=3976

Автореферат разослан «___»_____ 2022 года.

Ученый секретарь
диссертационного совета  Сафиуллин Николай Тахирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В условиях построения в Российской Федерации информационного общества и формирования глобального информационного пространства подавляющее большинство систем принятия решений и управления в ключевых областях экономики и государственного управления создается с использованием современных информационных технологий. В информационных системах с каждым годом продолжает увеличиваться объем хранимой информации, включая сведения в сферах политики и обороноспособности страны, экономики, науки и техники, а также персональных данных граждан. Вследствие этого возрастает важность обеспечения защищенности информационных систем (далее — ИС) и информационно-телекоммуникационных сетей (далее — ИТС) от нарастающих угроз информационного характера, которые могут быть реализованы злоумышленниками, постоянно совершенствующими арсенал используемых ими средств и устройств. В целях противодействия угрозам безопасности приняты Доктрина информационной безопасности Российской Федерации[1], в которой на основе анализа основных информационных угроз и оценки состояния информационной безопасности (далее — ИБ) определены стратегические цели и основные направления обеспечения ИБ с учетом стратегических национальных приоритетов Российской Федерации, и Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»[2], который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак. Создана и функционирует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), представляющая собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[3].

В большинстве крупных вузов технического профиля организована подготовка студентов по специальностям укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность». В федеральных государственных образовательных стандартах данной группы введены требования по применению при подготовке специалистов в качестве тренировочной базы учебно-научных компьютерных полигонов (киберполигонов), включающих учебные стенды, воспроизводящие сетевую инфраструктуру объектов ИТС. Актуальность создания киберполигонов определена Федеральным проектом «Информационная безопасность» национальной программы «Цифровая

[1] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

[2] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 12.07.2017 № 187-ФЗ.

[3] Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

экономика Российской Федерации»[4], в рамках которой предусмотрено выполнение работ по созданию киберполигона для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области ИБ и информационных технологий современным практикам обеспечения безопасности. Одной из задач учебно-научного компьютерного полигона является создание условий для проведения научных исследований в сфере обеспечения ИБ, в том числе для тестирования как защищенности ИТС в целом, так и отдельных средств защиты информации, среди которых выделяются технические, программные, программно-аппаратные и иные средства, обеспечивающие обнаружение, предупреждение и ликвидацию последствий компьютерных атак, а также реагирования на компьютерные инциденты.

Среди указанных средств основными являются системы обнаружения атак (системы обнаружения вторжений, далее — СОА), телекоммуникационное оборудование (далее — ТКО), системы анализа защищенности (далее — САЗ), а также информационно-аналитические системы безопасности (далее — ИАСБ). Указанную категорию средств будем называть сетевыми средствами защиты информации (далее — ССЗИ). При этом задача предупреждения компьютерных атак решается ТКО (межсетевыми экранами, маршрутизаторами и т.п.), предназначенным для блокирования компьютерных атак, и САЗ (сканерами безопасности), предназначенными для заблаговременного выявления уязвимостей, способствующих реализации компьютерных атак. Задачу обнаружения компьютерных атак решают СОА. Для расследования инцидентов ИБ и ведения аналитической работы применяются ИАСБ, осуществляющие поиск взаимосвязей между объектами различных информационно-телекоммуникационных сетей, в том числе IP-сетей, социальных сетей и сетей операторов сотовой связи. Некорректная работа СОА может привести к пропуску атакующего воздействия и получению нарушителем возможности оказать воздействие, наносящее ущерб компьютерной информации. Вывод из строя ТКО, обеспечивающего работу ИТС, может привести к существенным задержкам передачи данных, к частичным потерям данных и к полному прекращению информационного взаимодействия между узлами сети, и, таким образом, к нарушению функционирования ИТС как единой распределенной информационно-управляющей системы, что также может повлечь ущерб компьютерной информации. Для оценки степени защищенности ИТС в целом применяются САЗ, реализующие методики, использующие порядковые шкалы защищенности и процедуры, основывающиеся в основном на экспертных оценках степени выполнения требований безопасности, которые закреплены в стандартах или в руководящих документах соответствующих ведомств.

Особое значение имеет качество разработки и конфигурирования ССЗИ, которое может быть проверено в ходе тестирования с применением экспериментально-обучающих компьютерных полигонов. В силу чрезвычайной

[4] Паспорт федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28.05.2019 № 9))

сложности алгоритмов, лежащих в основе ССЗИ, и их программной реализации программные средства ССЗИ должны быть подвергнуты комплексному тестированию на этапах испытания, оценки и сертификации. Задача тестирования — убедиться, что алгоритмы и защитные механизмы функционируют в соответствии с документацией и предъявляемыми к ним требованиями, и что не существует очевидных способов обхода или разрушения защиты. Тестирование ССЗИ и объектов ИТС проводится, в частности, в процессе проведения мероприятий по анализу защищенности ИТС и ИС от компьютерных атак. Современные компьютерные атаки, использующие совокупности различных уязвимостей компьютерных систем, применяют нетривиальные подходы, однако оперируют определенным набором стандартных действий, связанных с направлением удаленному узлу информации, представленной в виде запроса, данных или команды. Результативность реакции ССЗИ на определенное воздействие зависит от состояния внешней для ССЗИ среды и конфигурирования ССЗИ с учетом характеристик сетевой среды. При этом стремительное развитие компьютерных технологий приводит к существенному изменению параметров сетевой среды, появлению новых протоколов и сетевых служб, новых массивов данных, циркулирующих в компьютерных сетях. Аналогично, расследование инцидентов ИБ требует анализа больших и разноплановых массивов данных, фиксируемых современными ССЗИ.

Известные компьютерные полигоны, а также методики тестирования ССЗИ, используемые при проведении сертификационных испытаний и мероприятий по анализу уязвимостей, не позволяют в полной мере моделировать в процессе тестирования условия, существующие при проведении современных комплексных воздействий (комплексных атак), что снижает достоверность результатов мероприятий по анализу уязвимостей ИТС в целом. Кроме того, ряд законодательных ограничений не позволяет применять для тестирования реальные массивы данных, циркулирующие в действующих компьютерных системах. Современные компьютерные полигоны должны быть оснащены полноценными имитаторами, создаваемыми на основе перспективных методов искусственного интеллекта[5], позволяющими моделировать условия не только сети, работающей в штатном режиме, но и условия критической нагрузки на сеть, учитывая при этом вариативность и интенсивность обновления технологий, протоколов и средств построения ИТС, а также обеспечивать интерактивность сетевой среды (изменение сетевой обстановки в зависимости от выполняемых обучаемыми действий).

Таким образом, возникает потребность в методиках и практических инструментах тестирования ССЗИ, которые позволят моделировать комплексные атакующие воздействия и условия их проведения в реальных ИТС.

В образовательном процессе потребность при изучении методик тестирования ССЗИ и защищенности ИТС в целом в работе в условиях реальных сетей не может быть реализована без компьютерных полигонов. Задачей компьютерных полигонов в образовательной сфере по направлению ИБ является создание условий

[5] Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена указом Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации".

для формирования практико-ориентированных компетенций слушателей в части тестирования ССЗИ, выявления уязвимостей ИТС и ИС, обнаружения компьютерных атак и реагирования на инциденты ИБ. Создаваемые условия должны на основе автоматизированной обучающей системы (далее — АОС) максимально реалистично имитировать состояние внешней для ССЗИ сетевой среды. Сетевая среда имитируется в двух состояниях — состояние штатного (нормального) воздействия на ССЗИ и состояние нештатного (аномального, критического) воздействия. В состав аномального воздействия должны быть включены комплексные ситуационные задачи (тесты), предполагающие выявление инцидентов ИБ, их идентификацию и формирование отчетных аналитических документов обучающимися. Должен быть сформирован полный цикл профессиональных компетенций специалистов по расследованию инцидентов ИБ в ИТС, от обнаружения комплексной компьютерной атаки, выявления ее источников, уязвимостей, способствовавших ее реализации, до локализации субъектов атаки (инициаторов и исполнителей) на основе выявления взаимодействия пользователей в сетях связи (рисунок 1).

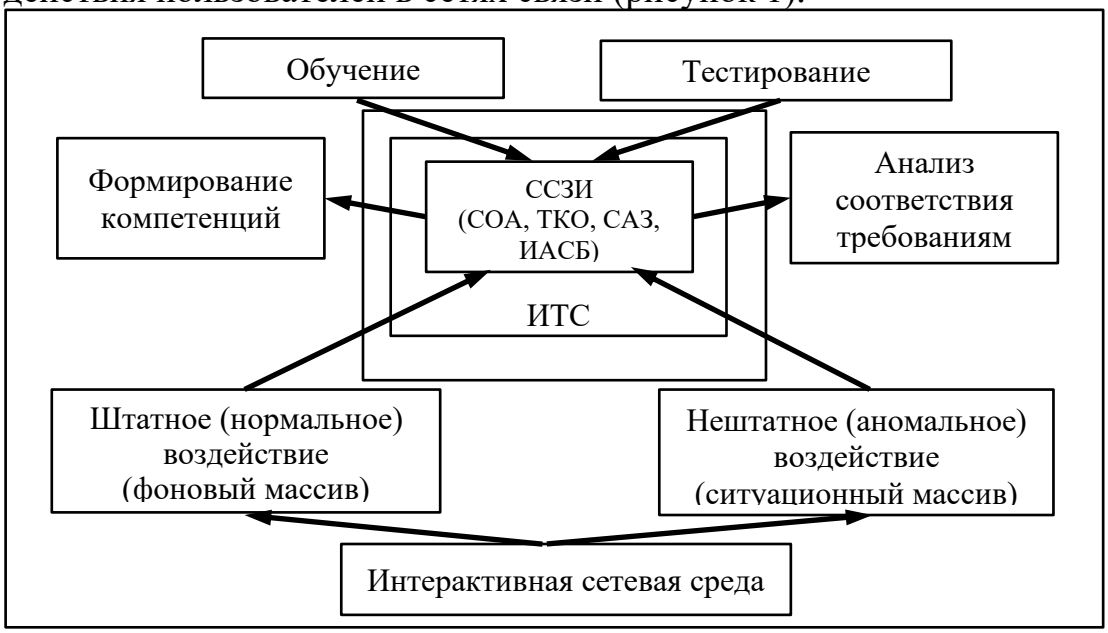

Рисунок 1. АОС в сфере ИБ

Реализация задач по обеспечению безопасности ИТС и ИС требует адекватного развития теоретических основ имитационного моделирования сетевой среды в процессе тестирования ССЗИ. В настоящее время *отсутствуют комплексные модели* синтеза интерактивной сетевой среды, предназначенные для проведения тестирования ССЗИ с учетом вариативности среды и атакующего воздействия, а также научно обоснованная *методология*[6] синтеза интерактивной[7] сетевой среды для компьютерных полигонов. Наблюдается объективное противоречие между потребностями по комплексному тестированию ССЗИ с учетом непрерывного развития информационных технологий и современных ИТС и существующим научно-

[6] Методология — система методов, применяемых в какой-либо науке.
[7] Интерактивность — способность информационной системы к активному и адекватному реагированию на действия пользователей.

методическим и математическим обеспечением систем и комплексов, реализующих тестирование ССЗИ, не удовлетворяющим указанным потребностям. Следствием неразрешенности этого противоречия является объективная необходимость теоретического обобщения и развития методов математического моделирования интерактивной сетевой среды, алгоритмов и программного обеспечения, интегрируемых в компьютерные полигоны, предназначенные для тестирования ССЗИ с учетом вариативности среды и комплексности атакующего воздействия.

Таким образом, разработка и внедрение научно обоснованной методологии имитационного моделирования при синтезе интерактивной сетевой среды, являющейся совокупностью методов, моделей, алгоритмов и программного обеспечения, позволяющей автоматизировать процессы синтеза массивов данных для компьютерных полигонов с учетом вариативности сетевой среды и комплексности атакующего воздействия, с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ, является актуальной научной проблемой.

Степень разработанности темы исследования. Построение компьютерных полигонов в сфере ИБ — активно обсуждаемая проблема, над решением которой работают многие отечественные и зарубежные исследователи. Разработаны многочисленные отдельные методики и алгоритмы для синтеза телетрафика, генерации потока пакетов, для имитации атакующего воздействия, оценки реалистичности синтезируемых массивов, выявления аномалий в сетевом трафике, анализа взаимодействия абонентов в сетях связи. Среди исследователей, создавших наиболее важные труды в данном направлении, следует отметить работы:

– в области алгоритмов выявления аномалий — А.А. Захарова, А.М. Ивашко, Д.Ю. Гамаюнова, П.Д. Зегжды, А.В. Козачка, И.В. Котенко, П.С. Ложникова, В.П. Лося, В.В. Никонова, В.В. Платонова, С.В. Поршнева, В.В. Райха, П.О. Семенова, С.Г. Синева, М.В. Степашкина;

– в области моделирования и синтеза сетевого трафика компьютерных атак — Н.А. Гайдамакина, А.С. Коллерова, Д.А. Хорькова, М.В. Щербы;

– в области создания самоподобного телетрафика — А.Н. Назарова, К.И. Сычева, В. Гароуси (V. Garousi), А. Авритзера (A. Avritzer), Е. Вейюкера (E.J. Weyuker), Дж. Жанга (J. Zhang), В. Лиланда (W. Leland), З. Лю (Z. Liu), Б. Мандельброта (B.B. Mandelbrot), В. Виллингера (W. Willinger), Ч.С.Д. Янга (C.S.D. Yang);

– в области методов и алгоритмов создания и тестирования ССЗИ — Ю.Д. Королькова, В.В. Липаева, А.Н. Соколова, С.С. Титова, Н. Пукетцы (N.J. Puketza), П. Липпмана (R.P. Lippmann), К. Кендалла (K.R. Kendall), Д. Вебера (D. Weber), Дж. Хейнса (J.W. Haines), Г. Шипли (G. Shipley), Дж. Снайдера (J. Snyder).

Отдельные аналитические модели и подходы к синтезу сетевого трафика, описываемые в известных работах, являются узкоспециализированными и сложны с точки зрения адаптации под конкретные виды задач по организации тестирования ССЗИ, что не позволяет создать комплексное научно обоснованное решение по автоматизации процессов синтеза массивов данных для тестирования ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия.

Объект исследования — процессы анализа защищенности информационно-телекоммуникационных систем и тестирования сетевых средств защиты информации, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты.

Предмет исследования — совокупность методов, моделей и алгоритмов синтеза интерактивной сетевой среды для компьютерных полигонов в сфере ИБ.

Границы исследования охватывают практическую реализацию теоретических положений исследования в отношении ССЗИ четырех категорий: СОА, ТКО, САЗ и ИАСБ.

Научная проблема диссертационного исследования заключается в необходимости создания научно-методического инструментария проектирования компьютерных полигонов в сфере ИБ на базе интерактивной сетевой среды, включая методы, модели, алгоритмы и программное обеспечение. Решение этой проблемы, имеющее важное значение для народного хозяйства, лежит в плоскости разработки общей методологии и частных методик, а также аппаратно-программного инструментария автоматизации процессов синтеза массивов данных для анализа защищенности ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия, с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ.

Исходя из сущности решаемой в диссертации научной проблемы, теоретическая цель исследования заключается в развитии научно-методического аппарата исследования вопросов обеспечения безопасности ИТС и ИС. Прагматической целью работы является создание условий для повышения показателей защищенности объектов ИТС и ИС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования.

Цель диссертационной работы — разработка научно-методического инструментария имитационного моделирования при синтезе интерактивной сетевой среды для компьютерных полигонов в сфере ИБ для обеспечения высокого уровня защищенности объектов ИТС и ИС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования.

Для достижения указанной цели в диссертации решаются следующие **частные научные задачи**, вытекающие из декомпозиции научной проблемы:

1. Систематизация и анализ современного состояния теории и практики, технологий, методов и средств анализа защищенности ССЗИ на примере СОА и ТКО, выделение основных характеристик, подлежащих тестированию с точки зрения возможности выявления комплексных компьютерных атак и уязвимостей ИТС и ИС, формирование требований к составу и содержанию массивов тестовых данных (сетевого трафика) при создании компьютерных полигонов в сфере ИБ.

2. Разработка комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере ИБ, включающего методы, модели и алгоритмы.

3. Разработка модели ССЗИ как объекта тестирования, учитывающей при синтезе тестовых массивов параметры сетевого трафика заданной сетевой среды функционирования с учетом вариативности сетевых сред в ИТС.

4. Разработка метода синтеза атакующих (ситуационных) массивов данных, где ситуационные задачи (комплексные атаки) представляют собой формируемую по определенным правилам последовательность элементарных тестовых воздействий, распределенных по времени и в пространстве сетевых адресов.

5. Разработка алгоритма, обеспечивающего автоматизацию процесса выявления пороговых параметров устойчивости ССЗИ на примере ТКО к компьютерным атакам типа «отказ в обслуживании».

6. Разработка моделей, алгоритмов и программного обеспечения синтеза массивов фоновых данных для тестирования СОА, ТКО и ИАСБ с обоснованием методов анализа реалистичности синтезируемых тестовых массивов.

7. Разработка алгоритмов и программных средств для создания учебно-научного компьютерного полигона по расследованию инцидентов ИБ.

Научная новизна заключается в создании научно-методического инструментария имитационного моделирования при синтезе интерактивной сетевой среды для компьютерных полигонов, впервые представленного в виде методологии, основанной на ряде разработанных методов, моделей, алгоритмов и аппаратно-программного инструментария автоматизации процессов синтеза массивов данных для тестирования ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия, с целью своевременного обнаружения, предупреждения и ликвидации последствий, компьютерных атак, а также реагирования на инциденты ИБ.

Теоретическая значимость. Создан новый научно-методический аппарат, имеющий существенное значение для развития методов, моделей, алгоритмов и программных средств обеспечения ИБ. Разработанный научно-методический аппарат впервые представлен в виде методологии синтеза интерактивной сетевой среды для компьютерных полигонов, включающей метод синтеза массивов фоновых данных основанный на модели интерактивной сетевой среды функционирования ССЗИ, матричной модели хранения статистических характеристик сетевой среды функционирования ССЗИ и процедуре анализа реалистичности тестовых массивов условно-реальных данных; метод синтеза массивов ситуационных задач (атакующего воздействия) включающий теоретико-графовую модель распространения атакующего воздействия в иерархической системе уязвимых объектов, динамическую модель комплексной атаки с применением алгоритмов сетей Петри и эволюционно-генетические алгоритмы для синтеза массивов атакующего воздействия; имитационно-статистический метод синтеза массивов условно-реальных данных о взаимодействии пользователей ИТС, основанный на пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС.

Практическая значимость работы заключается в том, что новое техническое решение по созданию учебно-научных компьютерных полигонов позволяет автоматизировать процессы синтеза тестовых массивов данных и сетевого трафика для выявления неизвестных уязвимостей при тестирования ССЗИ с учетом вариативности внешней сетевой среды и комплексности атакующего воздействия, позволяет организовать практико-ориентированное обучение специалистов по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а

также по реагированию на инциденты ИБ, что вносит значительный вклад в повышение безопасности ИТС и ИС.

Положения, выносимые на защиту (основные научные результаты исследования):

1. Комплексный метод синтеза интерактивной сетевой среды для компьютерных полигонов, основанный на выделении структурных элементов сетевого трафика реальных сетей с учетом функционального предназначения ССЗИ, учитывающий вариативность ИТС и динамику развития ситуационных задач, применяющий для массивов фонового сетевого трафика матричную модель, хранящую статистические распределения характеристик сетевой среды функционирования, осуществляющий синтез атакующих (ситуационных) массивов данных на основе алгоритмов сетей Петри, где ситуационные задачи представляют собой формируемую по определенным правилам последовательность элементарных тестовых воздействий, обеспечивает комплексность и вариативность тестового воздействия при оценке эффективности ССЗИ[8] [3, 6, 7].

2. Впервые предложенный имитационно-статистический метод синтеза массивов условно-реальных данных, основанный на пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС, применяющий модели синтеза сложных сетей, матричную модель хранения статистических характеристик сетевых сред и алгоритмы сетей Петри для формирования ситуационных задач, позволяет формировать массивы данных для тестирования ИАСБ[8] [2–4, 8, 10].

3. Метод синтеза атакующего воздействия и ситуационных задач, основанный на применении предложенной теоретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов для формирования статической структуры графа атак и алгоритмов сетей Петри для синтеза динамической составляющей атакующего воздействия, позволяет формировать массивы ситуационных задач при тестировании ССЗИ[8] [5, 6, 13].

4. Комплекс моделей, методик и алгоритмов для тестирования устойчивости ССЗИ к сетевым атакам типа «отказ в обслуживании», основанный на применении эволюционно-генетического подхода и метода синтеза интерактивной сетевой среды для компьютерных полигонов, включающий оригинальную модель интерактивной сетевой среды функционирования ССЗИ, учитывающую статические и динамические характеристики ИТС на сетевом, транспортном и прикладном уровнях сетевого взаимодействия, позволяет осуществлять автоматизированное тестирование ССЗИ и выявлять уязвимости ССЗИ к сетевым атакам, приводящим к нарушению производительности ССЗИ при определенных сочетаниях параметров входных данных, не являющихся пороговыми[9] [1, 9, 11–18].

Методология и методы исследования: теория вероятностей, математическая статистика, теория нечетких множеств и нечеткой логики, теория графов, теория матриц, аппарат сетей Петри, эволюционно-генетический аппарат, имитационное моделирование.

[8] Пункт 11 паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность
[9] Пункт 6 паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Достоверность и обоснованность полученных результатов подтверждается корректностью использованного математического аппарата и теоретических обоснований; непротиворечивостью полученных результатов известным решениям; достаточно широкой апробацией результатов диссертации; использованием методик, проверенных экспериментами и внедренных в действующие образцы учебных стендов компьютерного полигона по расследованию инцидентов ИБ.

Апробация результатов исследования. Основные результаты диссертации докладывались и обсуждались на Международных и Всероссийских научно-технических и научно-практических конференциях и семинарах с 2002 по 2020 годы, в том числе:

— Всероссийской научно-практической конференции «Информационная безопасность» (г. Екатеринбург, 2002 г.);

— V, VI, XI, XII, XIV, XV, XVI, XVII Всероссийских научно-практических конференциях «Безопасность информационного пространства» (гг. Екатеринбург, Курган, Тюмень, Челябинск, 2005, 2006, 2012, 2013, 2015, 2016, 2017, 2018 г.);

— 12 и 16-ой международной научно-технической конференции «Современные проблемы радиоэлектроники и телекоммуникаций, РТ–2016, РТ–2020» (г. Севастополь, 2016, 2020 г.);

— VI Международной научной конференции «Математическое и компьютерное моделирование», посвященной памяти Б.А. Рогозина (Омск, 2018 г.);

— II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (FISP–2020, г. Ставрополь, 2020 г.);

— Уральском симпозиуме биомедицинской инженерии, радиоэлектроники и информационных технологий (USBEREIT, г. Екатеринбург, 2019, 2020 г.).

Реализация результатов. Диссертация является обобщением результатов исследований, проводившихся автором в течение последних 20 лет в процессе учебно-научной деятельности по направлению «Информационная безопасность» в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». Результаты исследования внедрены в учебно-научный компьютерный полигон по расследованию инцидентов ИБ, развернутый на базе учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», использованы при построении обучающих стендов в составе учебных центров ООО «Институт Радиоэлектронных Систем» и Екатеринбургского научно-технического центра ФГУП «НПП Гамма». Разработанные методики, программное обеспечение и экспериментальные стенды были также использованы при проведении оценки защищенности образцов ТКО, применяемых в автоматизированных системах управления технологическими процессами, в ООО «Уральский центр систем безопасности».

Публикации. По результатам исследований, представленных в диссертации, опубликовано более 50 печатных работ. Основные научные результаты диссертации отражены в 18 работах, из них 14 статей, опубликованных в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ,

включая 4 статьи в изданиях, входящих в международные цитатно-аналитические базы Scopus и Web of Science; 4 свидетельства о государственной регистрации программы для ЭВМ.

Соответствие диссертации паспорту научной специальности. Представленная диссертация соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность: пункту 6 «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях» и пункту 11 «Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты».

Личный вклад автора. Все результаты исследований, составляющие основное содержание диссертации, получены автором самостоятельно. Разработка элементов учебно-научного компьютерного полигона по расследованию инцидентов ИБ велась на протяжении ряда лет несколькими авторскими коллективами путем выполнения ряда выпускных квалификационных и диссертационных работ, в которых автор выступал научным руководителем. Вклад соавтора в совместных работах с Н.А. Гайдамакиным состоит в обсуждении постановки научных задач и оценок полученных результатов. В работы, выполненные в соавторстве с учениками (А.В. Агафонов, В.В. Богданов, Р.В. Гибилинда, А.Р. Зайникаев, А.А. Муратов, И.А. Семенищев, П.В. Сушков, А.Н. Синадский, М.Н. Синадский), диссертантом внесен основной вклад, касающийся выбора научных методов и средств, синтеза математических моделей и алгоритмов, постановки экспериментов по проверке их адекватности и интерпретации результатов исследований.

Структура и объем диссертации. Диссертация состоит из введения, 4 глав, заключения, списка сокращений и условных обозначений и списка литературы. Общий объем диссертации 298 страниц. Диссертация содержит 72 рисунка и 9 таблиц. Библиография включает 258 наименований на 27 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе представлено аналитическое исследование, в качестве модели угроз даны понятие и расширенная систематика комплексных сетевых компьютерных атак, которые рассматриваются как совокупная последовательность элементарных атакующих воздействий. Введены объекты тестирования — ССЗИ (СОА, ТКО, САЗ и ИАСБ) в качестве элементов обеспечения безопасности ИТС (рисунок 2). Приведены основные свойства каждого типа ССЗИ, характеристики, подлежащие тестированию, и параметры синтеза соответствующих массивов данных (рисунок 3). Представлен обзор известных технологий, методов и средств тестирования ССЗИ на примере СОА и ТКО. Рассмотрены и классифицированы известные реализации синтеза фонового сетевого трафика, показаны их достоинства и недостатки.

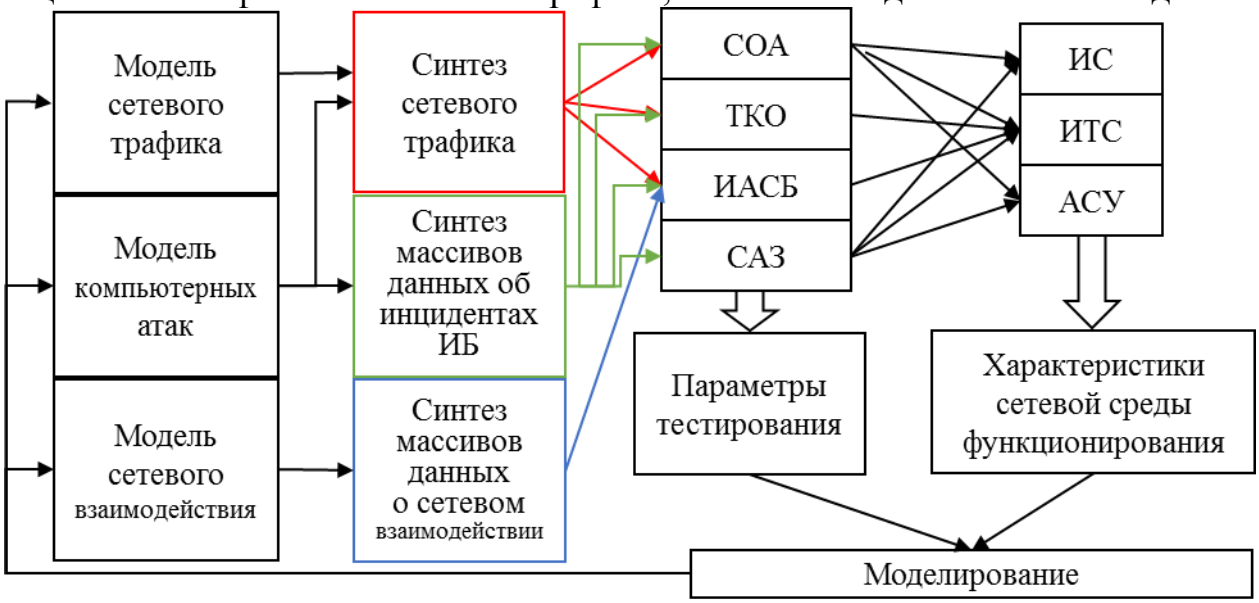

Рисунок 2. ССЗИ как объекты тестирования

При анализе известных подходов к тестированию ССЗИ выявлен ряд противоречий, требующих разрешения:

— для анализа наличия уязвимостей в ПО ССЗИ и конфигурировании ИТС недостаточным является выявление уязвимостей только с помощью сканеров безопасности, анализ защищенности сетевых систем необходимо проводить и с применением так называемых эксплойтов — программ, выполняющих атакующее сетевое воздействие с использованием определенных уязвимостей, однако ввиду их вредоносности не представляется возможным с помощью подобного ПО выполнить всеобъемлющее тестирование ССЗИ в реальной ИТС;

— натурное тестирование образцов ТКО с применением образцов тестового сетевого трафика является общепринятым и единственным эффективно реализуемым подходом к решению данной задачи. Во избежание нарушения работоспособности ИТС тестирование должно производиться в специально подготовленной тестовой сетевой среде;

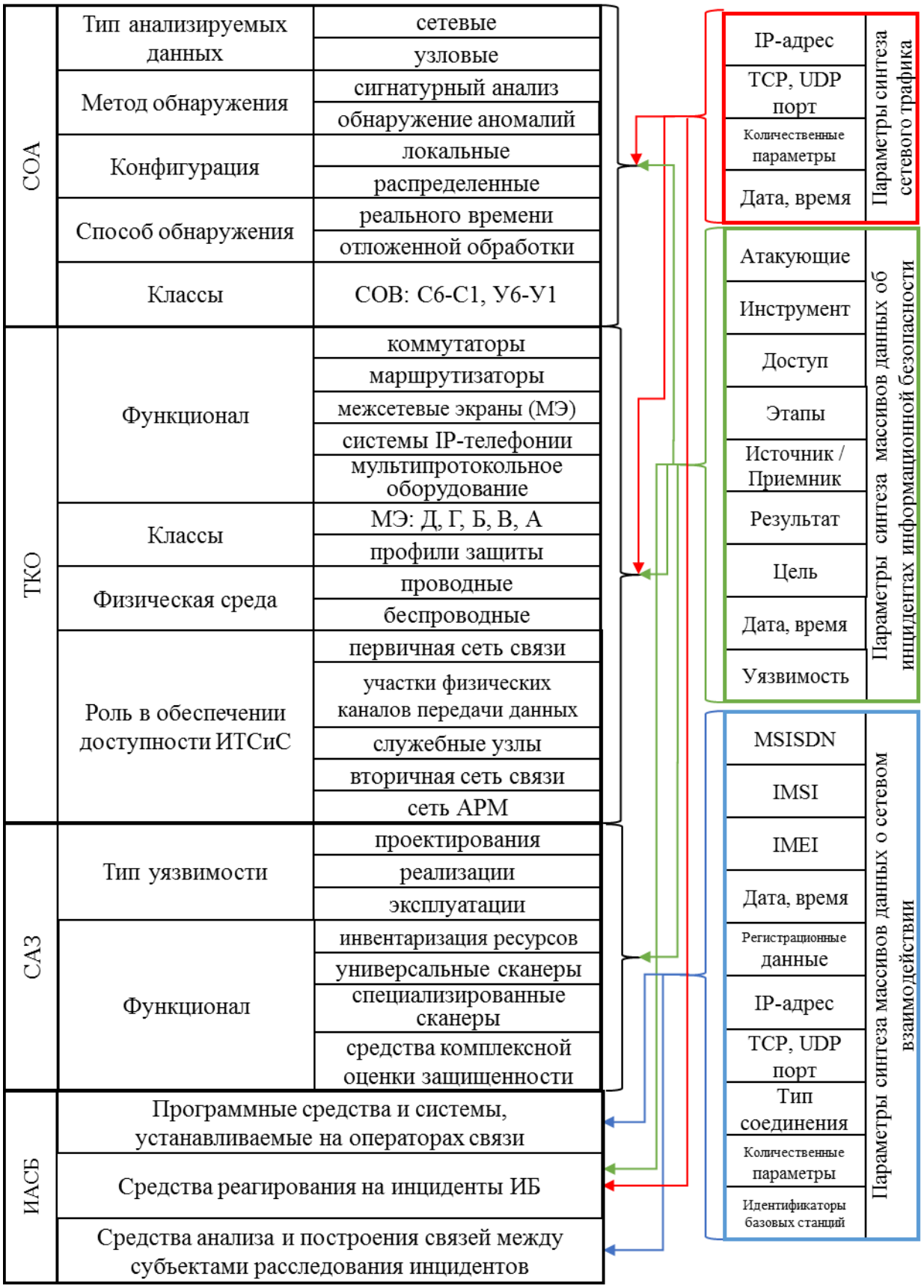

Рисунок 3. Классификация ССЗИ с учетом параметров синтеза массивов данных

— возможность успешной реализации компьютерных атак в большинстве случаев связана с рядом параметров сетевой среды функционирования ССЗИ. При

этом существующие методики оценки защищенности и тестирования ССЗИ не учитывают вариативность сетевой среды.

Очевидным решением указанных противоречий является тестирование ССЗИ на специально разработанных стендах в составе компьютерных полигонов на основе моделей сетевой среды и атакующего воздействия. Основными недостатками известных подходов к организации тестирования ССЗИ, усложняющими организацию стенда, являются: значительное количество узлов-жертв и атакующих узлов (в силу вариативности и многокомпонентности комплексного атакующего воздействия), ограничения по количеству атак (сложность подбора готовых к выполнению программных модулей и сценариев атак), сложность автоматизации запуска атакующего воздействия (невозможность автоматизированного циклического выполнения комплексных атак в силу необходимости участия человека-оператора), сложность регистрации момента осуществления комплексной атаки. В связи с указанными выше недостатками требуется новый подход к организации атакующего воздействия в задаче тестирования ССЗИ, основанный на формировании базы данных тестовых атак в виде массивов сетевого трафика и на математической модели сетевой среды функционирования ССЗИ, которая должна учитывать параметры сетевого трафика заданной сетевой среды функционирования. При этом должно обеспечиваться сходство синтезируемого тестового сетевого трафика с трафиком, циркулирующим в сетевой среде функционирования ССЗИ, а также учитываться свойство самоподобия сетевого трафика существующих компьютерных сетей.

Показано, что для обеспечения безопасности ИТС требуются надежные ССЗИ, гарантировать качество которых возможно на основе всеобъемлющих тестовых испытаний. В свою очередь, для тестирования ССЗИ необходимы стенды, в которых на основе имитационного моделирования и синтеза массивов тестовых данных должна быть создана имитационная среда функционирования реальных ИТС.

Во второй главе диссертации описана разработанная **методология синтеза интерактивной среды** для компьютерных полигонов в сфере ИБ. Для решения поставленной в диссертации научной проблемы разработан научно-методический инструментарий проектирования компьютерных полигонов в сфере ИБ на базе интерактивной сетевой среды, позволяющий осуществлять автоматизацию процессов синтеза массивов данных для анализа защищенности ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия, с целью своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на инциденты ИБ на объектах ИТС и ИС. В главе раскрываются структура и основные компоненты комплексного метода синтеза интерактивной среды, который предусматривает воздействие на тестируемый образец ССЗИ комбинации двух видов массивов данных: фонового и атакующего, для синтеза каждого из которых разработан собственный метод (рисунок 4).

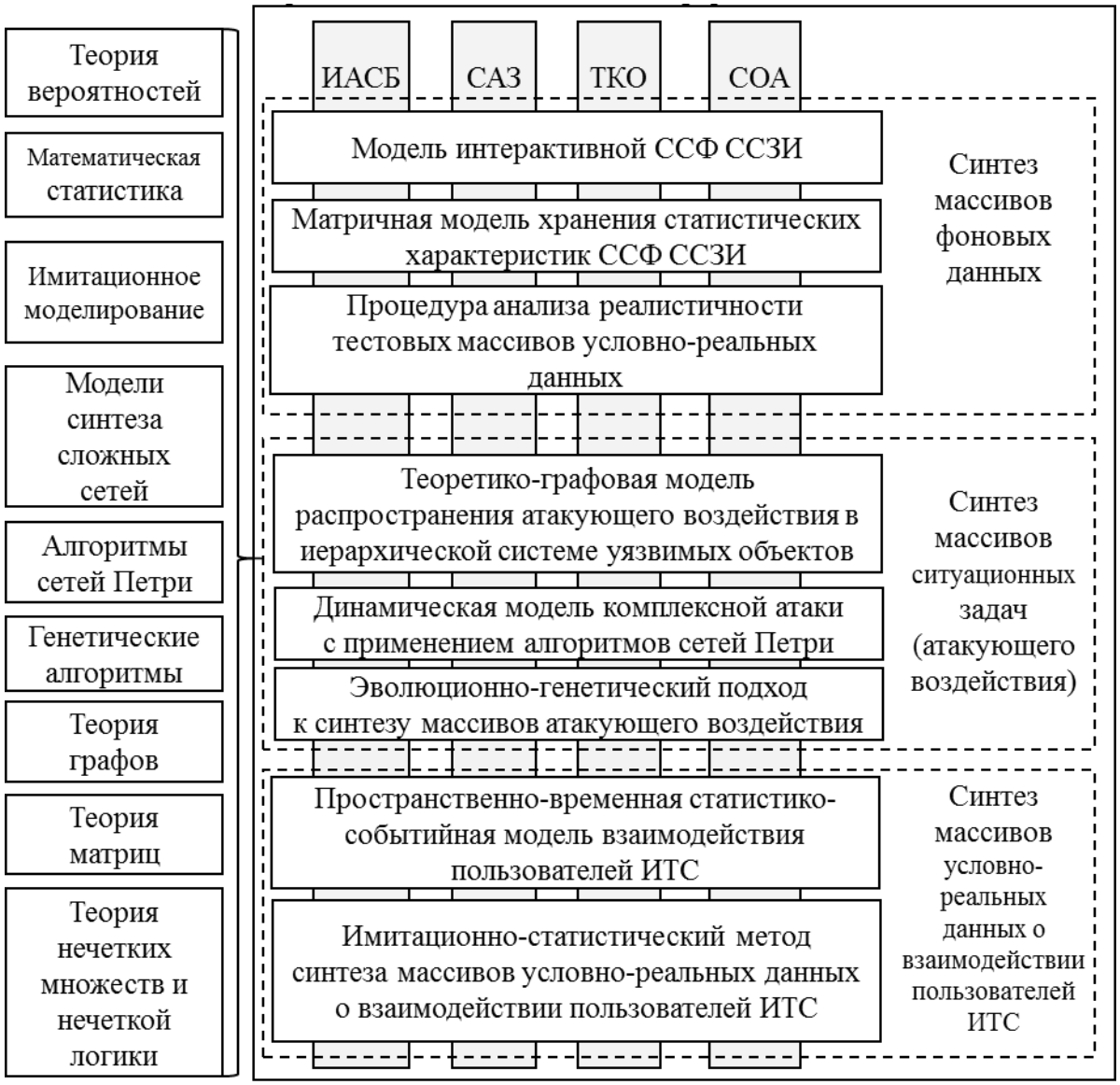

Рисунок 4. Схема компонентов комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере ИБ

Метод синтеза массивов фоновых данных основан на модели интерактивной сетевой среды функционирования (далее — ССФ) ССЗИ, матричной модели хранения статистических характеристик ССФ ССЗИ и процедуре анализа реалистичности тестовых массивов условно-реальных данных. Метод синтеза массивов ситуационных задач (атакующего воздействия) включает теоретико-графовую модель распространения атакующего воздействия в иерархической системе уязвимых объектов, динамическую модель комплексной атаки с применением алгоритмов сетей Петри и эволюционно-генетические алгоритмы для синтеза массивов атакующего воздействия. Имитационно-статистический метод синтеза массивов условно-реальных данных о взаимодействии пользователей ИТС основан на пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС.

В процессе разработки метода использованы теория вероятностей, математическая статистика, имитационное моделирование, модели синтеза сложных сетей,

аппарат сетей Петри, эволюционно-генетический аппарат, теория графов, теория матриц, теория нечетких множеств и нечеткой логики.

Тестирование ССЗИ осуществляется по трем основным направлениям: анализ выполнения требований к производительности ССЗИ, предъявляемых нормативными документами; выявление уязвимостей в программном обеспечении ССЗИ; анализ корректности реализации аналитических алгоритмов и методик, встроенных в ССЗИ. Процесс тестирования ССЗИ осуществляется в изолированной сетевой среде, максимально приближенной к условиям функционирования ССЗИ с учетом вариативности параметров ИТС. Для тестирования ССЗИ применяются специализированные экспериментальные стенды, позволяющие моделировать ССФ ССЗИ. ССФ должна, с одной стороны, быть идентичной условиям реальных сетей, с другой — учитывать функциональное предназначение тестируемого ССЗИ и позволять тестировать критичные к безопасности свойства ССЗИ. Модель ССФ должна учитывать характеристики ССЗИ, значимые для тестирования. Для получения характеристик выделяются свойства объекта тестирования, подлежащие тестированию. Тестовая среда, формируемая в соответствии с ССФ, должна соответствовать сетевой среде, наблюдаемой в реальных условиях. Процесс синтеза сетевого трафика для тестирования ССЗИ состоит из нескольких этапов (рисунок 5). Синтезируемый тестовый сетевой трафик представлен двумя компонентами: массив фоновых данных и массив данных атакующего воздействия (ситуационный массив). При синтезе тестирующего массива и его последующей генерации в канал связи стенда тестирования ССЗИ происходит комплексирование с учетом пространственно-временных параметров фонового и атакующего массивов в единый массив с возможностью изменения их соотношения с целью выявления граничных условий производительности ССЗИ. С целью обеспечения повторяемости эксперимента фоновый массив должен генерироваться по определенным закономерностям, учитывающим условия тестирования. Для синтеза фонового массива проводится анализ характеристик ССЗИ, подлежащих тестированию, формальное описание сетевого трафика в соответствии с моделью и выбор характеристик такой ССФ, которая удовлетворяет параметрам тестирования. Ввиду неэффективности хранения больших объемов информации и значительного разнообразия характеристик различных ИТС синтез фонового трафика осуществляется на основе ранее сохраненных статистических характеристик реального трафика. Для накопления соответствующих характеристик осуществляется статистический анализ трафика реальных ИТС, в которых применяются образцы ССЗИ, и характеристик трафика в сетях операторов связи, что не противоречит ФЗ «О связи». Целесообразно осуществлять запись значимых для последующей генерации характеристик трафика для их компактного хранения, для чего применяется матричная модель хранения характеристик ССФ в виде базы данных.

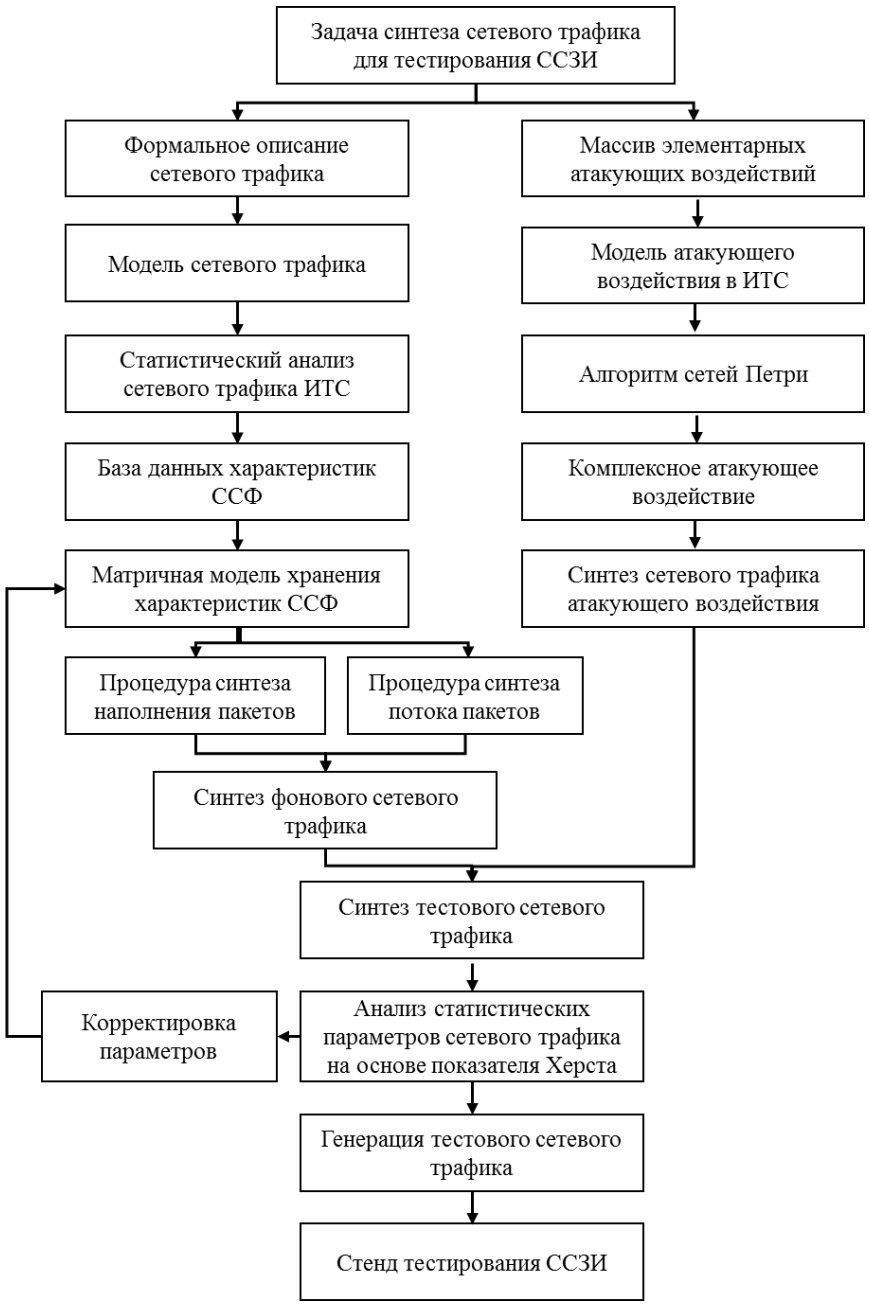

Рисунок 5. Этапы синтеза сетевого трафика

В рамках матричной модели характеристики ССФ как совокупности потоков сетевого обмена представлены в виде набора векторов, описывающих отдельные статистические свойства потока. Совокупность всех потоков в ИТС хранится в виде матрицы, строки которой являются проиндексированными векторами характеристик потоков. Особенностью матричного представления является возможность операций анализа характерных свойств потоков с помощью стандартных матричных операторов. Накопленная база данных статистических характеристик ССФ позволяет имитировать ИТС различных конфигураций.

Далее синтез массивов осуществляется на основании характеристик, заложенных в матричной структуре.

Применяются выбранная статистическая модель и соответствующая видам ИТС и тестируемых ССЗИ модель соединений. При синтезе фонового трафика учитываются как статистические распределения характеристик потока пакетов, так и наполнение области данных сетевых пакетов. Формирование области данных обеспечивается на основе алгоритмов, применяющих цепи Маркова[10] для генерации массивов текстовых строк.

Особенностями синтезируемого фонового сетевого трафика являются:

— присутствие в нем различных сетевых пакетов и различных сетевых протоколов, актуальных для компьютерных сетей различного типа;

[10] Цепь Маркова — последовательность случайных событий, где вероятность наступления каждого события зависит от состояния, достигнутого в предыдущем событии, широко применяется для генерации текстов, что определяет возможность использования в задаче формирования области данных сетевых пакетов.

— соответствие формальному описанию сетевых протоколов, тестируемым характеристикам ССЗИ определенного типа и трафику реальных ИТС.

Проводится анализ соответствия синтезируемых массивов реальному трафику ИТС, в качестве основного показателя соответствия используется общепринятое свойство самоподобия телетрафика, для измерения степени соответствия используется известный показатель Херста *H* (Hurst parameter), значения которого находятся в диапазоне от 0,5 до 1. Равенство этого коэффициента 0,5 указывает на отсутствие самоподобия, а близость к 1 — на проявление фрактальных свойств.

В случае тестирования параметров производительности ССЗИ, а также тестирования на наличие ранее неизвестных уязвимостей, связанных с некорректной обработкой различных аномалий в сетевом трафике, при синтезе применяется генетический алгоритм[11], позволяющий на основе исходной статистической модели осуществить варьирование отдельными характеристиками трафика.

Атакующее воздействие (ситуационные задачи) рассматривается как совокупность характеристик внешней среды, обладающая определенными закономерностями или сигнатурами, и состоит из тестов двух видов: для анализа корректности реализованных аналитических алгоритмов и для анализа производительности ССЗИ. Ситуационный (атакующий) массив данных содержит набор тестовых задач, предназначенных для выявления уязвимостей ССЗИ, в том числе возможных сбоев при аналитической обработке ССЗИ различных пороговых значений и комбинаций в анализируемых данных. Массив атакующего воздействия хранится в компактном в виде как набор характеристик сетевой среды.

Для анализа корректности реализованных алгоритмов и методик выделяются типовые аналитические методики (типовые комплексные атаки), для каждой формируется набор ситуационных задач (тестов). Синтез атакующих (ситуационных) массивов данных осуществляется на основе алгоритмов сетей Петри[12], где комплексные ситуационные задачи (далее — КСЗ) представляют собой формируемую по определенным правилам последовательность элементарных тестовых (атакующих) воздействий (далее — ЭТВ) как событий, распределенных по времени (рисунок 6). Для хранения типовых ЭТВ применяются шаблоны, содержащие, например, набор пакетов сетевой атаки. Исходный массив типовых ЭТВ формируется путем анализа известных атак на ИТС, на основе известных сценариев атакующего воздействия, кроме того, может формироваться аналитиком, проводящим тестирование. На основе пространственно-временной модели и алгоритмов сетей Петри формируется совокупность комплексных ситуационных задач. Особенностями трафика атакующего воздействия являются полное покрытие вариантами тестового воздействия всех видов сетевых компьютерных атак (ситуационных задач), характерных для тестируемого типа ССЗИ.

---

[11] Генетический алгоритм — это эвристический алгоритм поиска на основе случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе, широко используемый для решения задач оптимизации, в том числе может применяться в процессе подбора параметров массивов тестовых данных с целью выявления уязвимостей ССЗИ.

[12] Алгоритмы сетей Петри — аппарат моделирования синхронно-асинхронных распределенных систем и процессов, активно используемый для моделирования динамических дискретных систем, что обусловливает их применение в задаче синтеза атакующего воздействия.

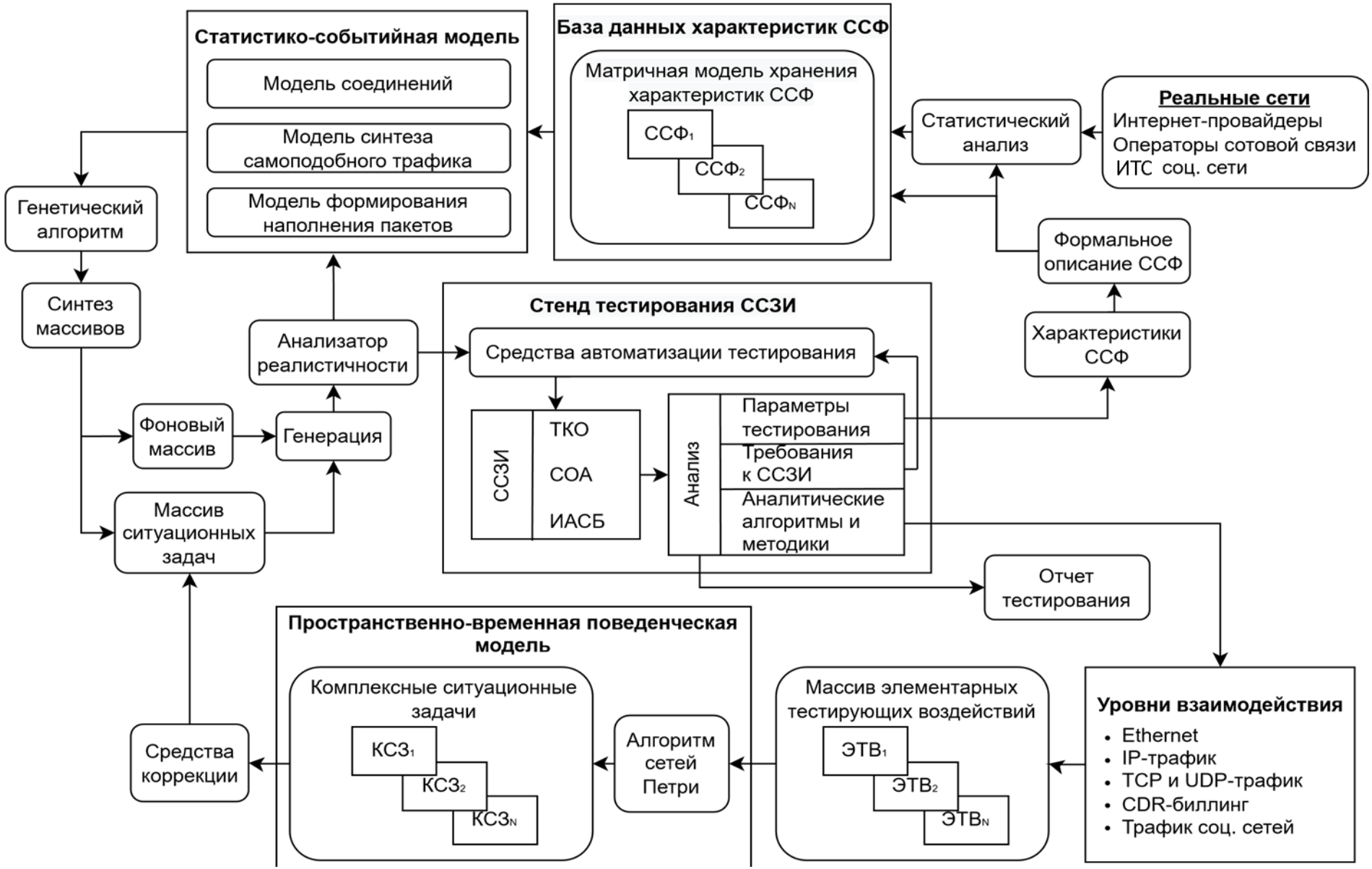

Рисунок 6. Схема взаимодействия компонентов метода синтеза интерактивной сетевой среды

Алгоритм комплексирования позволяет объединять данные фонового массива и массива ситуационных задач по пространству (адресному и географическому) и времени. Объединенный массив проходит анализ на самоподобие, при положительном результате осуществляется его передача на соответствующий стенд, где функционирует средство автоматизации тестирования.

С целью определения границ устойчивости ССЗИ к атакующему воздействию (тесты на оценку производительности) применяются средства автоматизации тестирования, которые учитывают характеристики сетевого трафика на входе и на выходе ССЗИ и осуществляют подбор тех характеристик атакующего воздействия, которые могут привести к нарушению функциональных возможностей ССЗИ. С целью поиска новых уязвимостей ССЗИ, заключающихся в сбоях при определенных сочетаниях параметров внешней среды, целесообразна автоматизация процесса тестирования как поиск граничных (пороговых) значений атакующего воздействия. Автоматизированная методика тестирования ССЗИ предназначена для выявления граничных для производительности ССЗИ значений параметров, определяющих структуру и статистические характеристики сетевого трафика компьютерных атак. В качестве основы для данной методики применяется эволюционно-генетический подход, позволяющий производить тестирование ССЗИ по схеме «черного ящика». Способ анализа результатов работы генетического алгоритма с применением кластерного анализа с использованием алгоритма сдвига среднего позволяет обобщить и очертить границы значений параметров атакующего воздействия, приводящего к превышению заданных требованиями к ССЗИ пороговых значений параметров производительности.

Разработанный комплексный метод составляет основу единого научно-методического инструментария имитационного моделирования интерактивной сетевой среды для тестирования ССЗИ, обеспечивает комплексность и вариативность тестового воздействия.

Сетевой трафик рассматривается как множество всех составляющих его потоков, каждый из которых представлен множеством IP-пакетов, создаваемых в процессе двунаправленного обмена данными между двумя конечными узлами сети с использованием протокола транспортного уровня (TCP, UDP) или управления сетью (ICMP) в течение определенного интервала времени. Характеристиками сетевого трафика являются вероятностные распределения как характеристик потоков данных между узлами сети, так и пакетов внутри потоков. Основные классифицирующие признаки пакетов: идентификатор протокола $a_i \in A$, адреса и порты узлов источника $s_i \in S$, $ps_i \in PS$ и получателя $d_i \in D$, $pd_i \in PD$, время отправки $ts_{,i}$ и приема $tr_{,i} \in T$ i-го пакета, длина пакета $l_i \in L$, задержка передачи пакета $z_k = tr_k - ts_k$.

Каждый пакет k является элементом потока p, который в свою очередь принадлежит множеству всех возможных потоков P. Пакет описывается в виде кортежа его характерных свойств:

$$k = \langle a_k, s_k, d_k, ps_k, pd_k, ts_k, tr_k, z_k, l_k \rangle \in K. \quad (1)$$

Параметры потока пакетов p: объем потока b (сумма длин пакетов l); момент времени начала потока τ; разность межпакетных интервалов i-х отправленного и принятого пакетов $t_{p,i}$:

$$t_{p,i} = (tr_{,i} - tr_{i-1}) (ts_i - ts_{i-1}). \quad (2)$$

На основе данных характеристик отдельных пар пакетов вычисляются интегральные параметры потока:

— средняя задержка передачи пакетов: $\bar{z_l} = \frac{\sum_{i=1}^{n} z_i}{n}$, (3)

— средняя разность межпакетных интервалов: $\bar{t_p} = \frac{\sum_{i=1}^{n} t_{p,i}}{n}$, (4)

— среднеквадратическое отклонение разности межпакетных интервалов (джиттер): $\delta(t_p) = \sqrt{\frac{\sum(t_{p,i} - \bar{t_p})^2}{n-1}}$. (5)

Топология моделируемой сетевой среды описывается как совокупность множеств узлов сетей $H=S \cup D$, сетей W и сетевых интерфейсов Y.

Исходная последовательность пакетов сетевого трафика разбивается на множество групп, представляющих собой потоки, имеющие идентичные значения указанных выше параметров пакетов: a_i, s_i, d_i, ps_i, pd_i.

Статистические характеристики сетевого трафика, связанные с размером и распределением сетевых пакетов во времени внутри каждого из логических соединений, задаются векторами C_0, C_1 и C_2. Данные характеристики рассматриваются как случайные величины и задаются функциями распределения (далее — ФР). Определены векторы статистических характеристик:

— не связанных с направлениями передачи данных:

$$C_0 = <F_h, F_f>, \quad (6)$$

где F_h — ФР вероятности события генерации трафика конечными узлами потока, а F_f — ФР длительности потока внутри потока:

— связанных с направлениями передачи:

- от узла-инициатора к взаимодействующему узлу:

$$C_1 = <F_{l1}, F_{t1}>, \quad (7)$$

- от взаимодействующего узла к узлу-инициатору:

$$C_2 = <F_{l2}, F_{t2}>, \quad (8)$$

где F_{li} — ФР размера пакета, F_{ti} — ФР промежутка времени между началами передач двух последовательных пакетов. Каждый из векторов C_1 и C_2 содержит функции распределения вероятности размера пакета F_{li} и промежутка времени между началами передач двух последовательных пакетов F_{ti}

Таким образом, поток P может быть описан выражением:

$$P = <a, s, d, ps, pd, b, \tau, \bar{z}, \sigma(t_p), C_0, C_1, C_2>. \quad (9)$$

Для вектора потоков $<P_i>^n_{i=1}$ определена ФР F_g вероятности события генерации в сетевом трафике потока каждой из n_g групп, а также ФР F_c среднего значения генерируемых в сети потоков в секунду.

Таким образом, интерактивная модель M сетевой среды функционирования ССЗИ, используемая для синтеза тестового сетевого трафика, представлена выражением:

$$M=<H, W, Y, <P_i>^n_{i=1}, F_g, F_c>. \quad (10)$$

Разработанная модель *M* позволяет создать на ее основе алгоритмы и программный комплекс, решающий задачу синтеза массивов фонового сетевого трафика, в соответствии со статистическими характеристиками потоков информации в компьютерных сетях.

Синтез тестовых массивов данных осуществляется на основе статистических характеристик реальных ИТС, хранящихся в виде базы данных параметров сетевого трафика. Применяется метод хранения характеристик сетевой среды в виде набора матриц. В рамках матричной модели характеристики каждого потока представлены в виде набора векторов, описывающих отдельные статистические свойства потока. Совокупность всех потоков в ИТС хранится в виде матрицы, строки которой являются проиндексированными векторами характеристик потоков:

$$F = \langle A, S, D, PS, PD, T, B, L, Z \rangle \in \mathbf{R}^{f \times \Sigma}. \quad (11)$$

Предложенные модели сетевых сред функционирования для тестирования СОА, ТКО и для ИАСБ позволяют разрабатывать на их основе алгоритмы синтеза тестовых массивов фоновых данных, которые состоят из следующих шагов:

— определение значений характеристик сетевой среды ССЗИ с применением функций квантования, запись результатов в виде набора матриц;

— синтез области данных генерируемых массивов на основе цепи Маркова с дискретным временем;

— синтез потоков пакетов в виде дампа сетевого трафика в соответствии с матрицей характеристик сетевого трафика на основе функций деквантования;

— оценка адекватности синтезируемых массивов трафика с использованием показателя Херста, заключающаяся в сравнении значений показателя Херста для исходного и синтезированного трафиков.

С целью синтеза тестовых массивов данных для ИАСБ разработан **имитационно-статистический метод синтеза массивов условно-реальных данных**, основанный на пространственно-временной статистико-событийной модели взаимодействия абонентов ИТС, применяет матричную модель хранения статистических характеристик сетевых сред и алгоритмы сетей Петри для формирования комплексных ситуационных задач. Пространственно-временная статистико-событийная модель взаимодействия абонентов ИТС, основанная на поведении абонентов с точки зрения сети операторов связи, является совокупностью модели соединений *MS*, модели перемещений абонентов в течение заданного промежутка времени *MSH* и модели взаимодействия в социальных сетях *MI*:

$$M = \langle MS, MSH, MI \rangle. \quad (12)$$

Модель соединений *MS* учитывает статистические распределения биллинговой информации и социальные характеристики абонентов операторов сотовой связи, предполагает формирование массива строк биллинга *D*. Каждая строка соответствует направленному событию (соединению) в сети, имеющему инициатора и принимающую сторону. Соединения формируются на основе шаблонов, каждый из которых описывает типовое поведение абонентов с точки зрения совершаемых дей-

ствий в ИТС. Взаимодействие пользователей ИТС рассматривается в виде социальных графов[13] $G = (U, E)$, где U — множество вершин графа); E — множество ребер графа. G_M и G_S — социальные графы сервисов мобильной связи и социальных сетей. Ситуационная задача t описывается шаблоном взаимодействия пользователей $G_t = (U_t, E_t)$. Для описания вершины графа $u_x(G)$ используются атрибутивные текстовые и структурные компоненты учетных записей объекта в ИТС. Пользователь ИТС $u_x(G)$ описывается набором текстовых $Atr(u_x(G))$ и структурных атрибутов: $u_x(G) = \{O(G, u_x(G)), Atr(u_x(G))\}$. Структурные атрибуты представляют систему взаимоотношений между пользователями ИТС, описываются как окрестность[14] $O(G, u_x(G))$ вершины социального графа.

Основные текстовые атрибуты пользователя u_x в сети сотовой связи (граф G_M): $IMSI(u_x(G_M))$ — IMSI, $IMEI(u_x(G_M))$ — IMEI, $MSISDN(u_x(G_M))$ — MSISDN, $surname(u_x(G_M))$, $name(u_x(G_M))$, $secname(u_x(G_M))$ — фамилия, имя и отчество. Среди атрибутов учетной записи u_x пользователя в социальной сети (граф G_S) выделяются: $MSISDN(u_x(G_S))$ — MSISDN (номер телефона, указанный при регистрации), $IP(u_y(G_S))$ — IP-адрес, $UID(u_y(G_S))$ — идентификатор пользователя, $nickname(u_y(G_S))$ — его текстовый псевдоним.

В синтезируемом массиве биллинговой информации D каждая строка соответствует событию (действию) в сети и формируется из массивов, описывающих события различного типа — T, G, C и S:

– T — массив событий отправки сообщений о подключениях к базовым станциям для передачи координат: $T = \{t\}_{i=1}^{n_t}$;

– G — массив событий получения GPRS-трафика: $G = \{g\}_{i=1}^{n_g}$;

– C — массив звонков $C = \{c\}_{i=1}^{n_c}$, состоит из массивов исходящих C_o и входящих C_i звонков: $C = C_i + C_o$;

– S — массив СМС-сообщений $S = \{s\}_{i=1}^{n_s}$, состоит из *массивов* исходящих S_o и входящих S_i СМС-сообщений: $S = S_i + S_o$, (где n_t — количество перемещений, n_g — подключений, n_c, n_{co} и n_{ci} —звонков, n_s, n_{si} и n_{so} — сообщений).

Массив соединений Y является совокупностью массива звонков и массива СМС-сообщений: $Y = C + S$, где n_y — количество соединений ($n_y = n_c + n_s$). Характеристики элементов массива соединений Y:

– идентификатор типа соединения абонентов $\boldsymbol{A} \in (\overline{1, n_a})$, n_a – количество различных типов соединений;

– идентификаторы абонентов, участвующих в соединении $h_1, h_2 \in H$ — источник и получатель соединения;

– идентификаторы абонентов h_1 и h_2 в сети сотовой связи (IMSI, MSISDN, IMEI) и социальной сети (MSISDN, UID, IP).

---

[13] ***Социальный граф*** — граф, узлами которого являются социальные объекты (пользователи, абоненты), а ребрами — социальные связи между ними.

[14] ***Окрестность*** вершины $u_x(G) \in U$ $O(G, u_x(G)) = (UO(G, u_x(G)), EO(G, u_x(G)))$ — подграф, порожденный этой вершиной и всеми смежными с ней в графе G.

При формировании массива соединений *Y* учитываются статистические характеристики биллинговой информации, хранящиеся в виде базы данных матриц характеристик сетевой среды ИТС:

– $K_0 = \langle F_{time}, F_{dur}, F_n, F_a \rangle$ — не связанные с адресацией соединения, описываемые ФР: F_{time} — времени суток, F_{dur} — длительности события, F_n — количества соединений, F_a — вероятности генерации типа события;

– $K_1 = \langle F_l, F_t \rangle$ — связанные с адресацией соединения: F_l — ФР выбора получателей соединения, а F_t — ФР промежутков времени между началами инициализации двух последовательных соединений.

Аналогично формируются массивы *T* и *G* подключения к базовым станциям для передачи координат и получения GPRS-трафика.

Таким образом, структура соединений определена вектором $\langle Y_i \rangle_{i=1}^{n_Y}$:

$$Y_i = \langle A, h_1, h_2, p_1, p_2, K_0, K_1 \rangle. \quad (13)$$

Модель соединений *MS* определяется выражением:

$$MS = \langle H, W, \langle Y_i \rangle_{i=1}^{n_Y} \rangle. \quad (14)$$

Модель перемещений *MSH* предназначена для генерации полей, описывающих географические координаты совершения события, имитирует перемещения абонентов в заданном временном интервале в рамках населенного пункта, который представляется квадратом, состоящим из массива клеток. Для каждой клетки задаются модифицируемые списками параметры LAC (Location Area Code — код локальной зоны) и CellID (уникальный номер, предназначенный для идентификации базовых станций). Передвижение абонентов в рамках населенного пункта описывается шаблонами перемещений *SH*, которые представляют собой упорядоченные по времени списки LAC и CellID, по которым отслеживается передвижение абонента в течение заданного времени. Для создания траекторий перемещений абонентов применяются алгоритмы сетей Петри, где квадраты карты населенного пункта рассматриваются как множество узлов *P*, а пути — множество взвешенных переходов сети *T*. Каждый переход t_{ij} обладает весом $m(t_{ij})$, имеющим смысл количества совершенных соединений между абонентами, которым соответствуют начальный $p_{\text{н}}$ и конечный $p_{\text{к}}$ узлы перехода (рисунок 7).

В модели взаимодействия пользователей в социальных сетях *MI* учитываются множества абонентов оператора сотовой связи *H* и «семей» *W*, а также массив взаимодействия в социальных сетях *YI*, являющийся совокупностью информационных сообщений трех типов: публичное, публичное направленное и приватное, содержащее информацию исключительно для одного получателя.

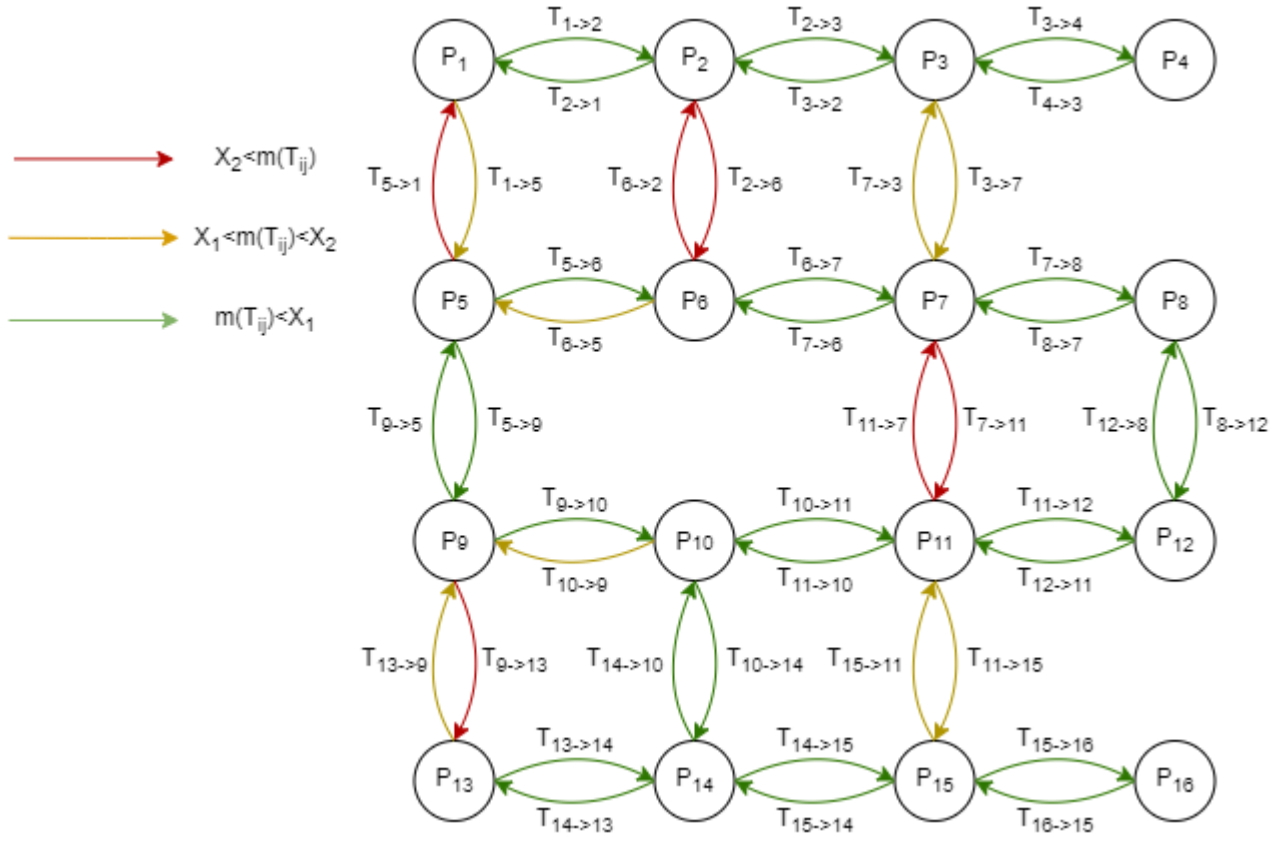

Рисунок 7. Пример сети Петри, используемой в модели перемещений *MSH*

На основе разработанной пространственно-временной статистико-событийной модели *M* создан программный комплекс, решающий задачу синтеза массивов биллинговой информации, в котором для построения модели соединений *MS* на основе модели перемещений *MSH* использован алгоритм сетей Петри. Процесс синтеза массивов условно-реальных данных о взаимодействии пользователей ИТС основан на модели *M* и представлен последовательными этапами формирования статических и динамических компонентов (рисунок 8). Этап 1. Формирование статических компонентов записей d_M и d_S, к которым относятся персональные идентификаторы пользователей и структура их взаимосвязей внутри ИТС. С целью создания структурной основы для описания взаимодействия пользователей ИТС используется метод формирования статической структуры социальных графов G_M и G_S на основе композиции моделей построения сложных сетей с учетом заданного шаблона взаимодействия пользователей G_t [2, 4].

Процесс формирования структуры социального графа G_M в соответствии с моделью Ваттца-Строгатца начинается с генерации регулярной решетки со степенью вершин *K*. Затем происходит выбор случайным образом соседних вершин в количестве $|U_t|$, с распределением значений вершин и ребер в соответствии с U_t и E_t. Для графа G_S генерируется случайный граф с количеством вершин m_0.

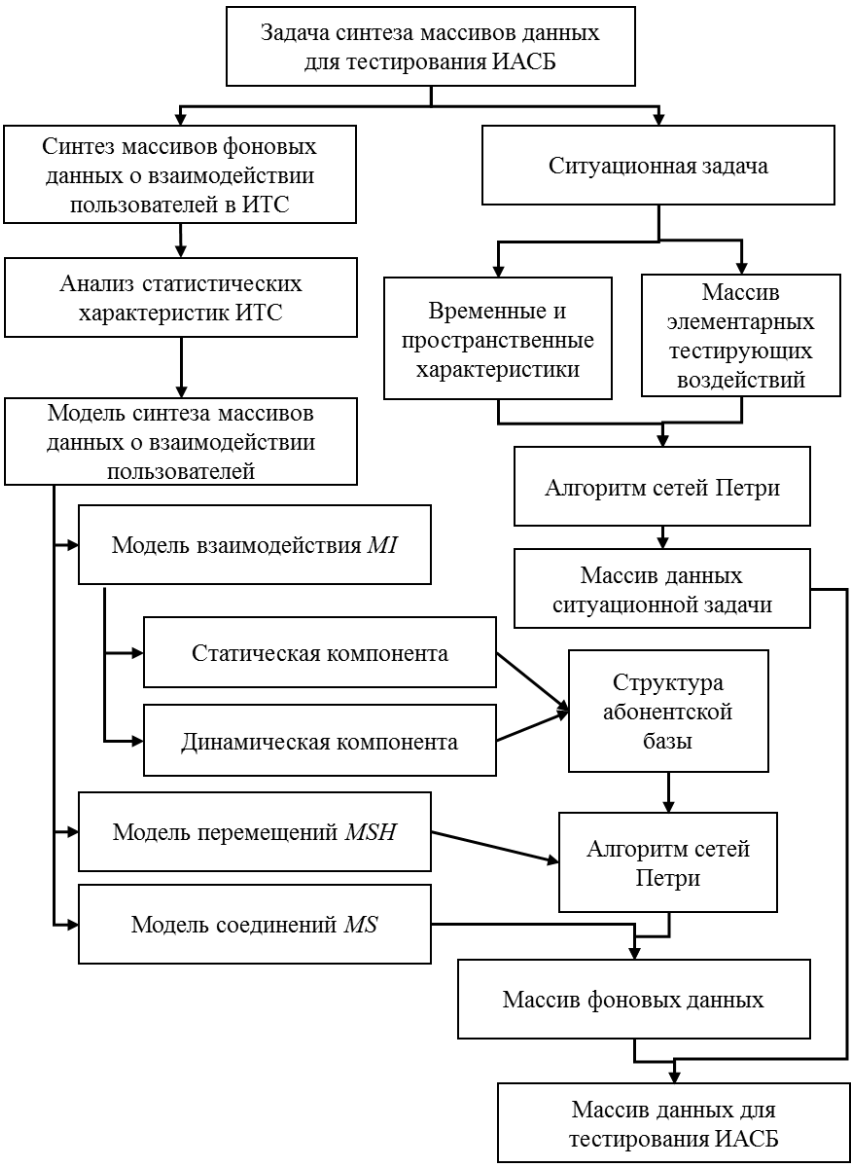

Рисунок 8. Схема синтеза массивов данных для тестирования ИАСБ

Случайный граф (начальное ядро социального графа) строится в соответствии с моделью Эрдёша-Реньи. Исходными данными являются количество вершин m_0 и вероятность p_0, с которой между двумя произвольными вершинами образуется ребро. После создания структурного ядра графа происходит последовательное добавление вершин в количестве $m_{\max}$, определенном изначально. При создании статической структуры сервиса социальных сетей G_S в соответствии с моделью Барабаши-Альберт определяются численность пользователей имитируемого сервиса $|U_S|$, количество ребер C, с которыми новая вершина добавляется в структуру графа. Параметр C определяет степень кластеризации вершин графа.

Этап 2. На основе созданных социальных связей пользователей происходит генерация динамических компонентов коммуникационного события (тип, участники, место, время начала и продолжительность). Используются статистические распределения следующих групп параметров: событийные (поля *BillingType*, *Type*); социальные (поля *PhoneB*, *UIDB*); пространственные (поля *LAC*, *CellID*); временные (поля *Time*, *CallDuration*).

Задача синтеза динамической составляющей массива фоновых данных, предполагающая наличие большого количества активных объектов с отчетливо выраженным индивидуальным поведением, относится к категории синтеза сложных систем, для решения применены цветные сети Петри — кортеж $CPN = <P, T, TM, I, O, M>$, где P — множество позиций, T — множество переходов, TM — множество

временных моментов для срабатывания переходов, I — множество входящих в переходы дуг, O — множество выходящих из переходов дуг, M — множество меток в начальный момент времени.

Представленные статические и динамические компоненты массивов данных соответствуют объектам сетей Петри: динамические (изображаются метками (фишками, маркерами) внутри позиций) и статические (им соответствуют вершины и дуги сети Петри). Для отражения динамических свойств в сеть Петри введено понятие разметки сети, которая реализуется с помощью меток $m_k \in M$, размещаемых в позициях. Метки окрашиваются в различные цвета в зависимости от типа коммуникационного события: B — отправка сообщений о подключениях к базовым станциям для передачи координат; G — получение GPRS-трафика; C — совершение звонка; S — отправка СМС-сообщения; публичная (public) и приватная (private) переписка; социальный статус получателя сообщения (*family/others*).

Для упорядочивания таблиц взаимодействия пользователей ИТС по времени начала события в модели введен временной механизм, реализованный с помощью глобальных часов и временных штампов меток. Метка становится доступной для перехода, если ее штамп меньше значения счетчика глобальных часов. В результате инициализации начальной разметки сети происходит распределение меток с заданными параметрами по определенным позициям в соответствии со статистическими распределениями различных характеристик рассматриваемых ИТС, затем происходит последовательное перемещение меток между позициями, что позволяет создавать строки d_M и d_S в массивах D_M и D_S.

При выполнении циклов сети Петри имитируется информационный обмен между заданным количеством пользователей $|U_M|$ и $|U_S|$ в определенный временной период $[t_{\text{start}}, t_{\text{end}}]$. Результатом выполнения всех циклов являются синтезированные массивы D_M и D_S требуемого формата.

Таким образом, имитационно-статистический метод синтеза массивов условно-реальных данных представляет собой последовательность этапов, имитирующих различные параметры процесса взаимодействия пользователей на основе статистических распределений требуемых показателей в реальных ИТС.

Генерация графа атакующего воздействия, используемого в процессах анализа защищенности ИТС и создания ситуационных задач при тестировании ССЗИ, осуществляется на основе **метода синтеза атакующего воздействия и ситуационных задач**, основанного на применении теоретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов для формирования статической структуры графа атакующего воздействия и алгоритмов сетей Петри для синтеза динамической составляющей атакующего воздействия (траектории развития атаки). Конечной целью моделирования является синтез последовательности пакетов для последующей генерации имитируемого атакующего воздействия. При этом комплексная компьютерная атака должна быть представлена совокупностью элементарных тестирующих (атакующих) воздействий, каждое из которых в свою очередь является последовательностью ранее записанных сетевых пакетов известной компьютерной атаки. Задача синтеза — расстановка последовательности пакетов в синтезируемом массиве имитируемой

компьютерной атаки с учетом характеристик моделируемой ИТС (диапазоны IP-адресов, функциональность узлов с точки зрения сетевого взаимодействия, имитируемая сетевая инфраструктура, соответствие уязвимостей ИТС ЭТВ, имеющимся в тестовой базе) и временных интервалов.

Синтез (проектирование) комплексного атакующего воздействия в иерархической (с точки зрения сетевой достижимости узлов) системе уязвимых объектов ИТС основан на представлении атаки в виде исходного двудольного графа *G(A,H,E)*. Компьютерные атаки представляются в виде множества вершин *A*, а атакуемые узлы имитируемой уязвимой ИТС — в виде множества вершин *H* (рисунок 9). Множество ребер (дуг) *E* выражает степень реализуемости компьютерной атаки по отношению к атакуемому узлу. Граф *G(A,H,E)* комплексного атакующего воздействия является вершинно и реберно взвешенным. Веса вершин комплексных компьютерных атак a_k характеризуют потенциальную реализуемость компьютерной атаки по отношению ко всем узлам *H* имитируемой ИТС с точки зрения воздействия на конфиденциальность, целостность и доступность информации. Веса узлов h_m характеризуют потенциальную уязвимость узла ко всему множеству компьютерных атак из *A*. Веса ребер e_{km} определяют степень реализуемости атаки, измеряемую от 0 до 10 в зависимости от усредненной интегральной оценки критичности атакующего воздействия Base Score, вычисляемой в соответствии с общепринятой системой оценки уязвимостей CVSS.

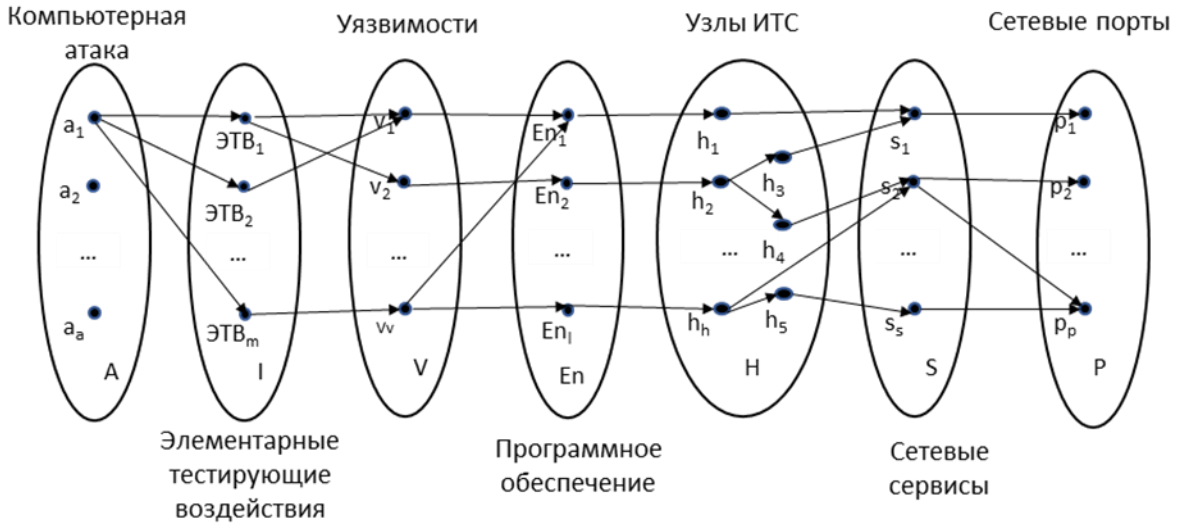

Рисунок 9. Граф воздействия комплексной атаки на узел ИТС

Каждая комплексная компьютерная атака из множества вершин *A* представлена подмножеством ЭТВ *I*. Каждое ЭТВ из множества *I* использует одну или несколько уязвимостей *V*, присущих определенному ПО. Рассматривая моделируемую ИТС как иерархическую совокупность взаимодействующих узлов, подверженных воздействию компьютерных атак с использованием уязвимостей, зависящих от программного окружения, граф комплексного атакующего воздействия *G(A,H,E)* представляется семи-дольным графом *G(A, I, V, En, H, S, P, E^{AI}, E^{IV}, E^{VEn}, E^{HEn}, E^{HH}, E^{HS}, E^{SP})*. Множество дуг графа *G* описывается прямоугольными матрицами: E^{AI} — вхождения ЭТВ в комплексные атаки; E^{IV} — использования ЭТВ

уязвимостей; E^{VEn} — воздействия уязвимостей на программное окружение; E^{HEn} — программное окружение узлов ИТС; E^{HH} — взаимная сетевая достижимость узлов ИТС; E^{HS}— наличие на узле сервиса; E^{SP} — использование сервисом TCP/UDP-порта.

Для учета взаимной сетевой достижимости узлов ИТС на основе матрицы E^{HH} строится итоговая матрица достижимости узлов по отношениям структурной вложенности E^{HHR}. Вычисление матрицы E^{HHR} осуществляется на основе степеней матрицы E^{HH} по выражению:

$$E^{HHR} = E^{HH} + (E^{HH})^2 + (E^{HH})^3 + \ldots + (E^{HH})^n,$$

где E^{HH} — единичная матрица сетевых узлов, n — максимальная глубина «леса» H (максимальная степень матрицы E^{HH}, приводящая к нулевой матрице результата). Смысл степеней матриц $(E^{HH})^k$ заключается в том, что их элементы отображают наличие или отсутствие пути длиной k между узлами i и j в графе H.

Для формирования развернутого графа воздействия комплексной атаки на узел сети (с учетом ЭТВ, уязвимостей и их воздействия на ПО, наличия ПО на узлах сети и взаимодействия между узлами) необходимо от исходного графа комплексного атакующего воздействия G перейти к графу «атака-узел» $G_{ij}(a_i, I, V, En, h_j, S, P, E^{AI}, E^{IV}, E^{VEn}, E^{HEn}, E^{HH}, E^{SP}, E^{HS})$, описывающему пути, ведущие от комплексной компьютерной атаки к узлу. В графе G_{ij} множества вершин и дуг представляют собой подмножества соответствующих вершин и дуг графа G. Алгоритм формирования графа G_{ij} состоит из нескольких этапов: выбор исходной и конечной вершины; определение всех вершин, смежных с исходной и конечной вершиной; построение путей, ведущих от атаки к узлу.

В рамках предложенной формализации решается задача создания исходного статического графа последовательности атакующих воздействий, на основе которого в дальнейшем строится динамическая модель комплексной атаки, учитывающая последовательность временных интервалов и вариативность применения элементарных атакующих воздействий (путей развития атаки в графе G_{ij}) с применением алгоритмов сетей Петри со случайными задержками. Компьютерная атака развивается во времени, значительная часть временных задержек носит стохастический характер, определяемый, в частности, временем передачи сетевых пакетов между атакующим и атакуемым. На каждом этапе комплексной атаки алгоритм выбирает переход сети Петри с учетом конечной цели атаки, результата ЭТВ с точки зрения нарушения конфиденциальности, целостности и доступности информации, что обеспечивает альтернативное развитие комплексной атаки, а также случайный характер синтезируемых задержек (рисунок 10).

Совокупность статической теоретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов и динамической модели комплексной атаки с применением алгоритмов сетей Петри позволяет реализовать управляемый процесс синтеза сетевого трафика комплексных компьютерных атак (ККА), элементы которых в виде ЭТВ хранятся в базе данных (БД КА). Полученный сетевой трафик может многократно использоваться для тестирования различных СОА.

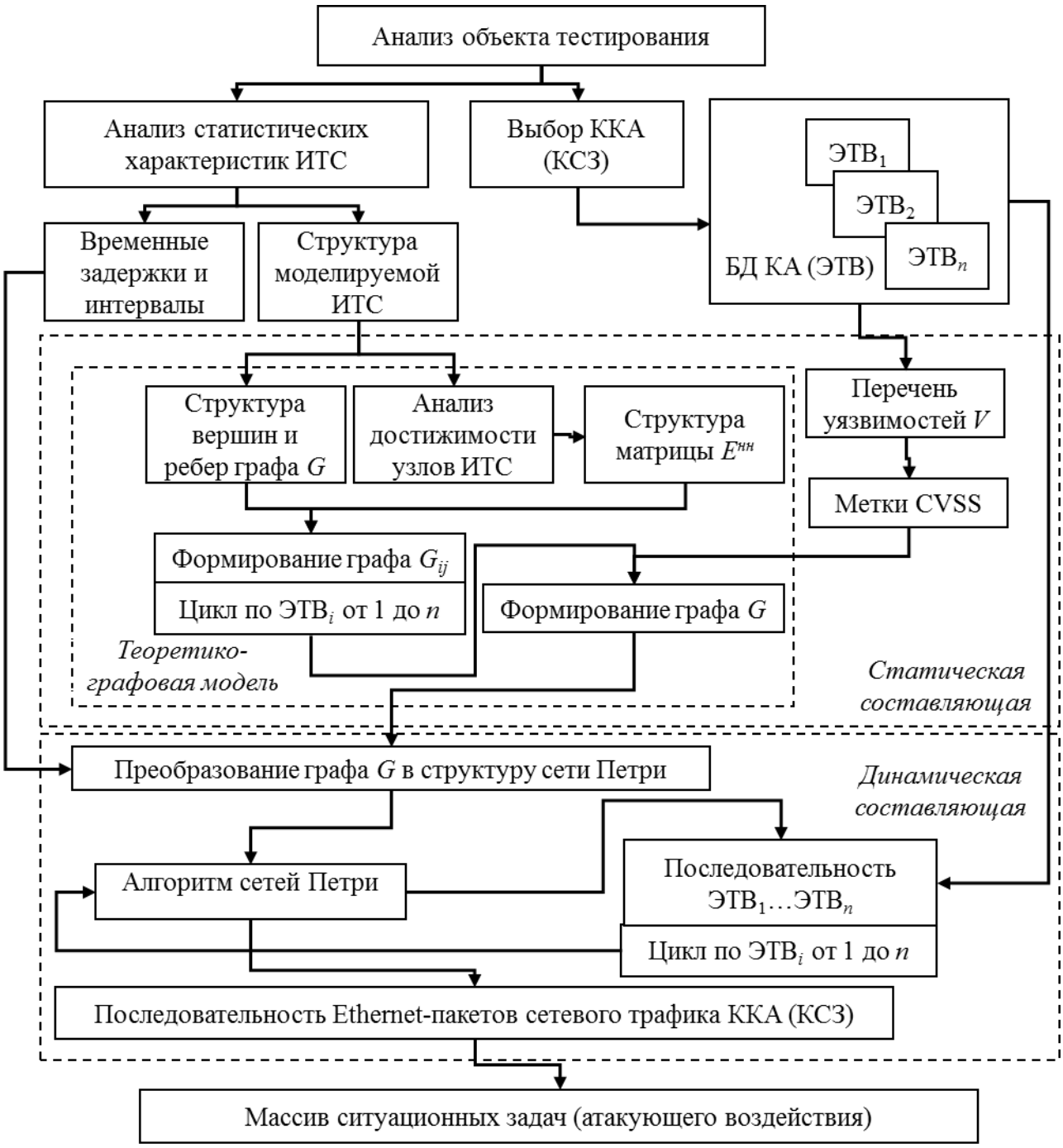

Рисунок 10. Схема процесса синтеза массива атакующего воздействия

С целью выявления ранее неизвестных уязвимостей ССЗИ разработан **комплекс моделей, методик, алгоритмов и программного обеспечения для тестирования устойчивости ССЗИ к сетевым атакам типа «отказ в обслуживании»**, основанный на применении эволюционно-генетического подхода.

Одна из задач ТКО — обеспечение передачи информации с обеспечиваемой степенью доступности $\omega \in \Omega$, которая может быть нарушена атакующим воздействием типа «отказ в обслуживании». Процесс выявления уязвимости ТКО к таким атакам представляет собой поиск сочетаний параметров сетевого трафика атакую-

щего воздействия, к которому ТКО оказывается уязвимо. Совокупность параметров трафика для тестирования ТКО может быть представлена в виде вектора ψ в общем пространстве параметров тестового сетевого трафика Ψ. Поиск уязвимостей — выявление экстремумов многомерной функции $\omega(\psi)$ является задачей переборного типа, которая может быть решена с применением генетического алгоритма. При разработке генетического алгоритма необходимо определить параметры особи (входные и выходные); функцию приспособленности особи; механизмы скрещивания, мутации и селекции; условия завершения. В качестве входных параметров особи рассматривается совокупность параметров модели сетевой среды функционирования ССЗИ M, описывающей топологию моделируемой сети и структуру циркулирующего в ней сетевого трафика: H, W, Z, $\langle G_i \rangle_{i=1}^{n_g}$, F_g, F_c. Выходными параметрами особи являются параметры тестового сетевого трафика, входящие в вектор ψ:

$<n_h,\ n_w,\ n_z,\ p_s,\ p_{tcp},\ p_{\mathrm{udp}},\ p_{icmp},\ \overline{n_f},\ \sigma(n_f),\ \overline{t_f},\ \sigma(t_f), \overline{l_p}, \sigma(l_p), \overline{t_p}\ \ \sigma(t_p),\ \overline{t_d},\ \sigma(\delta t_p),\ q>$,

где количество взаимодействующих узлов n_h и сетей n_w и задействованных в процессе взаимодействия сетевых интерфейсов ТКО n_z; относительная доля p_s пакетов, сгенерированных узлами-инициаторами соединений; относительные доли потоков TCP p_{tcp}, UDP p_{udp} и сеансов взаимодействия ICMP p_{icmp}; средние значения и среднеквадратические отклонения количества потоков ($\overline{n_f}$ и $\sigma(n_f)$), длительности потоков ($\overline{t_f}$ и $\sigma(t_f)$), длины пакета ($\overline{l_p}$ и $\sigma(l_p)$), разности межпакетных интервалов ($\overline{t_p}$ и $\sigma(t_p)$).

Также выходными параметрами алгоритма являются результаты тестирования образца ТКО с использованием данного сетевого трафика, определяющие обеспечиваемую ТКО доступность информации $\omega \in \Omega$ и отражающие успешность применения данного сетевого трафика как потенциальной реализации атаки типа «отказ в обслуживании»: средняя задержка передачи пакетов $\overline{t_d}$; среднеквадратическое отклонение разности межпакетных интервалов отправленных и принятых пакетов $\sigma(\delta t_p)$; относительная доля потерь пакетов q. В процессе тестирования ТКО выявляются критические области пространства параметров сетевого трафика, где по крайней мере один из параметров доступности информации превышают заданные требованиями к ИТС пороговые значения (рисунок 6).

Каждая из особей μ_i популяции генетического алгоритма представляет собой определенное сочетание значений параметров модели M сетевой среды функционирования ТКО, которому взаимно однозначно соответствует хромосома — последовательность бит χ_i.

Процесс отбора особей реализуется с использованием элитной стратегии, подразумевающей перенос особей, соответствующих наибольшим значениям по крайней мере одного из элементов вектора ω, из предыдущего поколения популяции в следующее. Шаг изменения размера популяции равен трем (в соответствии с механизмом скрещивания перенос одной родительской особи в следующее поколение

вызывает появление двух дополнительных потомков), минимальный размер популяции — шести (для процедуры скрещивания необходимы как минимум две особи, каждая из которых генерирует по два потомка).

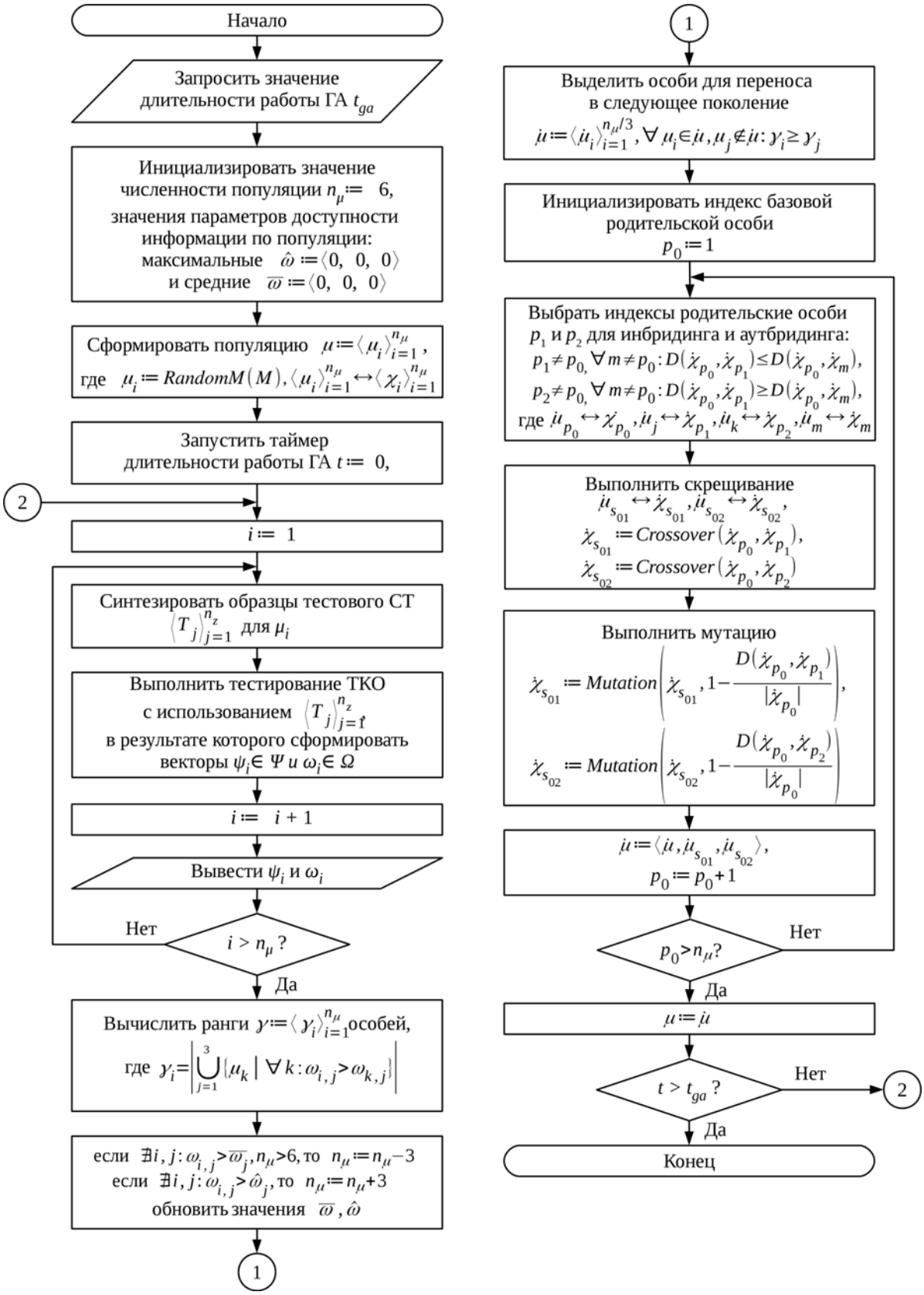

Рисунок 11. Схема генетического алгоритма для тестирования ТКО

В алгоритме использованы следующие функции и процедуры:

— *RandomM* — процедура инициализации особи μ_i с помощью генератора случайных чисел;

— D — функция расстояния Хэмминга между хромосомами особей;

— *Crossover* — процедура скрещивания особей путем двухточечного кроссинговера со случайным выбором границ областей обмена битами соответствующих хромосом;

— *Mutation* — процедура мутации особи методом сальтации ее хромосомы с вероятностью, определяемой отношением расстояния Хэмминга между ее родительскими особями и длиной хромосомы. Производится выбор в генотипе особи, представленном в виде *n*-битовой бинарной строки $\chi = \langle \chi_i \rangle_{i=1}^{n}$, где $\chi_i \in \{0,1\}$, границ $j_0, j_1 \in \{1, n-1\}$, где $j_0 < j_1$, в пределах которых заменяются значения бит генотипа на противоположные и формируется измененный генотип $\dot{\chi}$.

Результатом работы генетического алгоритма является база данных, содержащая множество точек $\rho = \{\rho_i \mid \rho_i \in \Psi \times \Omega\}$, где $\rho_i = \langle \psi_i, \omega_i \rangle$, $\psi_i \in \Psi$, $\omega_i \in \Omega$, отражающих соответствие параметров трафика, обрабатываемого ТКО, обеспечиваемой им доступности информации. Практическая значимость решения состоит в возможности нахождения ранее неизвестных уязвимостей, приводящих к нарушению производительности ТКО при определенных сочетаниях параметров входных данных, не являющихся пороговыми.

Для каждого ССЗИ разрабатывается уникальная методика тестирования, основанная на требованиях нормативных документов к данному виду ССЗИ. На основе комплексного метода имитационного моделирования интерактивной сетевой среды предложены **комплексы моделей, методик, алгоритмов и программного обеспечения и учебно-экспериментальных стендов** синтеза тестовых массивов данных, которые представлены в **третьей главе** диссертации и предназначены для тестирования СОА, ТКО.

Экспериментальный стенд (рисунок 12), предназначенный для тестирования СОА, содержит программное обеспечение модуля управления тестированием с использованием базы данных ЭТВ, которое позволяет формировать сценарии атакующего воздействия любой сложности без необходимости присутствия реальных узлов-жертв в момент тестирования.

Стенд тестирования ТКО (рисунок 13), позволяющий с применением генетических алгоритмов выявлять ранее неизвестные уязвимости ТКО, приводящие к нарушению производительности оборудования при определенных сочетаниях параметров входных данных, не являющихся пороговыми, содержит [11, 12]:

— модуль тестирования, выполняющий воспроизведение тестового сетевого трафика (СТ) и одновременную запись сетевого трафика, принятого после обработки тестируемым образцом ТКО. В модуле применяются алгоритмы разделения потока сетевого трафика, направляемого программами воспроизведения (ПВ) на

входные сетевые интерфейсы (СИin) ТКО, и алгоритмы агрегации сетевых потоков, поступающих от выходных сетевых интерфейсов (СИout) через программы записи (ПЗ) сетевого трафика;

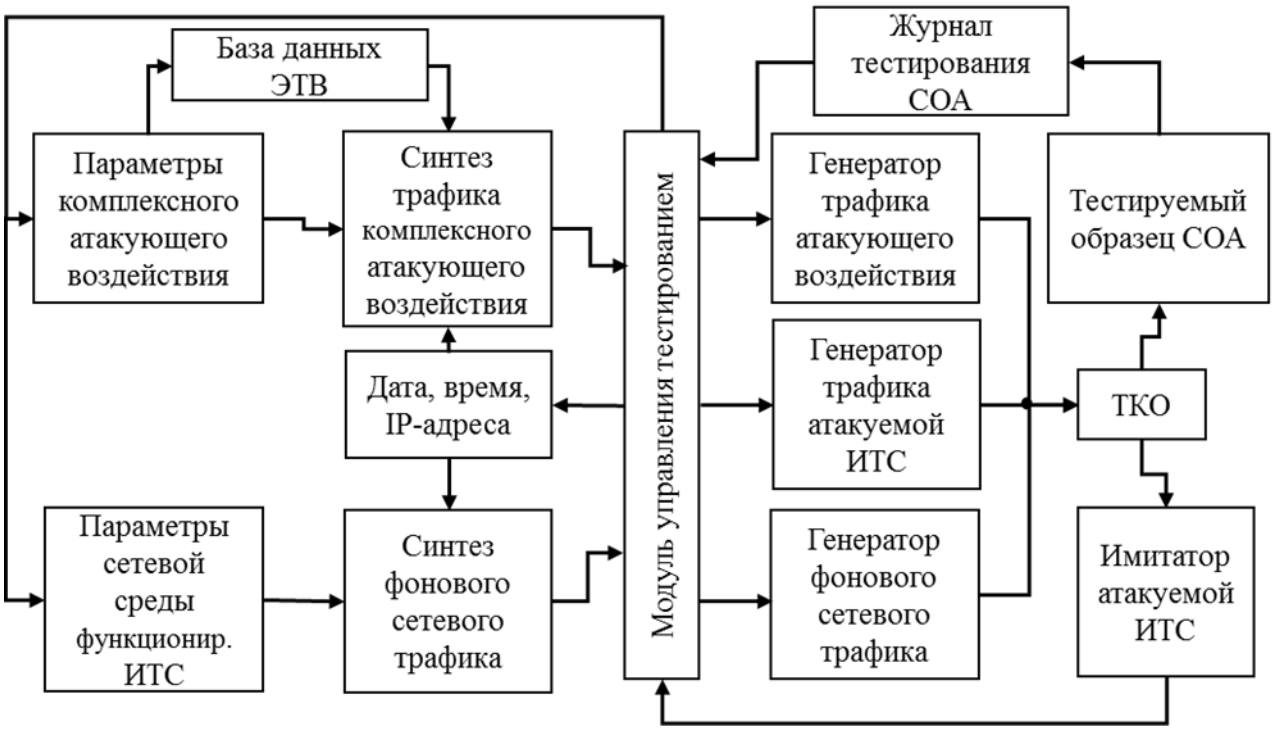

Рисунок 12. Структура стенда тестирования СОА

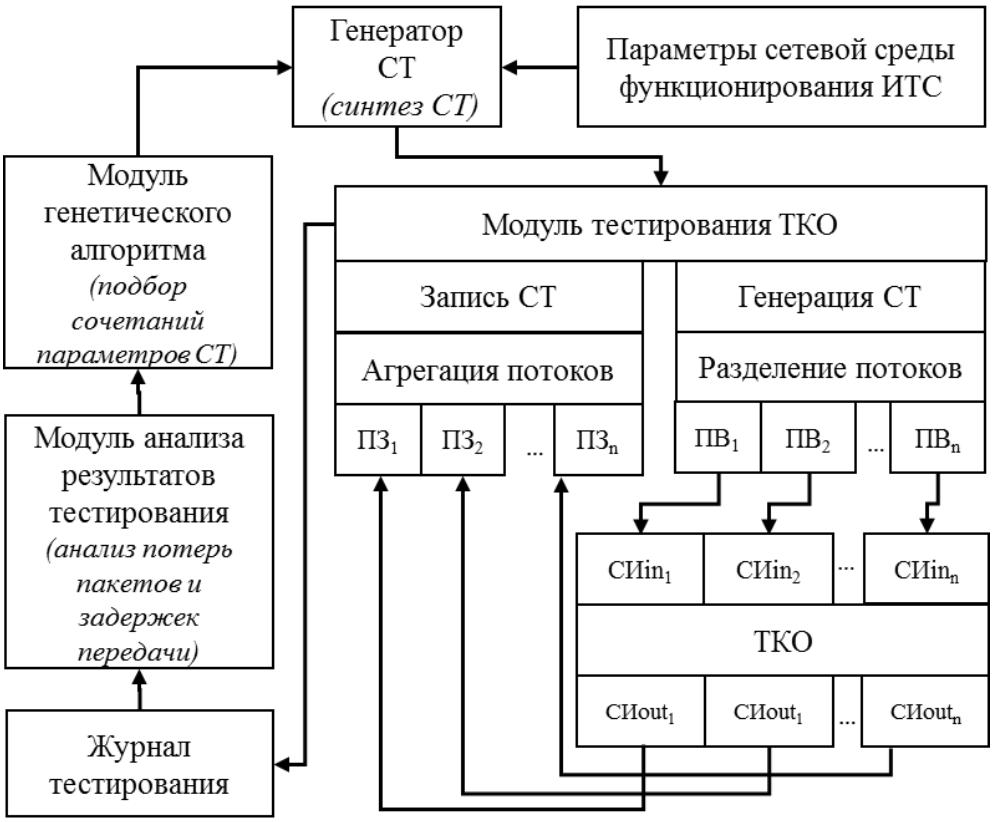

Рисунок 13. Структура комплекса тестирования ТКО

— генератор сетевого трафика, синтезирующий тестовый сетевой трафик с параметрами, заданными параметрами модели *M* сетевой среды функционирования ТКО в ИТС;

— модуль генетического алгоритма, производящий на основе генетического алгоритма поиск множества точек в пространстве параметров сетевой среды функционирования ТКО, в которых обеспечиваемая ТКО доступность информации оказывается наихудшей;

— модуль анализа результатов тестирования, предназначенный для выявления критических областей в пространстве параметров сетевой среды функционирования ТКО на основе алгоритма кластерного анализа скользящего среднего.

В четвертой главе приведено описание структуры разработанного учебно-научного компьютерного полигона по расследованию инцидентов ИБ (далее — киберполигон), который представляет собой комплекс моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных, основанный на разработанном методе имитационного моделирования интерактивной сетевой среды для тестирования ССЗИ.

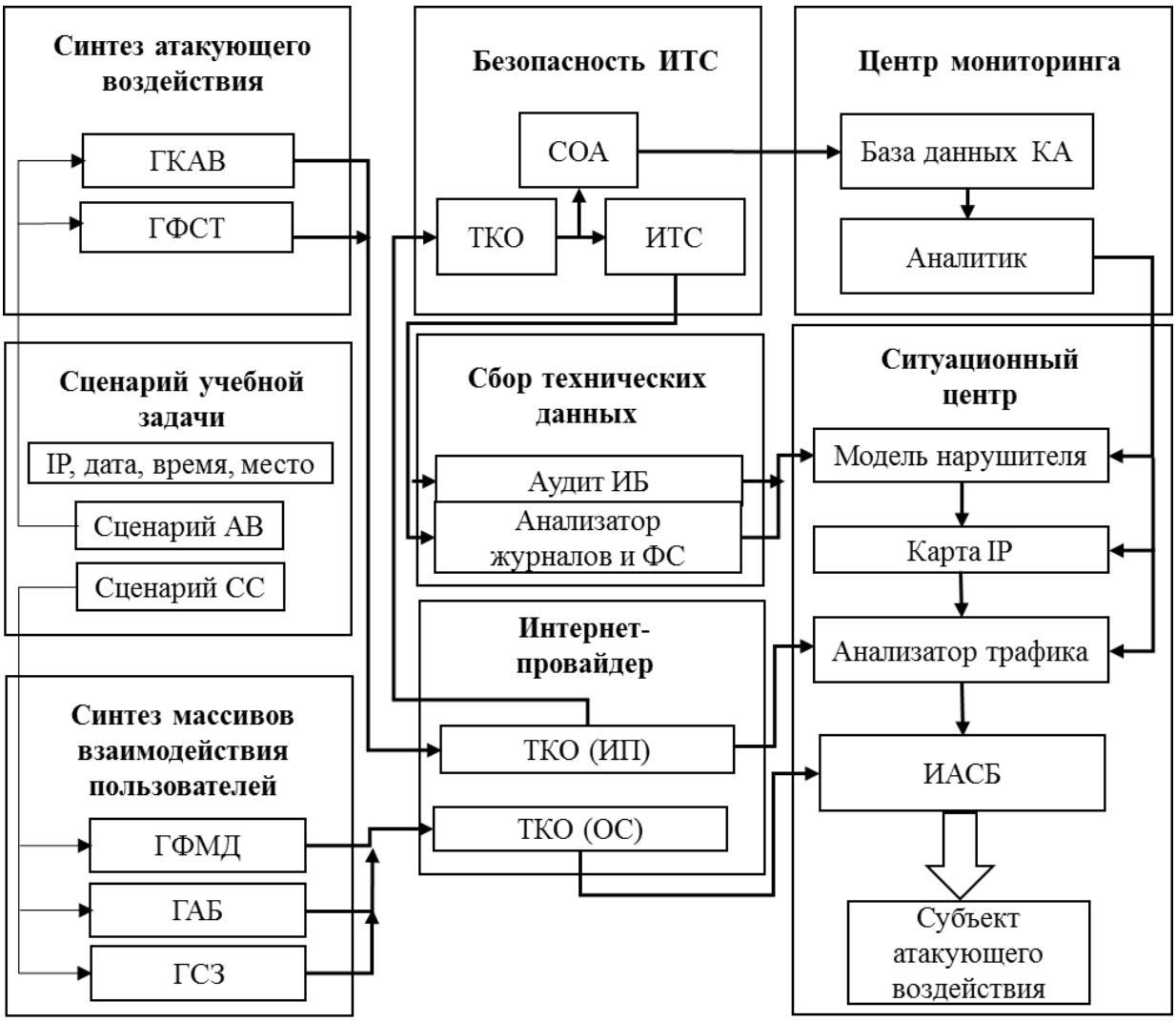

Рисунок 14. Схема информационного взаимодействия сегментов киберполигона по расследованию инцидентов ИБ

Киберполигон (рисунок 14) — это совокупность программно-аппаратных средств, которые предназначены для анализа событий, зафиксированных различными техническими средствами. Модель киберполигона для тестирования ССЗИ и расследования инцидентов ИБ является совокупностью моделей сетевых сред синтеза компьютерной атаки, синтеза биллинговой информации и синтеза взаимодействия пользователей в социальных сетях, что позволяет формировать единую ситуационную задачу по расследованию инцидентов ИБ с учетом действий нарушителей ИБ во временном, пространственном, а также информационном аспектах. Единая ситуационная задача охватывает процедуры тестирования и эксплуатации элементов ИТС, а также реагирования и расследования компьютерных инцидентов и включает подзадачи:

— тестирование наличия уязвимостей в ССЗИ и ИТС в целом;

— выявление комплексного атакующего воздействия на ИТС;

— сбор и анализ технических данных при реагировании на инциденты ИБ;

— проведение расследования инцидентов ИБ, локализация источников и субъектов компьютерных атак.

Киберполигон является совокупностью сегментов, объединенных в единую информационную систему, представленных соответствующими стендами, каналами связи и вычислительными ресурсами. Сегменты киберполигона развернуты в лабораториях учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина» (далее — УНЦ ИБ).

Сегмент «Синтез атакующего воздействия» предназначен для формирования массивов сетевых пакетов, содержащих сигнатуры сетевых компьютерных атак, на основе использования генераторов комплексного атакующего воздействия (ГКАВ) и фонового сетевого трафика (ГФСТ). Из сегмента в сетевую инфраструктуру киберполигона поступает совокупность массивов синтезированного сетевого трафика в соответствии со сценарием учебной задачи, регламентирующим IP-адреса атакующих узлов и временные метки атакующего воздействия, адреса электронной почты, учетные записи в социальных сетях.

Сегмент «Безопасность ИТС» обеспечивает формирование сетевой инфраструктуры ИТС и содержит ряд стендов, имитирующих ИТС и ИС различного назначения. На базе сегмента выполняются практические задания по проведению аудита ИБ, производится подключение САЗ к элементам ИТС с целью выявления потенциальных возможностей внешнего и внутреннего нарушителей и построения модели нарушителя и графов атак. Результатом работы узлов сегмента, помимо выявленных уязвимостей узлов ИТС в рамках аудита ИБ, являются записи об атакующем воздействии, которые генерируются СОА и поступают для дальнейшего анализа в сегмент «Центр мониторинга». В состав имитируемой типовой ИТС (рисунок 15) входят блоки корпоративной сети предприятия с демилитаризованной зоной (ДМЗ), содержащей серверные приложения, системы предотвращения утечки данных (DLP).

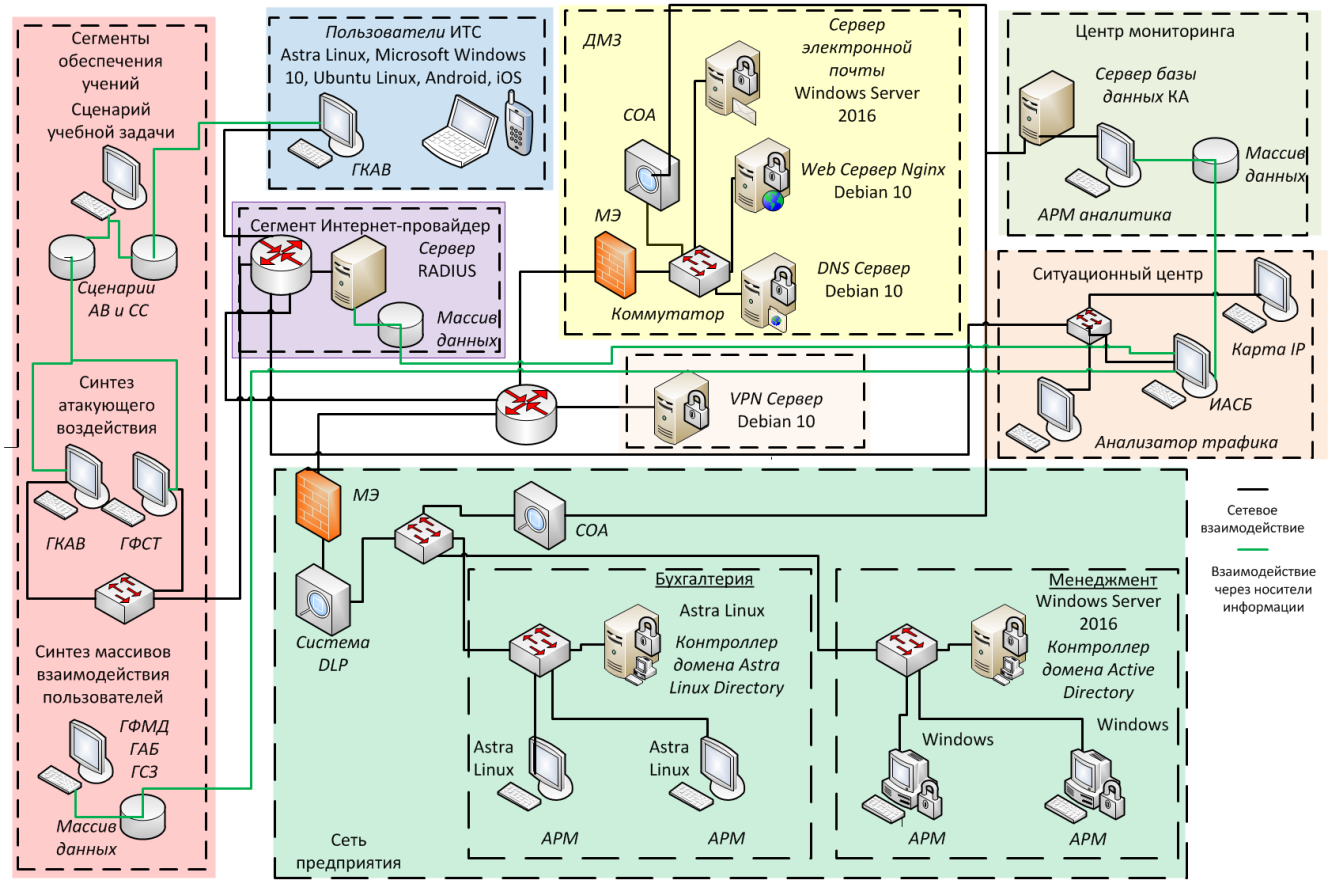

Рисунок 15. Основные компоненты киберполигона

Сегмент «Сбор технических данных» представляет совокупность образов дисков ИТС и ИС с интегрированными следами инцидентов ИБ, позволяющих проводить анализ событий инцидента для последующего формирования модели нарушителя. Сегмент «Центр мониторинга» имитирует функциональные задачи корпоративного центра мониторинга системы обнаружения компьютерных атак, включая сбор информации с сенсоров СОА, накопление информации в базе данных компьютерных атак, организацию мониторинга хода атакующего воздействия на автоматизированных рабочих местах аналитиков группы реагирования на инциденты. Одним из результатов работы аналитиков является построение карты IP-адресов атакующего воздействия с детализацией территориальной принадлежности атакующих. Сегмент «Ситуационный центр» предназначен для выявления субъектов (источников) атакующего воздействия, включает комплект ИАСБ для анализа информации о взаимодействии пользователей в сетях операторов сотовой связи и социальных сетей. На вход в сегмент поступают результаты проведения мероприятий по оценке защищенности ИТС и ИС, анализа комплексного атакующего воздействия, выявленные IP-адреса атакующих и атакованных ИТС, территориальная и юридическая принадлежность IP-адресов к провайдерам сети Интернет, а также анализа сетевого трафика по IP-адресам и информации о взаимодействии пользователей.

Сегмент «Интернет-провайдер» является совокупностью оборудования и программного обеспечения типового провайдера услуг сети Интернет, также предоставляющего доступ к сетям сотовой связи. Содержит и по запросу передает

информацию о взаимодействии пользователей, накапливаемую в ТКО. Сегмент «Синтез массивов взаимодействия пользователей» предназначен для синтеза массивов данных о взаимодействии пользователей в ИТС, состоит из генератора массивов фоновых данных (ГФМД), имитирующего взаимодействие произвольных пользователей, генератора ситуационной задачи (ГСЗ), позволяющего интегрировать задаваемое сценарием поведение атакующих в сетях связи, и генератора абонентской базы (ГАБ), предназначенного для синтеза имитируемых идентификаторов субъектов взаимодействия в ИТС. Из сегмента в виде файлов, предназначенных для загрузки в ИАСБ, поступают синтезированные массивы биллинговой информации и массивы данных о принадлежности сетевых идентификаторов, в том числе номеров операторов сотовой связи.

Сегмент «Сценарий учебной задачи» является инструментом преподавателя для формирования уникальной учебной задачи по расследованию инцидента ИБ. Сценарий задачи определяет совокупность условий для синтеза массивов данных, объединенных единым сценарным планом, предполагающим единые цели атакующих, диапазон IP-адресов, временной интервал и территориальную зону, учитываемые как при синтезе IP-трафика (сценарий АВ), так и при формировании массивов информации о взаимодействии в сетях операторов связи и в социальных сетях (сценарий СС). Результатом работы сегмента являются конфигурационные файлы, описывающие соответствующие сценарии, которые последовательно загружаются в качестве входных данных в сегменты «Синтез атакующего воздействия» и «Синтез массивов взаимодействия пользователей» с целью дальнейшего синтеза сетевого трафика, массивов биллинговой информации и журналов ТКО.

Сегмент «Синтез атакующего воздействия» построен на основе разработанных программных средств, реализующих функционал генераторов комплексного атакующего воздействия и фонового сетевого трафика. «Программный комплекс нагрузочного тестирования систем обнаружения компьютерных атак с применением генетического алгоритма» [17] и «Программный комплекс синтеза массивов данных для стенда тестирования телекоммуникационного оборудования» [18] предназначены для автоматизированного нагрузочного тестирования СОА и ТКО с применением генетического алгоритма. Комплексы позволяют проводить натурное тестирование СОА и ТКО в изолированной сетевой среде с применением синтезированного сетевого трафика, имитирующего комбинацию сетевого трафика штатного информационного взаимодействия узлов компьютерной сети и атакующего воздействия, генерировать вариативный сетевой трафик с интеграцией имитируемого атакующего воздействия в соответствии со сценарием учебной задачи. Формирование оптимального набора характеристик для синтеза трафика обеспечивается применением генетического алгоритма.

Сегмент «Центр мониторинга» имитирует инфраструктуру и функциональные задачи типового центра мониторинга системы ГосСОПКА, включая сбор информации с сенсоров СОА, накопление информации о компьютерных атаках в базе данных (БД КА), организацию мониторинга на АРМ дежурной смены и ведение аналитической работы на АРМ аналитиков. Работа аналитика по разбору инцидентов ИБ поддерживается специально разработанным программным обеспечением

«Карта провайдеров сети Интернет», назначение которой — выявлять и визуализировать на карте территориальную принадлежность IP-адресов и юридические адреса Интернет-провайдеров, владеющих IP-адресами на территории Российской Федерации.

Сегмент «Ситуационный центр» является основным и завершающим цепочку расследования инцидента ИБ, предназначен для визуализации хода проведения мероприятий по расследованию компьютерных инцидентов в рамках взаимодействия руководителей, аналитиков и технических специалистов, обеспечивающих расследование инцидента ИБ. В основе сегмента лежат распространенные ИАСБ, в которые стекается информация из остальных сегментов. Путем анализа поступающей информации из «Центра мониторинга» формируются сведения о территориальной принадлежности атакующих и модели нарушителя. Из сегмента «Интернет-провайдер» по запросам передается информация, содержащая сетевой трафик, массивы журналов ТКО, массивы биллинговой информации. Результатами работы ИАСБ являются сведения о субъектах атакующего воздействия.

IDEF0-схемы основных блоков разработанного комплекса программных средств АОС киберполигона по расследованию инцидентов ИБ демонстрируют взаимосвязь процессов при организации и проведении учений по ИБ (рисунок 16 – рисунок 20).

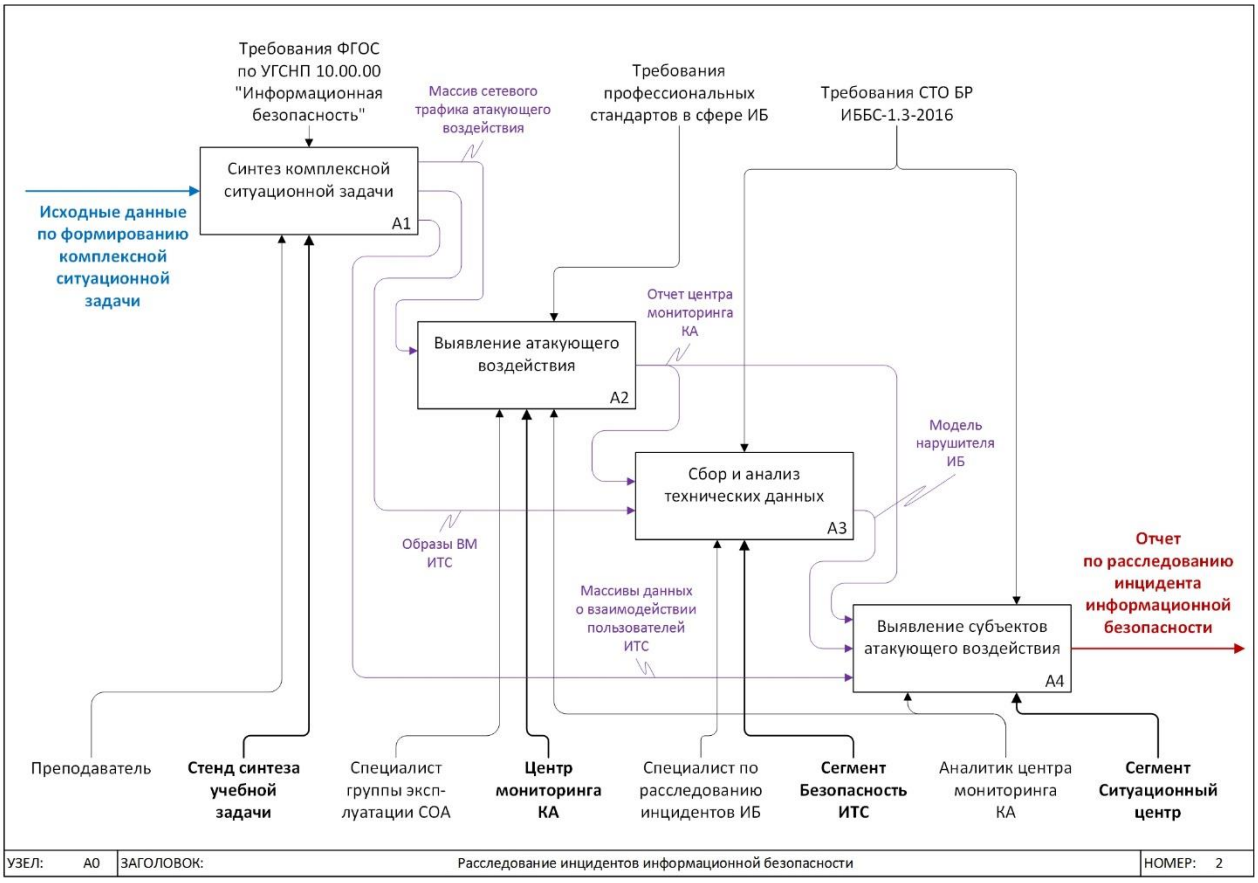

Рисунок 16. IDEF0-схема A0 основных процессов АОС киберполигона

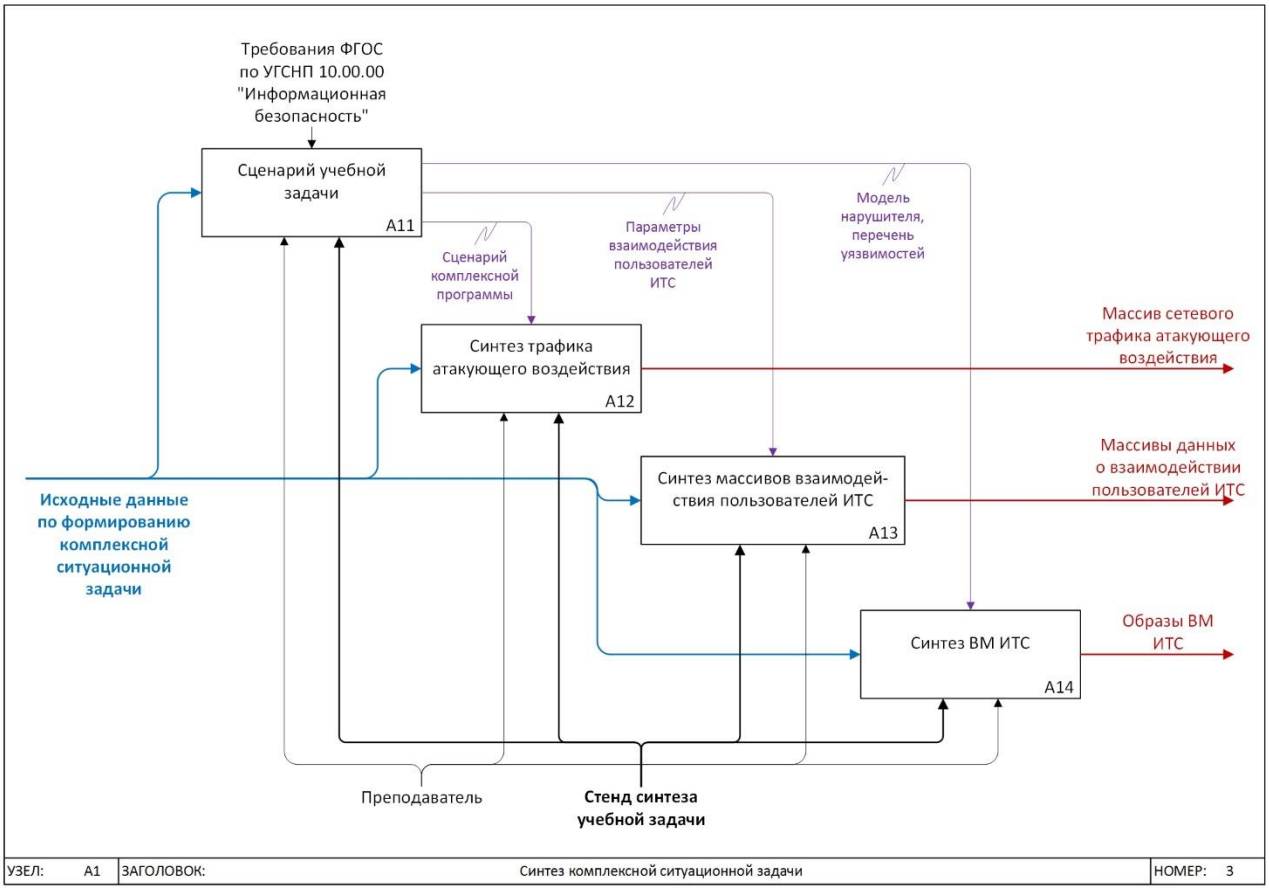

Рисунок 17. IDEF0-схема A1 процесса синтеза комплексной ситуационной задачи

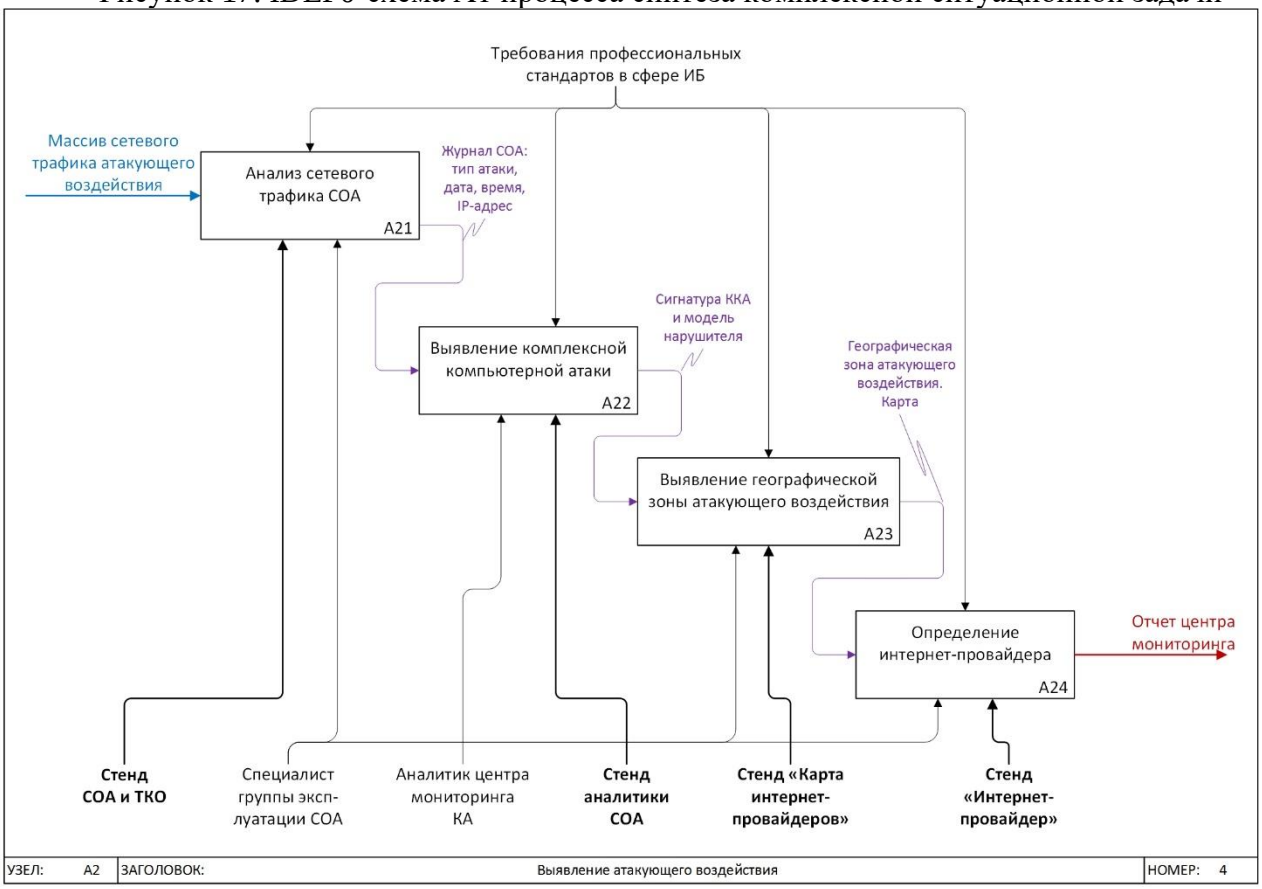

Рисунок 18. IDEF0-схема A2 процесса выявления атакующего воздействия

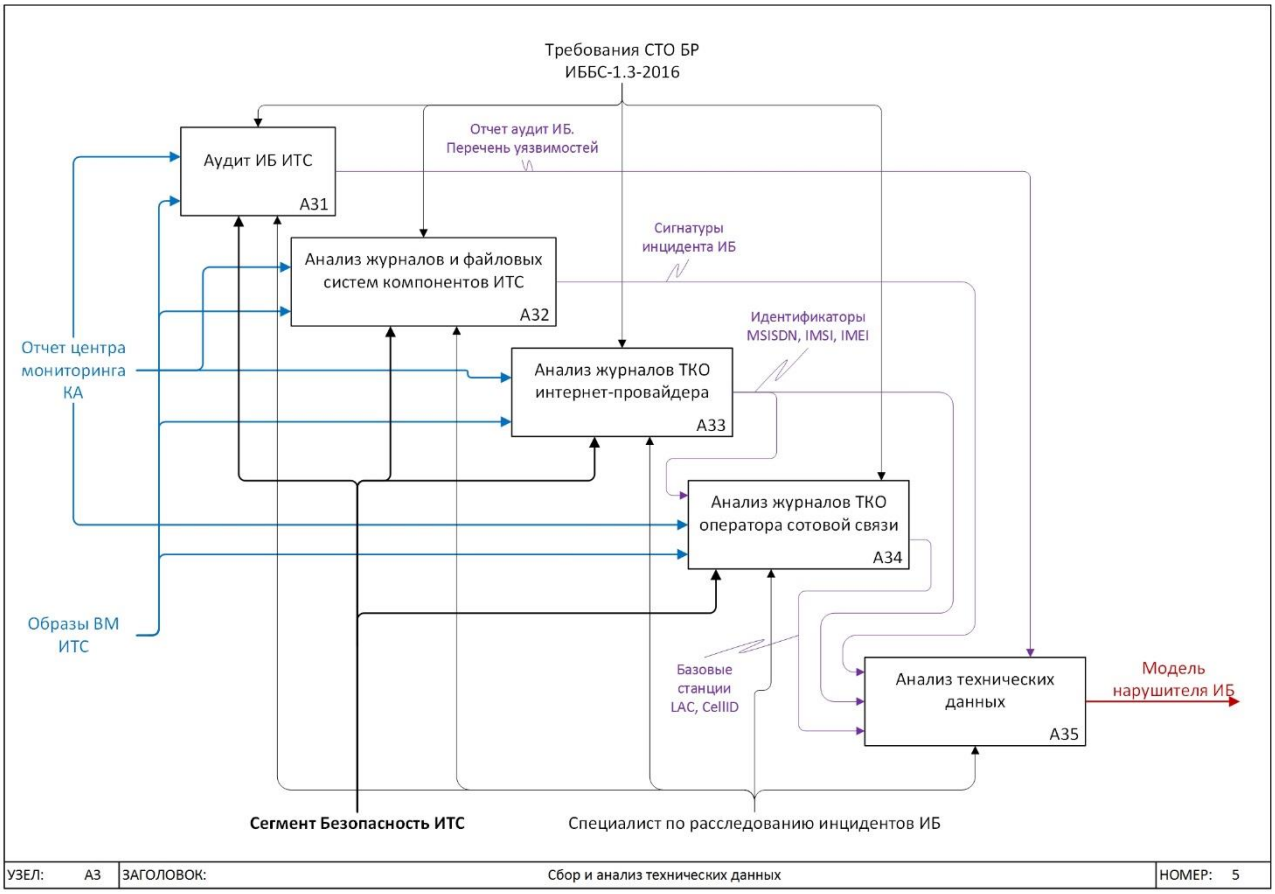

Рисунок 19. IDEF0-схема A3 процесса сбора и анализа технических данных

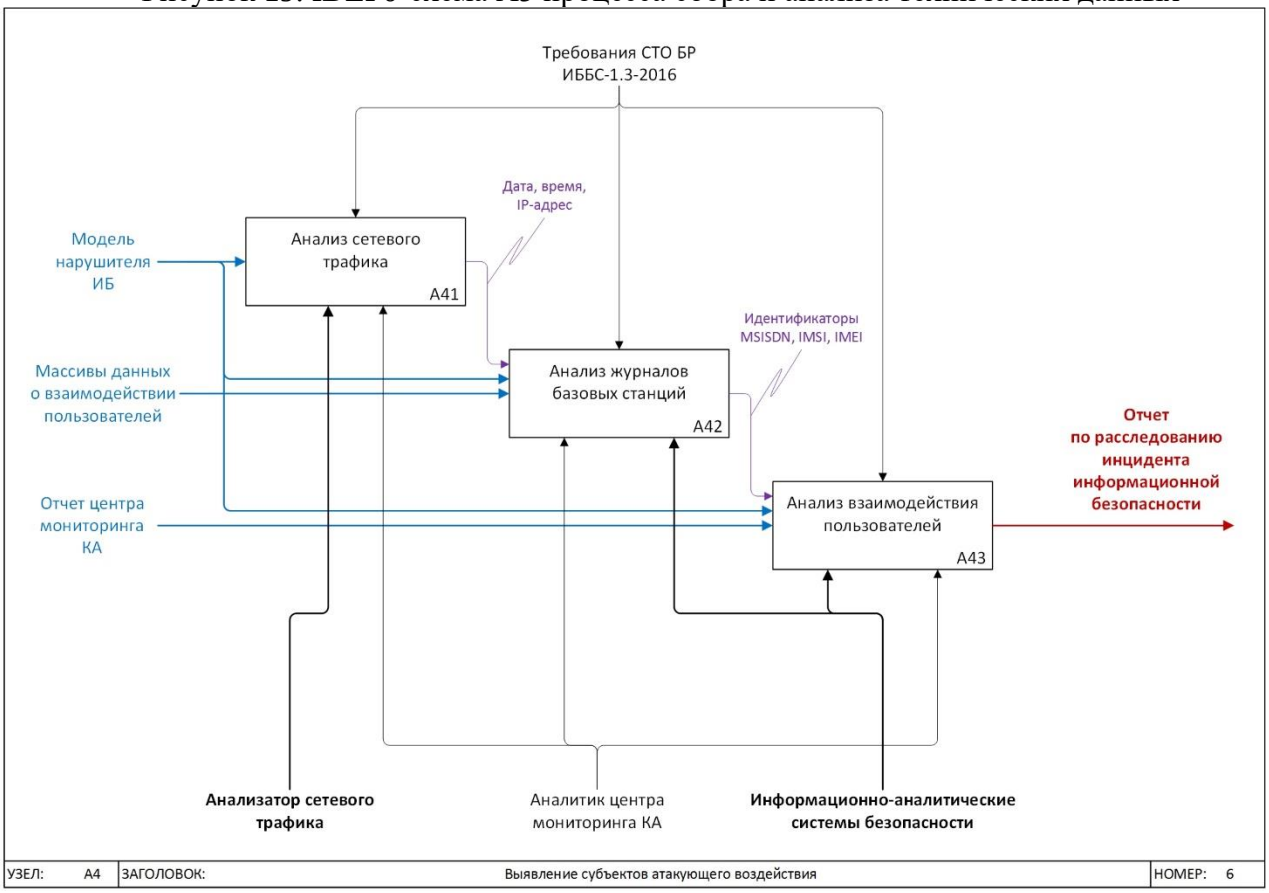

Рисунок 20. IDEF0-схема A4 процесса выявления субъекта атакующего воздействия

В основе сегмента «Синтез массивов взаимодействия пользователей» лежит разработанное специализированное программное обеспечение. Алгоритм «Программного обеспечения синтеза массивов данных о сетевом взаимодействии пользователей в составе учебного компьютерного полигона по расследованию инцидентов информационной безопасности» [15] реализует комплексный метод синтеза массивов условно-реальных данных, основанный на пространственно-временной статистико-событийной модели взаимодействия абонентов ИТС, применяющий модели синтеза сложных сетей, матричную модель хранения статистических характеристик сетевых сред и алгоритмы сетей Петри для формирования комплексных ситуационных задач.

При синтезе фонового массива биллинговой информации используются генерируемые идентификаторы абонентов, статистические распределения видов событий по времени и продолжительности, массивы базовых станций выбранной местности и шаблоны перемещений (рисунок 21).

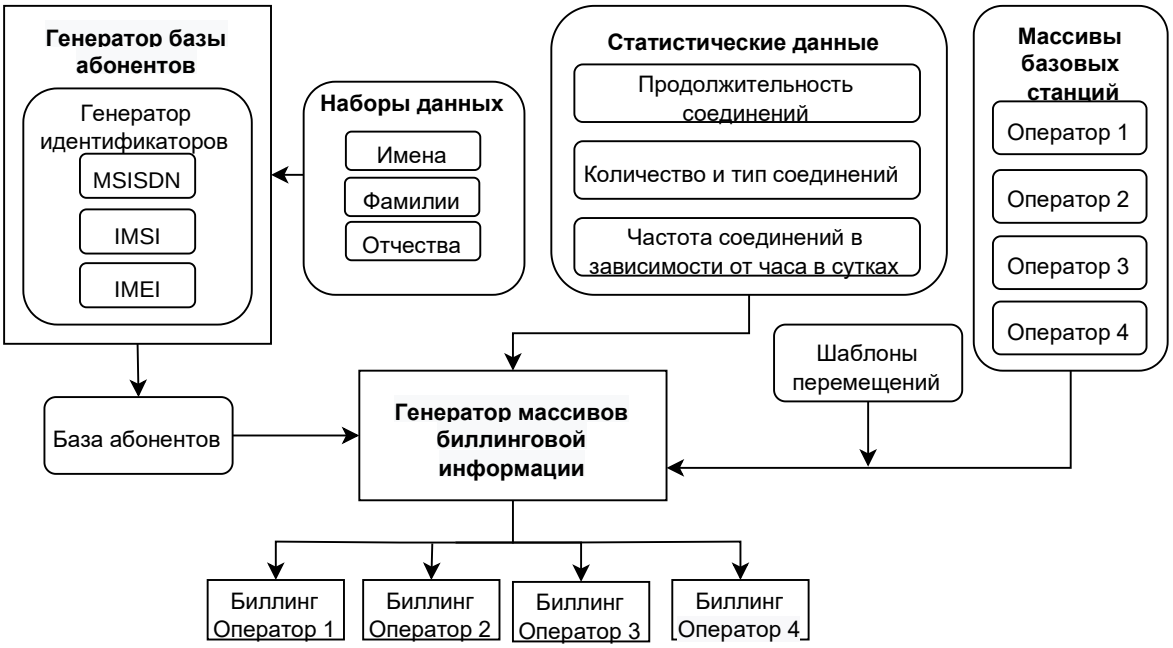

Рисунок 21. Схема синтеза массивов биллинговой информации

«Программное обеспечение синтеза массивов данных для стенда тестирования информационно-аналитических систем безопасности» [16] позволяет на основе модифицированной модели синтеза сложных сетей формировать массивы условно-реальных данных о взаимодействии пользователей в информационно-телекоммуникационных сервисах, предназначенные для тестирования информационно-аналитических систем безопасности. Алгоритм применяет модель Ваттца-Строгатца для синтеза структуры графа, описывающего взаимодействие в сетях операторов сотовой связи, модель Эрдеша-Реньи для задания начального распределения ребер социального графа, модель Барабаши-Альберт для формирования статической структуры сервиса социальных сетей.

Таким образом, киберполигон, представленный комплексом моделей, алгоритмов, программного обеспечения и экспериментальных стендов для тестирования ССЗИ с применением синтезируемых тестовых массивов данных, создает имитационную среду, обеспечивающую комплексность и вариативность тестового воздействия, и позволяет осуществлять автоматизированное тестирование ССЗИ. Киберполигон базируется на разработанном методе имитационного моделирования интерактивной сетевой среды для тестирования ССЗИ. Предложенный метод, в свою очередь, основан на оригинальной комплексной модели интерактивной сетевой среды функционирования ССЗИ, учитывающей статические и динамические характеристики ИТС на сетевом, транспортном и прикладном уровнях сетевого взаимодействия, а также на выделении структурных элементов сетевого трафика реальных сетей с учетом функционального предназначения тестируемого ССЗИ, обеспечивает вариативность имитируемых ИТС и динамику развития ситуационных задач. В рамках метода воздействие на тестируемый образец ССЗИ осуществляется комбинацией двух видов трафика: фонового и атакующего, где для массивов фонового сетевого трафика применяется матричная модель, хранящая статистические распределения характеристик сетевой среды функционирования, а синтез атакующих (ситуационных) массивов данных осуществляется на основе алгоритмов сетей Петри, где ситуационные задачи представляют собой формируемую по определенным правилам последовательность ЭТВ.

Создание ситуационных задач при тестировании ССЗИ осуществляется на основе предложенного метода синтеза и анализа атакующего воздействия и ситуационных задач, использующего предложенную теоретико-графовую модель распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов, что позволяет формировать сценарии действий нарушителя и генерировать граф атакующего воздействия, используемый в процессе анализа защищенности ИТС. С целью выявления ранее неизвестных уязвимостей ССЗИ к сетевым атакам типа «отказ в обслуживании», приводящим к нарушению производительности ССЗИ при определенных сочетаниях параметров входных данных, не являющихся пороговыми, в состав киберполигона включен стенд тестирования ТКО, основанный на применении эволюционно-генетического подхода. Для тестирования ИАСБ предложен метод синтеза массивов условно-реальных данных, использующий пространственно-временную статистико-событийную модель взаимодействия абонентов ИТС, модели синтеза сложных сетей и алгоритмы сетей Петри для формирования комплексных ситуационных задач.

Адекватность предложенных моделей и алгоритмов, а также их программной реализации подтверждена серией экспериментов по выявлению уязвимостей в программном обеспечении ССЗИ, а также при расследовании инцидентов ИБ, что отражено в актах внедрения результатов диссертационного исследования в ООО «Уральский центр систем безопасности».

ЗАКЛЮЧЕНИЕ

Итоги диссертационного исследования состоят в формулировании и решении научной проблемы, имеющей важное значение для народного хозяйства и заключающейся в создании научно-методического инструментария при синтезе интерактивной сетевой среды для учебно-научных компьютерных полигонов, позволяющего автоматизировать процессы синтеза тестовых массивов данных для тестирования ССЗИ с учетом вариативности сетевой среды и комплексности атакующего воздействия, в том числе с целью подготовки специалистов по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также по реагированию на компьютерные инциденты. Предложенное решение в виде научно-методического инструментария, представляющего собой комплекс методов, моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных в составе учебно-научного компьютерного полигона в сфере ИБ позволяет достичь поставленной цели — повышения показателей защищенности ИТС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования, что вносит значительный вклад в повышение защищенности ИТС и ИС. Результаты имеют межотраслевой характер, использованы как на предприятиях и организациях, в том числе для тестирования ССЗИ, так и в образовательных учреждениях министерства науки и высшего образования Российской Федерации. Предложенный научно-методический инструментарий практико-ориентирован, универсален, опирается на современные методы математического моделирования систем и сигналов, с некоторой степенью адаптации пригоден для тестирования ССЗИ любого типа.

Перспективами дальнейшей разработки темы исследования является:

— развитие методологии и научно-методического инструментария исследования моделей сетевых сред для тестирования перспективных ССЗИ, в том числе средств ГосСОПКА, обеспечивающих ликвидацию последствий компьютерных атак, поиск признаков компьютерных атак в сетях электросвязи, а также средств, применяемых в сфере компьютерной криминалистики;

— создание моделей, имитирующих сетевое взаимодействие в современных мессенджерах и ИТС на базе «облачных» технологий, в развитие научно-методического инструментария компьютерных полигонов в сфере ИБ.

Цель диссертационного исследования достигнута. Все поставленные на исследование научные задачи решены в полной мере.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи, опубликованные в рецензируемых научных журналах и изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. Gaidamakin N. File Operations Information Collecting Software Package Used in the Information Security Incidents Investigation / Gaidamakin, N., Gibilinda, R. & **Sinadsky, N.** // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0559-0562. (0,4 п.л./0,1 п.л.) (Scopus).
2. Gaidamakin N. Method of Forming the Static Structure of Social Graphs in the Problem of Modeling Interaction Between Users of Information and Telecommunication Services / Gaidamakin, N., **Sinadsky, N.** & Sushkov, P. // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0586-0588. (0,3 п.л./0,1 п.л.) (Scopus).
3. Semenishchev I. Method for Forming the Dynamic Components of Conditionally Real Data Arrays Based on Color Petri Net Algorithms for Organizing a Computer Training Platform for Investigating Information Security Incidents / Semenishchev, I., Sinadskiy, A., Sinadsky, M., **Sinadsky, N.** & Sushkov, P. // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0582-0585. (0,4 п.л./0,1 п.л.) (Scopus).
4. Гайдамакин Н.А. Комплексный имитационно-статистический метод синтеза массивов условно-реальных данных на основе структурно-параметрической модели взаимодействия пользователей информационно-телекоммуникационных сервисов / Гайдамакин Н.А., **Синадский Н.И.**, Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2020. — № 1 (35). — С. 12–23. (1,3 п.л./0,4 п.л.)
5. Гайдамакин Н.А. Метод экспресс-анализа событий, связанных с воздействиями на файлы, предназначенный для расследования инцидентов информационной безопасности / Гайдамакин Н.А., Гибилинда Р.В., **Синадский Н.И.** // Вестник СибГУТИ. — 2020. — № 4. — С. 3-10. (0,8 п.л./0,6 п.л.)
6. Гайдамакин Н.А. Событийная модель процесса идентификации воздействий на файлы при расследовании инцидентов информационной безопасности, основанная на математическом аппарате сетей Петри / Гайдамакин Н.А., Гибилинда Р.В., **Синадский Н.И.** // Вестник СибГУТИ. — 2020. — № 1. — С. 73-88. (0,9 п.л./0,3 п.л.)
7. **Sinadskiy N.** Statistical Model for the Synthesis of Billing Information / **Sinadskiy, N.**, Sinadskiy, A. & Semenishchev, I. // 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2019. – pp. 303-306. (0,4 п.л./0,1 п.л.) (Scopus, WoS)
8. Семенищев И.А. Синтез массивов биллинговой информации на основе статистико-событийной модели взаимодействия абонентов сетей сотовой связи /

Семенищев И.А., Синадский А.Н., **Синадский Н.И.**, Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2018. — № 1 (27). — С. 47–56. (1,0 п.л./0,4 п.л.)

9. Агафонов А.В. Автоматизация тестирования сетевых средств защиты информации на основе применения эволюционно–генетического подхода / Агафонов А.В., **Синадский Н.И.** // Математические структуры и моделирование. — 2018. — № 2 (46). — С. 125-134. (1,0 п.л./0,5 п.л.)

10. **Синадский Н.И.** Модификация методов анализа социальных графов на основе применения атрибутивных компонентов учетных записей для идентификации сообществ пользователей социальных сетей / **Синадский Н.И.**, Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2017. — № 2 (24). — С. 32–40. (0,9 п.л./0,5 п.л.)

11. Агафонов А.В. Тестирование защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением генетического алгоритма / Агафонов А.В., **Синадский Н.И.** // Вестник УрФО. Безопасность в информационной сфере. — 2017. — № 2 (24). — С. 4–8. (0,5 п.л./0,2 п.л.)

12. Агафонов А.В. Структура и принцип работы комплекса тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании» / Агафонов А.В., **Синадский Н.И.** // Вестник УрФО. Безопасность в информационной сфере. — 2015. — № 4 (18). — С. 4–11. (0,9 п.л./0,4 п.л.)

13. Богданов В.В. Алгоритм обнаружения комплексных компьютерных атак на основе признаков, получаемых путем формализации положений политики безопасности с использованием аппарата иерархических нечетких систем / Богданов В.В., **Синадский Н.И.** // Проблемы информационной безопасности. Компьютерные системы. — 2008. — № 1. — С. 13–26. (1,6 п.л./0,8 п.л.)

14. Богданов В.В. Система обнаружения компьютерных атак на основе положений политики безопасности / Богданов В.В., **Синадский Н.И.** // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2007. — Т. 2. — С. 11–14. (0,4 п.л./0,2 п.л.)

Свидетельства о регистрации программ для ЭВМ:

15. Свидетельство о государственной регистрации программы для ЭВМ № 2022611054. Программное обеспечение синтеза массивов данных о сетевом взаимодействии пользователей в составе учебного компьютерного полигона по расследованию инцидентов информационной безопасности / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021669185 от 25.11.2021; дата государственной регистрации в Реестре программ для ЭВМ 19.01.2022. — 1 с.

16. Свидетельство о государственной регистрации программы для ЭВМ № 2022611053. Программное обеспечение синтеза массивов данных для стенда тестирования информационно-аналитических систем безопасности / Синадский

М.Н., **Синадский Н.И.** — Заявка № 2021669809 от 27.11.2021; дата государственной регистрации в Реестре программ для ЭВМ 19.01.2022. — 1 с.

17. Свидетельство о государственной регистрации программы для ЭВМ № 2021681075. Программный комплекс нагрузочного тестирования систем обнаружения компьютерных атак с применением генетического алгоритма / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021680589 от 05.12.2021; дата государственной регистрации в Реестре программ для ЭВМ 17.12.2022. — 1 с.

18. Свидетельство о государственной регистрации программы для ЭВМ № 2022611833. Программный комплекс синтеза массивов данных для стенда тестирования телекоммуникационного оборудования / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021680409 от 05.12.2021; дата государственной регистрации в Реестре программ для ЭВМ 02.02.2022. — 1 с.

СПИСОК СОКРАЩЕНИЙ

АОС — автоматизированная обучающая система
ИБ — информационная безопасность
ИАСБ — информационно-аналитические системы безопасности
ИС — информационная система
ИТС — информационно-телекоммуникационная сеть
КСЗ — комплексная ситуационная задача
САЗ — система анализа защищенности
СОА — система обнаружения атак
ССЗИ — сетевое средство защиты информации
ССФ — сетевая среда функционирования
ТКО — телекоммуникационное оборудование
ЭТВ — элементарное тестирующее воздействие