ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИИ Б.Н. ЕЛЬЦИНА»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – РТФ

УЧЕБНО-НАУЧНЫЙ ЦЕНТР «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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

Диссертация на соискание ученой степени
доктора технических наук

Екатеринбург
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 принят ряд основополагающих документов [1-29]. Основными являются Доктрина информационной безопасности Российской Федерации [1], в которой на основе анализа информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации, и Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [7], 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 [5].

В большинстве крупных вузов технического профиля организована подготовка студентов по специальностям укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» [30-33]. 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, реализующие сетевую инфраструктуру объектов ИТС. Актуальность создания киберполигонов определена Федеральным проектом «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» [3, 4, 10], в рамках которой предусмотрено выполнение работ по созданию киберполигона [9] для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности.

Одной из задач учебно-научного компьютерного полигона является создание условий для проведения научных исследований в сфере обеспечения информационной безопасности, в том числе для тестирования программного обеспечения, оборудования, элементов информационных технологий на реализацию функций информационной безопасности [20-22] и защищенность как ИТС в целом, так и отдельных средств защиты информации, среди которых выделяются технические, программные, программно-аппаратные и иные средства, обеспечивающие выявление уязвимостей ИТС, обнаружение, предупреждение и ликвидацию последствий компьютерных атак, а также реагирования и расследования инцидентов информационной безопасности.

Среди указанных средств основными являются системы обнаружения компьютерных 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 информационной безопасности и ведения аналитической работы применяются ИАСБ, одной из основных функциональных задач которых является поиск взаимосвязей между объектами различных компьютерных сетей, в том числе IP-сетей, социальных сетей и сетей операторов сотовой связи.

Некорректная работа СОА может привести к пропуску атакующего воздействия и возможности нарушителя 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 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 сложности алгоритмов, лежащих в основе ССЗИ, и конфигурирования их программной реализации программные средства ССЗИ должны быть подвергнуты комплексному тестированию в процессе анализа защищенности. 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 (в процессе аудита информационной безопасности).

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 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 информационной безопасности требует анализа больших и разноплановых массивов данных, фиксируемых современными ССЗИ.

Известные компьютерные полигоны, а также методики тестирования ССЗИ, используемые при проведении мероприятий по анализу защищенности, не позволяют в полном объеме моделировать в процессе тестирования условия, существующие при проведении современных комплексных воздействий (атак), что снижает результативность мероприятий по анализу защищенности как отдельных ССЗИ, так и ИТС. 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 [8], 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 условия проведения комплексного атакующего воздействия 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 информационной безопасности является создание условий для формирования практико-ориентированных компетенций слушателей в части тестирования ССЗИ, выявления уязвимостей ИТС и ИС, обнаружения компьютерных атак и реагирования на инциденты информационной безопасности. 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 или критического) воздействия. В состав аномального воздействия должны быть включены комплексные ситуационные задачи (тесты), предполагающие выявление инцидентов информационной безопасности, их идентификацию и формирование отчетных аналитических документов обучающимися. Должен быть сформирован полный цикл профессиональных компетенций специалистов по расследованию инцидентов информационной безопасности в ИТС и ИС, 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.

Реализация задач по обеспечению безопасности ИТС и ИС требует адекватного развития теоретических основ 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*[1] *моделирования* интерактивной[2] сетевой среды для компьютерных полигонов. Наблюдается объективное противоречие между потребностями по комплексному тестированию ССЗИ с учетом непрерывного развития информационных технологий и современных ИТС и ИС и существующим научно-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 информационной безопасности в ИТС и ИС, является актуальной научной проблемой.

Степень разработанности темы исследования. Построение компьютерных полигонов в сфере информационной безопасности — активно обсуждаемая проблема, над решением которой работают многие отечественные и зарубежные исследователи [39 – 256]. 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:

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

– в области алгоритмов выявления аномалий — А.А. Захарова, А.М. Ивашко, Д.Ю. Гамаюнова, П.Д. Зегжды, И.В. Котенко, 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 синтеза, создания и тестирования ССЗИ — Ю.Д. Королькова, А.В. Козачка, А.С. Кислицина, В.В. Липаева, П.С. Ложникова, А.Н. Соколова, С.С. Титова, А.А. Шелупанова, А.В. Царегородцева, 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 информационной безопасности.

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 информационной безопасности 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 информационной безопасности на объектах ИТС и ИС.

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 информационной безопасности для обеспечения высокого уровня защищенности 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 информационной безопасности.

2. Разработка комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности, 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 информационной безопасности.

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 информационной безопасности.

Теоретическая значимость. Создан новый научно-методический аппарат, имеющий существенное значение для развития методов, моделей, алгоритмов и программных средств обеспечения информационной безопасности. 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 уязвимостей при тестировании ССЗИ с учетом вариативности внешней сетевой среды и комплексности атакующего воздействия, организовать практико-ориентированное обучение специалистов по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также по реагированию

на инциденты информационной безопасности, 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[1] (опубликовано в [261, 264, 265]).

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[1] (опубликовано в [260 – 262, 266, 268]).

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[1] (опубликовано в [263, 264, 271]).

---

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

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[1] (опубликовано в [259, 267, 269 – 276]).

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.

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 компьютерных полигонов.

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.);

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

— 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 информационной безопасности, 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 [259-312]. 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 информационной безопасности 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. В совместных работах с Р.В. Гибилиндой в рамках разработанного автором комплексного метода синтеза интерактивной сетевой среды применен аппарат сетей Петри для моделирования и синтеза динамической составляющей ситуационных задач при расследовании инцидентов информационной безопасности. В совместных работах с А.В. Агафоновым автором предложено и обосновано применение эволюционно-генетического подхода к синтезу атакующего воздействия в задаче тестирования ТКО. В совместных работах с В.В. Богдановым, А.Р. Зайникаевым и А.А. Муратовым автором предложена и обоснована методика тестирования СОА с применением тео-

ретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов. В работах с И.А. Семенищевым, П.В. Сушковым, А.Н. Синадским, М.Н. Синадским автором предложен имитационно-статистический метод синтеза массивов условно-реальных данных, основанный на пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС.

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 [1 – 258] наименований на 27 страницах.

1. АНАЛИЗ ПРОБЛЕМЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ ПОЛИГОНОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Анализ актуальности создания компьютерных полигонов

1.1.1. Анализ задач, решаемых компьютерными полигонами в сфере информационной безопасности

Указом Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [2] в части достижения целевых показателей по обеспечению информационной безопасности предусматриваются, в том числе задачи по совершенствованию средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта, а также обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления.

Федеральным проектом «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» [3, 4, 9, 10] определена задача создания компьютерных полигонов (киберполигонов) в области информационной безопасности и информационных технологий для обучения современным практикам обеспечения безопасности. Под киберполигонами понимается инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них.

Целями создания киберполигонов являются, в том числе [10]:

— системное развитие кадрового потенциала Российской Федерации в области информационной безопасности и формирование практических навыков защиты

от реализации угроз информационной безопасности и компьютерных атак у учащихся, специалистов, руководителей в области информационных технологий и информационной безопасности;

— повышение уровня защищенности программного и аппаратного обеспечения информационной и промышленной автоматизированной инфраструктуры организаций Российской Федерации, включая программное обеспечение в составе Единого реестра российских программ для ЭВМ;

— совершенствование методического и нормативного обеспечения процессов информационной безопасности организаций в Российской Федерации.

Среди задач, для решения которых создаются киберполигоны, выделяются:

— проведение киберучений[1], соревнований и практических тренировок по информационной безопасности;

— отработка практических навыков выявления компьютерных атак, расследования инцидентов информационной безопасности, внедрения превентивных мер по предупреждению компьютерных атак;

— тестирование программного обеспечения, оборудования, элементов информационных технологий на реализацию функций информационной безопасности, защищенность и отсутствие уязвимостей;

— тестирование средств защиты информации на реализацию функциональных возможностей, защищенность и наличие уязвимостей.

Техническая инфраструктура киберполигона должна обеспечивать, в том числе:

— информационную систему, позволяющую проводить активные атакующие действия на инфраструктуры для эмуляции атаки;

— базовые типовые средства защиты информации для создаваемых элементов инфраструктур;

— базовые типовые средства мониторинга и управления инцидентами информационной безопасности в сетевых инфраструктурах;

[1] Киберучения — процесс практической подготовки и освоения навыков у учащихся, специалистов, экспертов и руководителей по обеспечению информационной безопасности путем моделирования компьютерных атак и отработки реакций на них

— средства моделирования типовых пользовательских операций при работе в информационных системах;

— средства моделирования действий внешнего и внутреннего нарушителей, реализующие автоматические компьютерные атаки в зависимости от инфраструктуры компьютерной сети.

Основной информационной технологией, применяемой при построении киберполигонов, является технология виртуализации, позволяющая, в том числе с использованием «облачных» технологий создавать совокупность информационных и технологических инфраструктур, эмулирующих корпоративные сети организаций, индустриальной инфраструктуры (автоматизированной системы управления технологическим процессом).

Автоматизированные обучающие системы (АОС) и компьютерные тренажеры стали привычным элементом практико-ориентированного обучения. АОС в классическом понимании — компьютерная сеть, состоящая из компьютеров разной мощности, видео- и аудиотехники, различных сервисных средств, предназначенная для поддержки учебного процесса в интерактивном режиме работы всех его участников. Для своего функционирования АОС требует разнообразного обеспечения, в том числе программного, технического и информационного методического.

Научные работы в сфере разработки имитационно-моделирующих обучающих комплексов (тренажеров), компонентов электронного учебника, компьютерных лабораторных практикумов, интерактивных компьютерных тренажеров, распределенных информационных образовательных систем показывают актуальность данного направления [202-208]. Ведутся разработки в сфере концепции «виртуального полигона», что связано с необходимостью рассмотрения сложных моделей для исследования поведения динамических объектов, требующих применения высокопроизводительной вычислительной техники. Разрабатываемые виртуальные полигоны, компьютерные тренажеры, применяемые для изучения сложных технических объектов, требуют создания комплексов математических моделей различных технологических процессов, различных явлений. Одно из предъяв-

ляемых требований к АОС — возможность оперативной коррекции параметров при обнаружении отклонений характеристик от данных, полученных в реальной системе, что должно обеспечиваться реализованными математическими моделями.

Основным требованием, предъявляемым к математическим моделям АОС, является адекватность результатов работы модели в рамках конкретной тренажерной задачи тем процессам, которые происходят в реальных устройствах и системах. В свою очередь адекватность моделирования определяется структурой математической модели и оптимальностью выбора параметров в определенной структуре. Разработка компьютерных тренажеров требует эффективных и легко реализуемых машинно-ориентированных методов и алгоритмов имитации динамических режимов, обеспечивающих необходимую точность имитации при допустимой сложности реализации.

В работах отмечается, что применение АОС одновременно с повышением качества подготовки обучающихся обеспечивает снижение интегральных затрат на подготовку персонала, так как проведение натурных или полномасштабных тренировок связано с существенными затратами на их организационное, техническое и материальное обеспечение. Вместе с тем основное внимание в указанных работах [202-208] уделено формированию АОС, как среды обучения, технические модели для создания имитируемой внешней среды, позволяющей проводить обучение по направлению 10.00.00 «Информационная безопасность», не приводятся. Компьютерный полигон как единое целое для обнаружения, предупреждения КА и расследования инцидентов информационной безопасности является комплексом многоуровневых приложений, что требует создания интерактивных моделей и распределенной вычислительной среды.

Кроме того, в «Национальной стратегии развития искусственного интеллекта на период до 2030 года» [8] обозначена необходимость повышения доступности и качества данных, необходимых для развития технологий искусственного интеллекта, включая разработку унифицированных и обновляемых методологий описания, сбора и разметки данных, к которым относятся данные, применяемые

для функционирования киберполигонов. Синтез условно-реальных данных, описывающих атакующие воздействия и взаимодействие пользователей ИТС, осуществляемый в соответствии с научно обоснованными моделями, является актуальной задачей.

1.1.2. Анализ компетентностной модели специалиста при создании компьютерных полигонов в сфере информационной безопасности

При подготовке специалистов в соответствии с федеральными государственными образовательными стандартами высшего образования (далее — ФГОС ВО) по укрупненной группе специальностей и направлений подготовки (далее — УГСНП) 10.00.00 «Информационная безопасность» в качестве тренировочной базы должны использоваться аудитории учебно-тренировочных средств моделирования информационно-коммуникационной среды (киберполигоны), включающие учебные стенды, реализующие сетевую инфраструктуру объектов ИТС и ИС.

Задачей компьютерных полигонов в сфере информационной безопасности является создание условий для формирования практико-ориентированных компетенций студентов в части тестирования ССЗИ, выявления уязвимостей ИТС, обнаружения компьютерных атак и реагирования на компьютерные инциденты (рисунок 1.1).

Киберполигон должен быть оснащен лабораториями, позволяющими осуществлять обнаружение КА, предупреждение КА (выявление уязвимостей ИТС), расследование инцидентов информационной безопасности (включая ликвидацию последствий КА). Каждая из лабораторий оснащается соответствующими стендами тестирования ССЗИ. Основой разрабатываемого полигона является АОС, позволяющая максимально реалистично имитировать состояние сетевой среды функционирования ССЗИ. При этом сетевая среда разрабатывается таким образом, чтобы обеспечивать вариативность информационных технологий, применяемых в ИТС, адаптивность тестовых задач к различным уровням подготовленности

обучаемых, интерактивность, возможность изменения характеристик среды в зависимости от действий обучаемых.

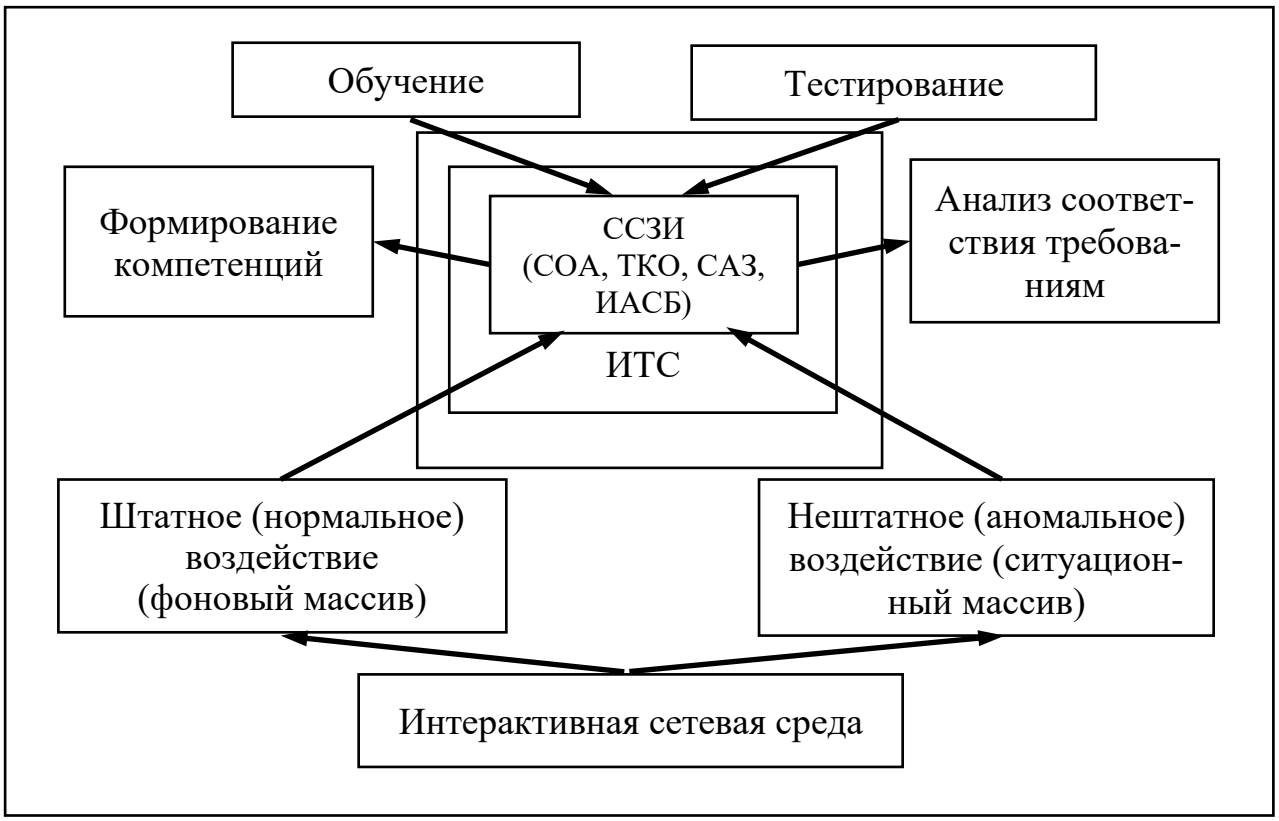

Рисунок 1.1. Автоматизированная обучающая система учебно-научного компьютерного полигона в сфере информационной безопасности

Одной из задач учебно-научного компьютерного полигона является создание условий для проведения научных исследований в сфере обеспечения безопасности ИТС, в том числе для тестирования отдельных ССЗИ и защищенности объектов ИТС в целом. Изучение и тестирование различных ССЗИ предусматривается ФГОС ВО по направлению 10.04.01 «Информационная безопасность» (уровень — магистратура) и по специальностям 10.05.01 «Компьютерная безопасность», 10.05.02 «Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности» [30-33].

В рамках обучения будущие специалисты в сфере обеспечения информационной безопасности должны получить общепрофессиональные компетенции

в сфере тестирования ССЗИ, выявления уязвимостей ИТС, обнаружения компьютерных атак и расследования компьютерных инцидентов (таблица 1.1). Профессиональные компетенции в обозначенных ФГОС детализируются профессиональными стандартами по направлению информационной безопасности: Код 06.030. Специалист по защите информации в телекоммуникационных системах и сетях; Код 06.031. Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности; Код 06.032. Специалист по безопасности компьютерных систем и сетей; Код 06.033. Специалист по защите информации в автоматизированных системах [34-37].

Таблица 1.1. Компетенции в соответствии с ФГОС 10.05.01, 10.05.02, 10.05.03, 10.05.04.

10.05.01	— ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях; в рамках специализации № 1 «Анализ безопасности компьютерных систем»: — ОПК-1.1. Способен проводить анализ защищенности и осуществлять поиск уязвимостей компьютерной системы; — ОПК-1.2. Способен оценивать корректность программных реализаций алгоритмов защиты информации; — ОПК-1.3. Способен проводить тестирование и использовать средства верификации механизмов защиты информации; в рамках специализации № 4 «Безопасность компьютерных систем и сетей»: — ОПК-4.2. Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения); в рамках специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»: — ОПК-6.1. Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;
10.05.02	— ОПК-13. Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности; — ОПК-15. Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием; — ОПК-9.3. Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям;

10.05.03	— ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем; в рамках специализации № 6 «Безопасность автоматизированных систем в кредитно-финансовой сфере»: — ОПК-6.2. Способен управлять инцидентами информационной безопасности, осуществлять контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы; в рамках специализации № 7 «Анализ безопасности информационных систем»: — ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; — ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации; — ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;
10.05.04	— ОПК-14. Способен оценивать эффективность информационно-аналитических систем методами моделирования; — ОПК-15. Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений на базе ситуационных центров; — ОПК-2.3. Способен решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности

Таблица 1.2. Трудовые функции в соответствии с профессиональными стандартами 06.030, 06.031, 06.032, 06.033.

06.030	— D/03.7. Проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в сфере разработки средств и систем защиты СССЭ от НСД, создания защищенных телекоммуникационных систем (Проводить выбор, исследовать эффективность и разрабатывать технико-экономическое обоснование проектных решений средств и систем защиты СССЭ от НСД, защищенных телекоммуникационных систем с целью обеспечения требуемого уровня защищенности); — E/01.7. Организация функционирования сетей связи специального назначения и их средств связи (Проводить комплексное тестирование, пуск и наладку средств связи сетей связи специального назначения, средств и систем их защиты от НСД); — E/03.7. Контроль защищенности от НСД и функциональности сетей связи специального назначения (Проводить инструментальный мониторинг защищенности сетей связи специального назначения от НСД); — G/01.8. Исследование эффективности способов, средств и систем защиты СССЭ от НСД (Анализировать программные, архитектурно-технические и схемотехнические решения СССЭ с целью выявления потенциальных уязвимостей их защиты от НСД);
06.031	— B/05.7. Исследование эффективности информационно-аналитических систем (Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации);

06.032	— C/01.7. Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации (Оценивать эффективность защиты информации); — C/03.7. Проведение анализа безопасности компьютерных систем (Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах); — C/04.7. Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов (Применять инструментальные средства проведения сертификационных испытаний); — C/05.7. Проведение инструментального мониторинга защищенности компьютерных систем и сетей (Применять инструментальные средства проведения мониторинга защищенности компьютерных систем. Применять методы анализа защищенности компьютерных систем и сетей); — C/06.7. Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов (Прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов); — D/03.8. Разработка и тестирование средств защиты информации компьютерных систем и сетей (Использовать приемы защиты от типовых атак компьютерных систем);
06.033	— B/01.6. Диагностика систем защиты информации автоматизированных систем (Определять источники и причины возникновения инцидентов); — B/06.6. Аудит защищенности информации в автоматизированных системах (Применять инструментальные средства контроля защищенности информации в автоматизированных системах); — D/01.7. Тестирование систем защиты информации автоматизированных систем (Анализировать основные узлы и устройства современных автоматизированных систем).

В указанных профессиональных стандартах, соответствующих профессиональной деятельности выпускников, освоивших программу специалитета по специальностям УГСНП 10.00.00, вводятся трудовые функции и соответствующие умения в сфере тестирования ССЗИ, выявления уязвимостей ИТС, обнаружения компьютерных атак и расследования компьютерных инцидентов (таблица 1.2).

Компетентностная модель специалистов в сфере тестирования ССЗИ, выявления уязвимостей ИТС, обнаружения компьютерных атак и расследования компьютерных инцидентов (рисунок 1.2) позволяет определить перечень объектов и функциональных задач, подлежащих реализации в рамках киберполигона в сфере информационной безопасности.

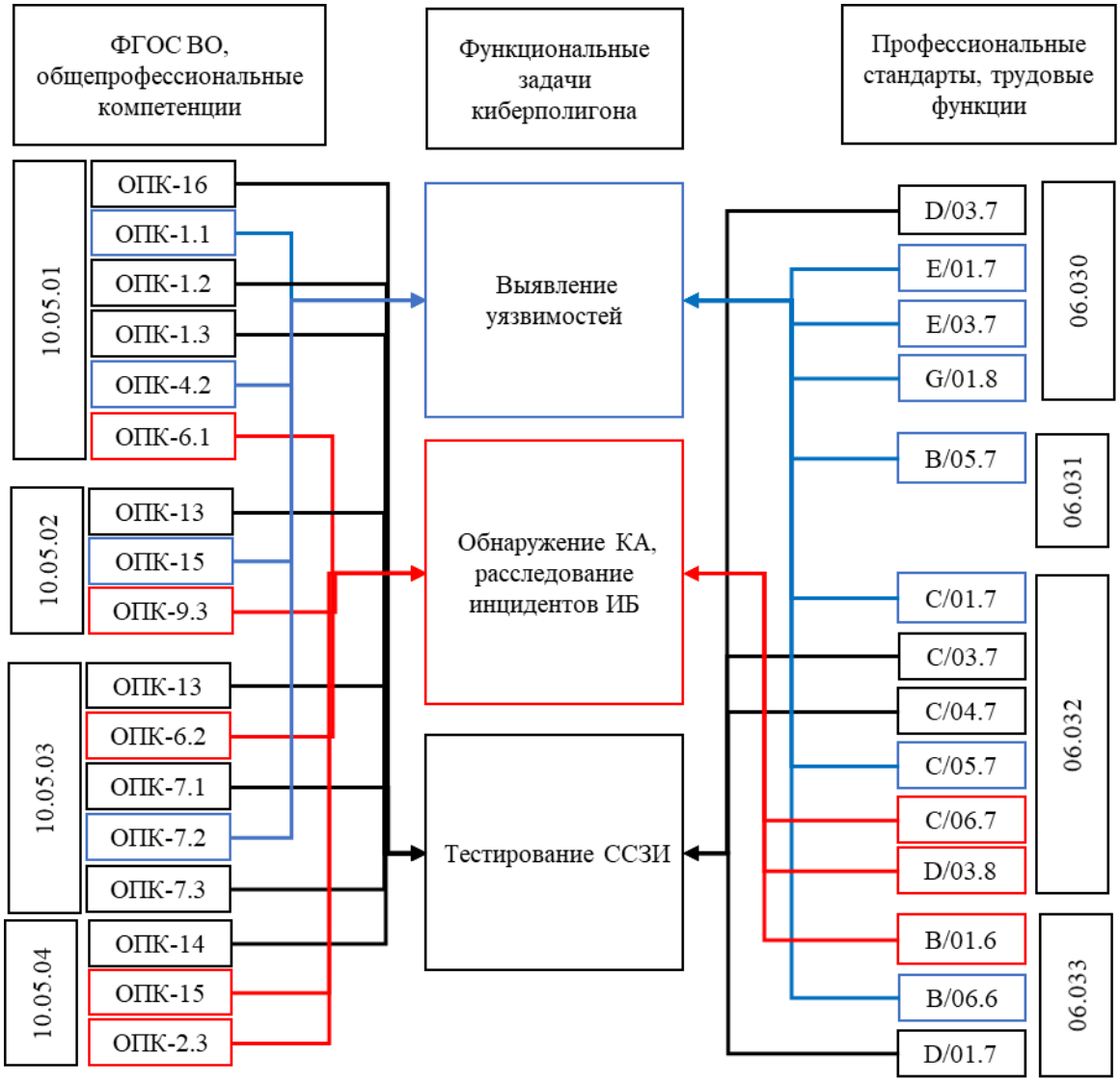

Рисунок 1.2. Компетентностная модель специалистов в сфере тестирования ССЗИ, выявления уязвимостей ИТС, обнаружения компьютерных атак и расследования компьютерных инцидентов

1.2. *Анализ сетевых средств защиты информации как объектов тестирования*

1.2.1. Сетевые средства защиты информации в процессе расследования инцидентов информационной безопасности

Среди средств защиты информации, для тестирования функциональных возможностей, защищенности и наличия уязвимостей которых создаются киберполигоны, выделяются четыре класса систем: системы обнаружения компьютерных атак (системы обнаружения вторжений, СОА), телекоммуникационное оборудование (ТКО), системы анализа защищенности (САЗ), а также информационно-аналитические системы безопасности (ИАСБ). Сетевые средства защиты информации (ССЗИ) предназначены для решения задач обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты.

СОА — средства, обладающие следующими функциональными возможностями:

— сбор и первичная обработка информации, поступающей от источников событий информационной безопасности (далее — события ИБ);

— автоматический анализ событий ИБ и выявление компьютерных инцидентов (компьютерных атак);

— ретроспективный анализ данных и выявление не обнаруженных ранее компьютерных инцидентов.

ТКО — аппаратное обеспечение, используемое в целях передачи информации и преобразования сигналов между каналом общего пользования и конечным оборудованием.

САЗ — средства, обладающие следующими функциональными возможностями:

— сбор и обработка сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации;

— сбор и обработка сведений об уязвимостях и недостатках в настройке ПО, используемого на объектах контролируемых информационных ресурсов;

— учет угроз безопасности информации.

ИАСБ — средства, обеспечивающие информационно-аналитическое сопровождение процессов ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Федеральный закон «Об информации, информационных технологиях и о защите информации» [6] вводит понятия информационной системы и информационно-телекоммуникационной сети:

— информационная система (ИС) — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; ИС включают: государственные ИС — федеральные ИС и региональные ИС, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов, муниципальные ИС, созданные на основании решения органа местного самоуправления, и иные ИС.

— информационно-телекоммуникационная сеть (ИТС) — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Национальным стандартом Российской Федерации ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» [12] введено понятие информационной инфраструктуры как совокупности объектов информатизации, обеспечивающей доступ потребителей к информационным ресурсам, где под объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. Вводится понятие критического объекта как объекта, нарушение непрерывности функционирования которого может нанести значительный ущерб

имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, а также выражаться в причинении вреда жизни или здоровью граждан.

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования устанавливаются ФСТЭК России. В настоящем исследовании не рассматриваются меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации, а также состояние защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

Термин инцидент информационной безопасности (далее — ИБ) определен в ГОСТ Р 53114-2008 как любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность, в том числе утрата услуг, оборудования или устройств, системные сбои или перегрузки, ошибки пользователей, несоблюдение политики или рекомендаций по ИБ, нарушение физических мер защиты, неконтролируемые изменения систем, сбои программного обеспечения и отказы технических средств, нарушение правил доступа. Стандарт Банка России СТО БР ИББС-1.3-2016 [15] вводит в числе других в рамках реагирования на инциденты ИБ следующие задачи:

— определение технических способов и схем реализаций угроз ИБ, целью и (или) результатом которых являются несанкционированное распоряжение денежными средствами и (или) нарушение непрерывности оказания платежных услуг (далее — угрозы ИБ), на основе сбора и анализа технических данных, формируемых объектами информационной инфраструктуры организации БС Российской Федерации и (или) клиентов;

— проведение идентификации субъектов, реализующих угрозы ИБ, на основе результатов обработки технических данных, полученных в рамках реагирования на инциденты ИБ.

При этом с целью определения признаков инцидента ИБ используются СОА, сбор технических данных осуществляется с помощью журналов и массивов сетевого трафика ТКО, с помощью САЗ может формироваться сценарий реализации инцидента ИБ и выявляться состав информационной инфраструктуры, задействованной в реализации инцидента ИБ. ИАСБ применяются для идентификации субъекта атакующего воздействия, вызвавшего инцидент ИБ, на основе результатов анализа технических данных, а также для поиска (выделения) содержательной (семантической) информации, ее анализа и оформления при определении технических способов и схем реализаций угроз ИБ.

1.2.2. Сетевые компьютерные атаки и инциденты информационной безопасности

Компьютерная атака (далее — КА) — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты ИТС и ИС, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [7]. Сетевые КА используют сетевую среду для осуществления удаленного доступа к объекту атаки. В целом КА рассматривается как любая злоумышленная деятельность, направленная против ИТС и ИС.

Систематика[1] КА, расширяемая с точки зрения выявления атакующего воздействия в сетевом трафике (рисунок 1.3), позволяет классифицировать атаки по девяти различным признакам (атакующий, используемый инструмент, тип уязвимости, тип доступа, объект доступа, источник / приемник атаки, результат атаки, цель атаки, этап атаки). КА рассматривается как последовательность отдельных

[1] Систематика — классификация, группировка предметов, явлений

этапов, каждый из которых может быть выполнен несколькими возможными способами для достижения атакующим поставленной цели, причем различные варианты могут быть использованы одновременно.

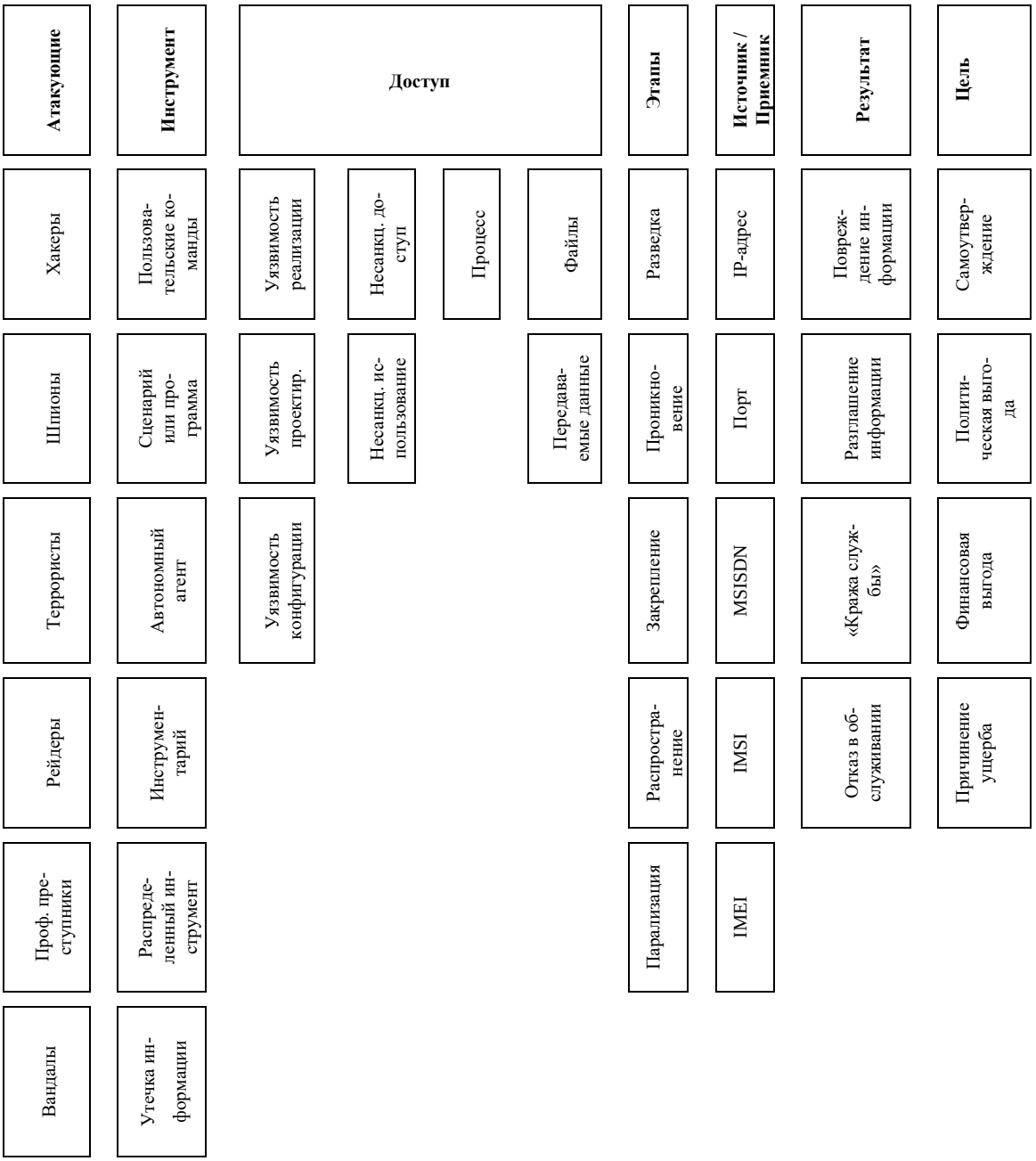

Рисунок 1.3. Систематика компьютерных атак

Различают простые и комплексные атаки. Простая атака включает в себя действия, выполняемые в рамках одного этапа комплексной атаки, реализует один из ее этапов: разведка, проникновение, закрепление, распространение и парализация. На этапе разведки путем выполнения таких действий как сканирование сетевого диапазона IP-адресов и TCP/UDP-портов, идентификация операционных си-

стем и сетевых служб, выявление их уязвимостей осуществляется сбор информации о потенциальной цели и направлении атаки. Этап проникновения предполагает применение выявленных уязвимостей с целью получения доступа к ресурсам ИТС для копирования, подмены или уничтожения данных. Этап закрепления характеризуется тем, что производятся действия, позволяющие в будущем проникать в систему без необходимости использовать уязвимость, с помощью которой произошло проникновение. На этапе распространения злоумышленником предпринимаются меры по использованию атакованных узлов с целью расширения атакующего воздействия на иные узлы сети, недоступные ранее. Завершающим этапом является парализация, когда осуществляются воздействия, приводящие к ущербу компьютерной информации. Здесь могут быть применены, в том числе атаки на отказ в обслуживании.

Под комплексными атаками будем понимать компьютерные атаки, состоящие из нескольких этапов, на каждом из которых злоумышленник может использовать различные методы для достижения конечной цели. Каждый этап комплексной атаки будем называть элементарным тестирующим (атакующим) воздействием (далее — ЭТВ). Менеджмент инцидентов, являющийся важной составляющей управления ИБ, включает в первую очередь расследование инцидентов в целях выяснения и устранения их причин и условий, им способствующих. Причинами, способствующими возникновению инцидентов ИБ, являются КА, а также действия пользователей, нарушающие действующую политику безопасности, принятую в организации.

Процесс расследования инцидентов ИБ включает, прежде всего, анализ событий («определённой совокупности обстоятельств» [13, п. 3.2.8]), являющихся, в соответствии с [15], составляющими частями инцидента ИБ. В процессе расследования определяются причины возникновения инцидента ИБ, регистрируется активность процессов, идентифицируются воздействия на файлы и др. Расследование инцидентов ИБ связано с анализом множества разно-форматных массивов данных, присущих компьютерной системе и содержащих информацию о воздействиях на файлы: временные отметки файлов, журналы событий операционной системы, журналы аудита, журналы средств защиты информации и т. д.

1.2.3. Системы обнаружения атак как объект тестирования

1.2.3.1. Основные типы СОА

Система обнаружения атак — это программный или программно-аппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы. Существует второй термин, характеризующий данный вид ССЗИ, — система обнаружения вторжений (далее — СОВ), явившийся дословным переводом исходного англоязычного термина IDS (Intrusion Detection System) [301, 302, 308].

Обнаружение атак базируется на методах сигнатурного анализа и (или) на методах обнаружения аномалий. При сигнатурном анализе предполагается наличие известного сценария атаки, следовательно, свидетельства ее реализации (либо попытки реализации) выявляются путем анализа сетевого трафика (либо анализа журналов регистрации событий) и поиска заранее известной последовательности событий или строки символов в упорядоченном во времени потоке информации. Атаки могут быть описаны различными способами, наиболее распространенным является описание атаки как набора правил (условий), детализирующих проявление атаки в структуре сетевых пакетов, в том числе правила могут содержать определенные значения отдельных полей заголовка пакета (IP-адрес и TCP/UDP-порт, установленные флаги сетевых пакетов на IP и TCP-уровнях, размер пакета и т. д.), структуру передаваемой информации. В правилах также описывается реакция системы на атаку и степень опасности атакующего воздействия.

В основе сигнатурных СОА лежит база данных известных атак (их сигнатур), от степени и регулярности обновления которой во многом зависит результативность обнаружения атак. Преимуществом сигнатурных СОА является относительная простота настройки системы правил, что позволяет адаптировать СОА под различные информационные технологии, сокращая избыточную базу данных атак, исключая сигнатуры атак, не относящиеся к примененному в ИТС про-

граммному обеспечению, и повышая производительность. Другой особенностью является низкая вероятность ошибок первого и второго рода.

Основной алгоритм для сигнатурных СОА – поиск строки-сигнатуры (шаблона) в массиве символов – в массиве сетевого трафика. Так, в первых версиях распространенной СОА Snort применялся алгоритм Боера-Мура (Boyer–Moore) для поиска подстрок. В дальнейшем алгоритмы, ускоряющие процесс сравнения строк, получили значительное развитие и применяются в современных версиях сигнатурных СОА: SBMH (set-wise Boyer—Moore—Horspool, 2003 г.,), ExB (exclusion-based, 2002 г.).

Подход к обнаружению атак, основанный на попытке обнаружения аномального поведения системы, предполагает, что в процессе «штатного» функционирования информационная система находится в некотором равновесном состоянии. Попытка реализации атаки ведет к выходу системы из этого состояния. При создании СОА, работающих по принципу обнаружения аномалий, должны быть определены механизмы принятия решения о попытке атаки защищаемой системы.

Главным преимуществом подхода, основанного на обнаружении аномального поведения системы, является теоретическая возможность обнаружения новых, не описанных ранее, атак. Эффективность выявления ранее неизвестных атак определяется способом описания нормального и аномального состояний информационной системы, а также зависит от количества параметров и свойств анализируемой ИТС. Для систем, основанных на обнаружении аномалий, наиболее часто встречаются ошибки первого и второго рода, что является их основным недостатком. При этом ложные срабатывания наиболее часто встречаются там, где сетевой трафик наиболее разнообразен в силу вариативности применяемых сетевых протоколов и служб. Другим недостатком является необходимость настройки системы и продолжительного обучения, что также связано с вариативностью и непрерывным совершенствованием информационных технологий и сложностью описания нормального поведения информационной системы.

Обнаружение комплексных атак, которые в настоящее время являются чрезвычайно опасными для ИС, затруднено вследствие необходимости анализа множества параметров и разнородных источников информации, выявления простых атак и поиска взаимосвязи между ними. Одним из требований, предъявляемых к СОА, предназначенной для обнаружения комплексных атак, является многоагентность, что предполагает наличие множества программных агентов (сенсоров либо аппаратно-программных датчиков) различного типа. Информация от агентов стекается в единый модуль анализа данных и принятия решений, в алгоритм которого закладывается система решающих правил на основе системы признаков и их пороговых значений, описывающих нормальное состояние ИТС. При этом разнородность сенсоров позволяет анализировать различные параметры ИТС и их окружения (в том числе, состояние окружающей среды). Наличие разнообразных по физической природе и технологии агентов позволяет выявлять комплексные атаки. Для обнаружения комплексных атак применяются различные математические методы, основная задача которых:

- получение и обработка информации от значительного количества разнородных источников информации;
- анализ редких нетипичных нормальных событий, редких нетипичных атак;
- распознавание атак в режиме реального времени.

В требованиях к СОА (СОВ) [16], разделяющих СОВ уровня сети и уровня узла, устанавливается шесть классов (шестой — низший). Для каждого из классов разработан соответствующий профиль защиты, определяющий функциональные требования и требования безопасности (пример — [17]).

1.2.3.2. Параметры сетевого трафика, анализируемые СОА

Для сетевых СОА, выявляющих атаки на основе анализа сетевого трафика, при формировании вектора признаков используются следующие статистические характеристики IP-сессии, рассчитываемые в единицу времени:

- количество входящих и исходящих IP-, TCP- и UDP-пакетов;
- количество внутрисетевых IP-, TCP- и UDP-пакетов;

— количество опросов неразрешенных портов UDP;

— количество запросов по протоколу UDP;

— количество незавершенных запросов по протоколу UDP, тайм-аут ответа на которые истек;

— количество опросов портов TCP, в том числе разрешенных;

— количество соединений TCP, находящихся в состоянии установления (SYN SEND), в открытом состоянии (ESTABLISHED), в состоянии закрытия (FIN SEND);

— отношение количества опросов разрешенных портов протокола TCP к количеству опросов всех портов этого протокола;

— отношение количества открываемых соединений TCP к общему количеству соединений.

1.2.4. Телекоммуникационное оборудование как объект тестирования

1.2.4.1. Телекоммуникационное оборудование в структуре информационно-телекоммуникационных систем

Для понимания целей, которые преследуются при проведении тестирования ТКО, необходимо указать роль телекоммуникационного оборудования в обеспечении доступности информации ИТС, включающего:

— первичную сеть связи — телекоммуникационную сеть, обеспечивающую передачу потоков данных и состоящую из множества соединенных друг с другом функциональных модулей;

— участки физических каналов передачи данных;

— ТКО — служебные узлы, объединяющие отдельные участки в единую телекоммуникационную сеть;

— вторичную сеть связи — множество узлов, которые реализуют информационные или телекоммуникационные услуги, например, электронной почты, web, голосовой связи, видеоконференций, а также могут осуществлять управление технологическими процессами;

— сеть автоматизированных рабочих мест — множество узлов, предназначен-

ных для использования информационных или телекоммуникационных услуг, предоставляемых вторичной сетью связи.

Угрозу информационной безопасности ИТС могут представлять как нарушение конфиденциальности и целостности хранящейся на узлах и циркулирующей в сетях информации, так и нарушение доступности ресурсов ИТС. Особенностью ТКО является то, что ТКО является первым и основным элементом ИТС, обеспечивающим взаимодействие узлов ИТС и передачу информации без задержек и потерь. Соответственно, атака на ТКО может привести к потерям и задержкам передачи данных, а также к нарушению информационного обмена и нарушению системы управления производственным процессом, в котором последовательность и полнота команд имеет первостепенное значение. Учитывая важность роли ТКО в обеспечении доступности информации, в рамках мероприятий по предупреждению компьютерных атак на ИТС включают анализ защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании».

В требованиях к межсетевым экранам (далее — МЭ) [18] как разновидности ТКО выделяются пять типов (А, Б, В, Г и Д), характеризующих область их применения, и шесть классов защиты (высший — первый), определяющих требования к функциям безопасности МЭ. Для каждого из типов и классов разработан соответствующий профиль защиты, определяющий функциональные требования и требования безопасности МЭ (пример — [19]).

1.2.4.2. Маршрутизаторы

Наиболее важным типом ТКО, применяемым в составе ИТС, являются маршрутизаторы. Маршрутизатор — выделенный компьютер специального назначения, соединенный с несколькими сетями, осуществляющий коммутацию пакетов между ними. Данный процесс также называется пересылкой (forwarding). Процесс пересылки может производиться для одного пакета множество раз на различных маршрутизаторах до тех пор, пока пакет не будет доставлен конечному адресату. Маршрутизатор IP отличается от прочих устройств коммутации пакетов тем, что коммутация пакетов осуществляется на основе заголовков про-

токола IP. При этом, как правило, маршрутизатор модифицирует заголовок IP полученных пакетов и включает в пакет новый заголовок канального уровня в соответствии с маршрутом дальнейшей передачи пакета. Помимо решения задачи коммутации пакетов маршрутизаторы также осуществляют управление маршрутизацией, то есть применение в процессе маршрутизации правил по выбору или исключению конкретных сетей, звеньев данных или ретрансляторов.

Маршрутизаторы могут реализовывать коммутацию с использованием следующих ресурсов:

— оперативной памяти и ресурсов центрального процессора устройства;

— оперативной памяти и вычислительных ресурсов процессоров сетевых интерфейсов и механизма прямого доступа к памяти;

— коммутационной матрицы.

Механизмом реализации компьютерных атак типа «отказ в обслуживании», нацеленных на ТКО, является исчерпание указанных ресурсов. Эффективность реализации атак определяется особенностями архитектуры конкретной модели ТКО.

1.2.4.3. Системы IP-телефонии

IP-телефония — телефонная связь по протоколу IP, набор технологий, протоколов и методов, обеспечивающих традиционные для телефонии методы набора номера, дозвона и передачу видео и голоса по сети Интернет. Сигнал по сетям передается в цифровом виде и перед передачей сжимается, что позволяет снизить нагрузку на сеть и избыток информации. Пакеты IP-телефонии снабжаются IP-адресом, для передачи используется IP-адресация. В IP-телефонии используются стандартные коммутаторы и специальные VoIP-шлюзы (Voice Over IP Gateway), обеспечивающие подключение обычных аналоговых телефонов к IP-сети. Они имеют встроенный маршрутизатор, позволяющий вести учет трафика, авторизовать пользователей, автоматически распределять IP-адреса, управлять полосой пропускания. Для передачи данных используются протоколы UDP (User Datagram Protocol) и RTP (Real-time Transport Protocol), не обеспечивающие надежность доставки данных, т.к. телефонная сеть некритична к потере пакетов. Основным па-

раметром, определяющим качество обслуживания в IP-телефонии, является время обработки сервером запроса, в случае увеличения которого будет происходить пропадание голоса, либо его задержка. Для ведения диалога необходимо, чтобы задержка не превышала 150 мс. Атака на сервер IP-телефонии может быть произведена совокупностью запросов различных типов, что требует получения зависимости производительности (времени ответа) серверов от всей совокупности запросов. Практическую значимость имеет задача нахождения таких характеристик трафика, при которых время ответа сервера не превышает допустимое, она может быть рассмотрена как задача поиска глобальных оптимумов.

1.2.5. Классификация и общая характеристика средств анализа защищенности компьютерных систем

Для проведения аудита информационной безопасности применяются средства, традиционно называемые системами анализа защищенности (САЗ) [303]. В литературе их также называют сканерами безопасности (security scanner) и сканерами уязвимостей (vulnerability scanner). В целом системы анализа защищенности — это программно-аппаратные комплексы, позволяющие проводить проверки автоматизированных систем на наличие тех или иных уязвимостей [26-28]: проектирования, реализации и эксплуатации.

При проведении аудита безопасности наибольший интерес представляют САЗ третьего типа — системы поиска уязвимостей эксплуатации. Такие системы также подразделяются в зависимости от уровня информационной системы, на котором осуществляется анализ: системы сетевого уровня, уровня операционной системы, уровня СУБД и уровня приложения. Эти системы будем называть специализированными САЗ. Существуют также универсальные системы поиска уязвимостей эксплуатации, позволяющие определять уязвимости на нескольких уровнях, их будем называть универсальными САЗ.

Вместе с тем не все задачи, возникающие в процессе проведения аудита безопасности, решаются САЗ, необходимы также системы, осуществляющие инвентаризацию ресурсов автоматизированной системы.

Кроме того, существует необходимость в системах, автоматизирующих анализ состояния на более высоких уровнях обеспечения информационной безопасности, чем технический, в частности на нормативно-методическом, организационном и технологическом. Также такие системы должны обеспечивать формирование итогового заключения по результатам проведения аудита безопасности и итоговой оценки уровня обеспечения безопасности в тестируемой системе.

Среди средств проведения аудита безопасности выделяются:

- программы инвентаризации сетевых ресурсов;
- универсальные сканеры безопасности;
- специализированные сканеры безопасности;
- средства комплексной оценки ИБ системы.

Программы инвентаризации сетевых ресурсов предназначены для выявления доступных сетевых узлов, определения перечня запущенных на узле сетевых служб и установленного программного обеспечения. Примерами программ инвентаризации сетевых ресурсов являются NMAP, Ad Rem Net Crunch, LANsurveyor.

Универсальные сканеры разработаны с целью комплексной проверки защищенности сканируемого узла. Как правило, они включают в себя функции программ инвентаризации сетевых ресурсов, а также функции по проверке уязвимостей операционных систем и установленного программного обеспечения. К универсальным сканерам безопасности можно отнести сканеры российского производства: XSpider (Max Patrol) (компания Positive Technologies), RedCheck (компания «АЛТЭКС-СОФТ»), Сканер-ВС (АО «НПО «Эшелон») и зарубежного производства: Tenable Nessus, GFI LAN guard Network Security Scanner и др.

Технология проведения аудита безопасности с использованием средств тестирования и анализа защищенности информационных систем предполагает выполнение следующих этапов:

— идентификация ресурсов ИТС и ИС;

— поиск возможных уязвимостей идентифицированных ресурсов ИС в базе данных уязвимостей (выдвижение гипотез);

— подтверждение выбранных уязвимостей — проведение атак (проверка гипотез);

— генерация отчетов.

Этап идентификации ресурсов ИТС и ИС осуществляется активными и пассивными методами. Активные методы предполагают сканирование сетевых портов удаленного узла, определение ОС удаленного узла и идентификацию сетевых сервисов на обнаруженных открытых портах удаленного узла. К пассивным методам относятся: методы прослушивания сетевого трафика в коммутируемой среде и методы определения сетевых протоколов с возможностью анализа туннелированных протоколов (FTP/HTTP, SMTP/HTTP и т.п.).

Основные операции, выполняемые САЗ:

— активное сканирование сетевых портов и идентификация ресурсов;

— тестирование уязвимостей;

— перехват и анализ сетевого трафика;

— пассивный сбор сетевой информации;

— обновление базы данных уязвимостей и тестов.

Специализированные сканеры предназначены для поиска уязвимостей в конкретных сетевых службах или программном обеспечении. Примерами специализированных сканеров безопасности являются:

– SAFETY-LAB Shadow Database Scanner — поиск уязвимостей, связанных с ошибками настройки и администрирования реляционных СУБД;

– Acunetix Web Vulnerability Scanner — поиск уязвимостей web-приложений;

– Atelier Web Firewall Tester — поиск ошибок в настройке и/или уязвимостей персональных межсетевых экранов.

Средства комплексной оценки ИБ системы предназначены для проведения анализа состояния ИБ на всех основных уровнях и получения итоговых оценок.

В большинстве случаев результатом работы САЗ является отчет, выполненный путем последовательного сканирования всех узлов сети на наличие известных уязвимостей, содержащий перечень найденных уязвимостей и рекомендации по их устранению. Вместе с тем в настоящее время внедряется иная парадигма анализа защищенности, учитывающая «топологию» компьютерной системы — взаимосвязь объектов компьютерной системы, их свойств и характеристик. Такой анализ защищенности называется топологическим, а средства, его выполняющие, топологическими сканерами безопасности. Топологический анализ защищенности предполагает построение графа атак на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети. Построенный граф содержит все известные сценарии атак для достижения нарушителем угроз. Результатом его анализа может являться:

- соотношение реализуемых мер безопасности и уровня защищенности сети;
- перечень наиболее критичных уязвимостей;
- перечень мер, позволяющих предотвратить использование уязвимостей в ПО, для которого отсутствуют обновления;
- наименьшее множество мер, реализация которых сделает сеть защищенной.

Сравнительное тестирование сканеров безопасности показывает различные результаты сканирования, связанные, прежде всего с различными сценариями тестирования, реализованными в том или ином САЗ [302]. Характеристиками САЗ, подлежащими сравнительному тестированию, являются как полнота и актуальность базы знаний об уязвимостях компьютерных систем, так и применяемые технологии, и алгоритмы выявления уязвимостей.

1.2.6. Информационно-аналитические системы безопасности

1.2.6.1. Выявление и реагирование на инциденты информационной безопасности

Деятельность по выявлению инцидентов ИБ и реагированию на инциденты ИБ является одним из активно развивающихся направлений в сфере ИБ. Данная деятельность регламентируется рядом нормативных документов, среди которых

национальные стандарты Российской Федерации ГОСТ Р ИСО/МЭК 27001:2005 и ГОСТ Р ИСО/МЭК 18044-2007 [13, 14]. Актуальность данного направления, в том числе в банковской сфере подтверждается введением с 2017 года стандарта Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» [15].

К числу инцидентов ИБ относятся свершившиеся, предпринимаемые или вероятные реализации угроз ИБ, целью и (или) результатом которых являются:

— несанкционированное распоряжение денежными средствами, которое привело или может привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами; к несвоевременности осуществления переводов денежных средств; к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях на осуществление переводов денежных средств (реквизитов платежей);

— деструктивное воздействие на информационную инфраструктуру, используемую для осуществления переводов денежных средств, которое привело или может привести к нарушению непрерывности оказания платежных услуг.

Такие угрозы ИБ могут осуществляться как работниками организации банковской сферы и иными лицами, имеющими легально предоставленный доступ к информационной инфраструктуре, используемой для осуществления переводов денежных средств (внутренними нарушителями ИБ), так и лицами, не имеющими такого доступа, в том числе не являющимися работниками организации банковской сферы (внешними нарушителями ИБ).

В связи с тесной интеграцией современных платежных систем (систем дистанционного банковского обслуживания) с системами связи, включая прежде всего системы сотовой связи, среди технических данных, сбор и анализ которых требуется для расследования инцидентов ИБ, выделяются [15]:

— протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;

— данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентами для осуществления доступа к системам дистанционного банковского обслуживания;

— протоколы (журналы) регистрации автоматических телефонных станций.

В рамках расследования инцидентов ИБ на каналах сотовой связи и в социальных сетях [240, 241, 297, 279] применяются и активно разрабатываются ИАСБ, такие как IBM I2[1], «Январь»[2], «Яхонт-ПД»[3] и др. [298], использующие сложные алгоритмы поиска взаимосвязей элементов современных телекоммуникационных систем. ИАСБ применяются также при расследовании инцидентов ИБ, связанных с мошенническими действиями при оплате услуг операторов сетей сотовой связи. Суть работы ИАСБ заключается в сборе исходных данных и первичной информации, её обобщении, установлении причинно-следственных связей влияния одних фактов на другие, на основании полученных результатов анализа и имеющегося алгоритма — агрегирование данных, подготовка аналитических справок и отчетов.

В основе ИАСБ лежат сложные математические алгоритмы [66, 67, 68, 69], реализованные в виде сложного программного обеспечения, включающего высокопроизводительные СУБД, системы анализа и визуализации данных. Для упрощения работы оператора-аналитика применяются определенные шаблоны типовых действий (методики). Каждая методика представляет собой совокупность последовательно выполняющихся сложных SQL-запросов к банку данных. Запросы также формируются программным способом. Результаты выполнения запросов визуализируются одним из методов визуализации графов.

ИАСБ накапливают и обрабатывают персональные данные абонентов сетей связи, в том числе:

[1] http://www-03.ibm.com/software/ products/ru/analysts-notebook
[2] http://www.mfisoft.ru/direction/sorm/sorm-3/
[3] http://www.norsi-trans.ru/pdetail/yahont-sorm3/

— информация об абонентах оператора и оказанных им услугах связи (включая услуги телефонии и передачи данных);

— сведения о пользователе, включая идентификатор пользователя в коммуникационном интернет-сервисе;

— информация о сетевом адресе, с которого осуществлена регистрация пользователя, с указанием времени регистрации;

— информация, которая должна вноситься при регистрации пользователя (дата и время регистрации пользователя; номер, дата и время договора);

— информация, внесенная пользователем (фамилия, имя, отчество (при наличии); псевдоним пользователя; дата рождения; адрес места жительства; реквизиты документа, удостоверяющего личность);

— внесенные пользователем принадлежащие ему идентификаторы в других средствах электронного взаимодействия, в том числе наименование сервиса и идентификатор.

Особенностью современных ИАСБ является сложность применяемых аналитических методик, математических алгоритмов и их программной реализации, что требует тестирования на различных массивах тестовых данных, в том числе имеющих пороговые значения.

При этом для организации тестирования алгоритмов, отработки и совершенствования методик поиска и анализа невозможно применять настоящие массивы информации о взаимодействии пользователей в сетях связи в силу того, что такие массивы содержат персональные данные пользователей, а доступ к ним и их хранение ограничены законодательно в соответствии со ст. 64 ФЗ «О связи» [11].

Следовательно, актуальной задачей является создание массивов данных необходимого объема для тестирования ИАСБ, учитывающих различные ситуации, складывающиеся в процессе взаимодействия пользователей в телекоммуникационной сфере.

1.2.6.2. Биллинговая информация

Биллинговые системы — автоматизированные системы расчетов, вычисляющие стоимость услуг связи для каждого клиента и хранящие информацию о тарифах и прочих стоимостных характеристиках, которые используются телекоммуникационными операторами для выставления счетов абонентам и взаиморасчетов с другими поставщиками услуг. Хранимая биллинговой системой информация называется биллинговой информацией. Международным союзом электросвязи выдвигается ряд рекомендаций по организации биллинговой информации, а Минкомсвязь России регламентирует основные аспекты функционирования биллинговых систем, в том числе расчёт длительности соединений, определение оплачиваемой длительности, регистрация вызовов при различных типах связи и т.п. Данные в расчетную систему поступают из подсистемы предварительной обработки данных, где собирается информация о соединениях с коммутаторов: данные о соединениях абонентов и привязка их соединений ко времени и базовым станциям. Подсистема предварительной обработки данных анализирует исходную информацию о соединении, определяет вид устанавливаемого соединения и его параметры: направление соединения, его источник, географическую и служебную информацию, а также информацию о роуминге.

Основным форматом информации о взаимодействии абонентов сетей связи является формат CDR (Call Data Record), в котором представлены массивы информации о соединениях в сетях операторов сотовой связи — массивы биллинговой информации. Формат рассматриваемых массивов данных имеет следующие столбцы, имеющие существенное значение для анализа [283]:

- EventId — уникальный идентификатор записи;
- BillTime — время звонка с точностью до секунды;
- CallDuration — длительность звонка в секундах;
- BillingType — тип соединения;
- LAC — Local Area Code или код локальной зоны — набора базовых станций;
- CellID — идентификатор соты, обслуживаемой базовой станцией;

– AbonentIMEI — IMEI абонента — серийный номер устройства;

– AbonentIMSI — IMSI абонента — глобальный ID абонента во всех мобильных сетях;

– AbonentPhone — MSISDN номер телефона — номер телефона абонента, инициировавшего соединение (MSISDN — Mobile Subscriber Integrated Services Digital Number — номер мобильного абонента цифровой сети);

– PhoneB — номер телефона, принимающего соединение.

1.2.7. Тестирование в рамках жизненного цикла сетевых средств обеспечения информационной безопасности

Разработка ССЗИ, как и программного обеспечения (ПО) в целом, является очень молодой и быстро развивающейся отраслью инженерной науки. Сложные системы в настоящее время создаются на основе системного подхода с внедрением языков программирования высокого уровня, методов структурного и модульного программирования, языков проектирования и средств их поддержки и т. д.

Для любого ПО характерен жизненный цикл — непрерывный процесс, который начинается с момента принятия решения о необходимости создания ПО и заканчивается в момент его полного изъятия из эксплуатации. Основным нормативным документом, регламентирующим жизненный цикл ПО, является стандарт ГОСТ Р ИСО/МЭК 12207-99 [29], в соответствии с которым жизненный цикл ПО состоит из основных (заказ, поставка, разработка, эксплуатация, сопровождение), вспомогательных (документирование, управление конфигурацией, обеспечение качества, верификация, аттестация, совместный анализ, аудит, решение проблем) и организационных (управление, создание и сопровождение инфраструктуры, усовершенствование, обучение) процессов.

Среди жизненного цикла ССЗИ выделяется его важнейшая часть — разработка ПО, включающая элементы процедуры тестирования, в том числе:

– программирование и тестирование ПО — разработка и документальное оформление каждого программного модуля и процедуры его тестирования;

– квалификационные испытания ПО и системы в целом — тестирование на соответствие квалификационным требованиям.

При разработке ПО проектировщикам необходимо выполнить работы на следующих основных стадиях [39]:

– предпроектной — определить особенности хранимой информации, выявить виды угроз и утечки информации и оформить техническое задание (ТЗ) на разработку системы;

– проектирования — выбрать концепцию и принципы построения системы защиты и разработать ее функциональную структуру, выбрать механизмы защиты, реализующие требуемые функции;

– разработки — разработать программное, информационное, технологическое и организационное обеспечение системы защиты;

– тестирования — провести отладку разработанной системы;

– документирования — разработать пакет технологической документации;

– внедрения — провести комплекс работ по эксплуатации и администрированию системы защиты.

В процессе разработки ПО в случае применения так называемой спиральной модели последовательность *анализ требований — проектирование — реализация — тестирование* выполняется более одного раза. На каждой итерации (витке спирали) создаются версии ПО, называемые прототипами.

Программное обеспечение ССЗИ подлежит комплексному тестированию, причем тестированию подлежат как собственно механизмы безопасности, так и пользовательский интерфейс к ним. Изготовитель или поставщик выполняет набор тестов, документирует его и представляет на рассмотрение аттестационной комиссии, которая проверяет полноту набора и выполняет свои тесты. Тесты должны показать, что защитные механизмы функционируют в соответствии со своим описанием, и что не существует очевидных способов обхода или разрушения защиты.

1.2.8. Систематика сетевых средств защиты информации при расследовании инцидентов информационной безопасности

Общая систематика ССЗИ, используемых при расследовании инцидентов информационной безопасности, локализации источников и субъектов компьютерных атак, с точки зрения сбора и анализа технических данных может быть представлена следующим образом:

Системы обнаружения атак (СОА)

- тип анализируемых данных
  - сетевые
  - узловые
- метод обнаружения
  - сигнатурный анализ
  - обнаружение аномалий
- конфигурация
  - локальные
  - распределенные
- способ обнаружения
  - реального времени
  - отложенной обработки

Средства анализа защищенности (САЗ)

- тип уязвимости
  - проектирования
  - реализации
  - эксплуатации
- функционал
  - программы инвентаризации ресурсов
  - универсальные сканеры
  - специализированные сканеры
  - средства комплексной оценки защищенности

Информационно-аналитические системы безопасности (ИАСБ)

- программные средства и системы, устанавливаемые на операторах связи
  - СОРМ2
  - СОРМ3
- средства реагирования на инциденты ИБ
  - анализаторы сетевого трафика
  - анализаторы журналов регистрации
  - анализаторы файловых систем
  - анализаторы вредоносного ПО
  - анализаторы биллинговой информации
- средства анализа и построения связей между субъектами расследования инцидентов
  - аналитические комплексы
  - средства визуализации графов связей

Телекоммуникационное оборудование (ТКО)

- коммутаторы
- маршрутизаторы
- межсетевые экраны
- системы IP-телефонии

1.3. *Анализ технологий и методов тестирования сетевых средств защиты информации*

1.3.1. Тестирование систем обнаружения атак

1.3.1.1. Методики и средства тестирования СОА

Первая работа [78], посвященная тестированию СОА, вышла в 1996 году, в ней предложена методика тестирования, основанная на известных методах тестирования программного обеспечения. Методика содержит несколько тестов, целью которых является проверка способности СОА выявлять известные компьютерные атаки, а также устойчивости системы при работе в критических условиях. Область применения методики ограничена тестированием сетевых систем обнаружения атак, использующих методы сигнатурного анализа. Действия законных пользователей и атакующее воздействие воспроизводятся путем имитации пользовательского ввода из командной строки при помощи специально разработанной программы. Тестирование способности СОА выявлять атаки выполнялось с использованием нескольких атак, включая попытку подбора пароля и передачу файла паролей по сети.

В проекте «The 1998 DARPA Off-Line Intrusion Detection Evaluation» [79] для тестирования СОА использован массив сетевого трафика, имитирующего работу крупной вычислительной сети с выходом в Интернет и содержащего следы реализации различных компьютерных атак. Сетевой трафик был получен при помощи специально разработанного стенда, в составе которого можно выделить три группы ЭВМ: атакуемые, атакующие и предназначенные для генерации фонового сетевого трафика. Атаки проводились из внешней сети, описание атак приведено в [80], их классификация приведена по [81]. Полученный сетевой трафик, содержащий смесь пакетов сетевых атак и пакетов фонового трафика, в течение 10 недель записывался при помощи анализатора, а затем подавался на вход тестируемых СОА. Предварительно в записанном трафике были идентифицированы и пронумерованы отдельные TCP-сессии, UDP и ICMP-пакеты, причем тем из них, которые содержали атаки, присваивалась соответствующая метка. Информация об этих сессиях и пакетах использовалась при определении правильности вы-

работки сигналов тревоги, а также при расчете вероятностей правильного обнаружения и ложного срабатывания.

Предложена методика оценки эффективности работы системы обнаружения, по результатам тестирования каждой СОА строилась «рабочая характеристика приемника» (receiver operating characteristic, ROC), отражающая зависимость вероятности правильного обнаружения атак определенного класса от количества ложных срабатываний (рисунок 1.4).

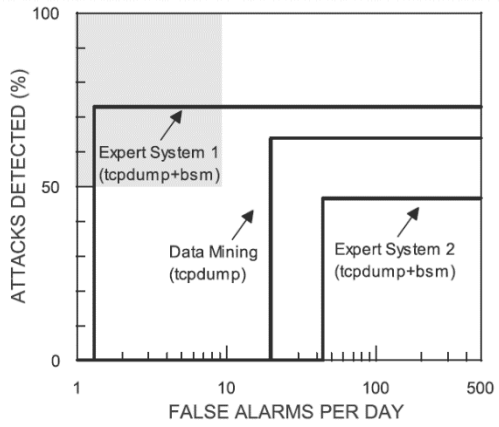

Рисунок 1.4. Пример рабочей характеристики СОА

Рабочая характеристика является наглядным способом представления возможностей обнаружителя (приемника) по выделению сигнала на фоне шума. Методика построения рабочей характеристики приемника предполагает фиксацию отношения сигнал-шум и непрерывное или дискретное изменение величины некоторого порогового значения, которое, в свою очередь, определяет соотношение вероятностей ложной тревоги и правильного обнаружения (см., например, [84]). В том случае, когда порог изменяется непрерывно, получаемая рабочая характеристика будет непрерывной, в случае дискретного изменения порога рабочая характеристика будет дискретной, то есть область определения рабочей характеристики ограничена значениями, которые может принимать порог. Если пороговое значение нельзя настраивать, то при данном соотношении сигнал-шум рабочая характеристика будет состоять из единственной точки, которая определяется алгоритмом функционирования обнаружителя. Указанный случай характерен для сигнатурных систем обнаружения атак, которые по природе своей не имеют настроек чувствительности. Очевидно, что полезность рабочей характеристики,

состоящей из одной точки, весьма мала, поэтому ее использование рационально лишь в тех случаях, когда алгоритм работы обнаружителя допускает настройку порогового значения.

Описанный выше способ тестирования, основанный на воспроизведении трафика компьютерных атак совместно с фоновым сетевым трафиком, позволяет обеспечить многократную повторяемость условий эксперимента. Тем не менее, детали реализации этого способа вызывают ряд нареканий [82]. Во-первых, авторы проекта никак не обозначили критерии реалистичности синтезируемого фонового трафика. Во-вторых, в работе не оценивается степень зависимости эффективности работы СОА от интенсивности сетевого трафика, используемого при тестировании. Вместе с тем такая зависимость имеет место даже для современных аппаратно-программных СОА, рассчитанных на работу с потоками интенсивностью несколько гигабит в секунду (см., например, [83]).

В 1999 году проект MIT/LL был дополнен рядом новых атак, соответствующие изменения внесены в состав стенда. Проект получил название «The 1999 DARPA Off-Line Intrusion Detection Evaluation», его основные результаты были опубликованы в [86], подробное описание проекта представлено в [87]. Отдельное внимание было уделено подготовке «скрытых атак» (stealthy attacks), представляющих собой версии известных атак, реализованных таким образом, чтобы затруднить их обнаружение [87]. Предпринята попытка анализа возможности выявления «новых атак», то есть атак, отсутствующих в базе данных СОА. Тестирование осуществлялось путем воспроизведения сетевого трафика, который был сгенерирован и записан с использованием разработанного стенда. Массив сетевого трафика состоял из двух частей: двухнедельного фрагмента, не содержащего атак, и фрагмента, записанного в течение недели и содержащего некоторое количество атак. Точное расположение всех атак в массиве было указано, причем для разметки трафика использовалась упрощенная по сравнению с проектом 1998 года процедура (не выделялись отдельные TCP-соединения, UDP- и ICMP-пакеты). Атака считалась успешно обнаруженной в том случае, когда СОА вырабатывала предупреждение во время осуществления атаки и правильно указывала IP-адрес атаку-

емого. Все предупреждения, сгенерированные в другие моменты времени, считались ложными срабатываниями.

Помимо проекта MIT/LL «The 1998/1999 DARPA Off-Line Intrusion Detection Evaluation», DARPA выступила спонсором аналогичного проекта Исследовательской лаборатории военно-воздушных сил США (Air Force Research Laboratory, AFRL). Основные результаты этой работы представлены в [88]. Сравнение двух проектов показывает, что они практически идентичны. Как и в [79], при построении рабочей характеристики авторы не указали интенсивность фонового трафика и общее количество реализованных атак, поэтому невозможно оценить эффективность работы СОА в условиях, отличных от тех, что рассматриваются в работе. Большое количество общих деталей, объединяющих работы AFRL и MIT/LL, и тот факт, что все они выполнены при поддержке DARPA, позволяет ссылаться на них как на один крупный проект (далее проект DARPA).

На основании анализа более поздних публикаций, посвященных тестированию систем обнаружения атак, можно сделать вывод, что проект DARPA стал основой большого числа дальнейших исследований и разработок по данной тематике. Он выявил основные трудности, с которыми приходится сталкиваться разработчикам собственных методик тестирования СОА, а также типичные ошибки, которые делаются в процессе тестирования.

В работе [89] взят за основу предложенный DARPA способ тестирования и разработано программное решение для синтеза сетевого трафика, содержащего компьютерные атаки. На базе ПО VMware разработан программно-аппаратный комплекс, позволяющий автоматически реализовывать компьютерные атаки, записывать сетевой трафик, передаваемый по сети в процессе их реализации, а также осуществлять разметку этого трафика с целью автоматизации последующего тестирования. В состав виртуальной сети комплекса входят виртуальные машины атакующего и атакуемого, а также несколько вспомогательных, выполняющих, в частности, функции DNS- и почтовых серверов. Кроме того, в состав комплекса входит хранилище резервных копий виртуальных машин, используемых в качестве атакуемых и вспомогательных, хранилище программ-эксплоитов, загружаемых атакующей виртуальной машиной, а также программа-координатор, которая

управляет конфигурацией виртуальной сети, отвечает за запуск компьютерных атак и запись сетевого трафика. Указывается, что перед реализацией каждой атаки «с нуля» воссоздается конфигурация виртуальной сети, в которой эта атака может быть реализована. Недостатком предложенного подхода является ограничение интенсивности реализуемых атак, в частности, невозможность реализации нескольких атак одновременно.

В работе [90] приводятся результаты тестирования СОА, которое проводилось не на специально разработанном стенде, а в работающей корпоративной сети. Все атаки реализовывались вручную, причем их количество было небольшим (менее 10). Дальнейшим развитием является работа [91], в которой авторы наряду с сетевыми протестировали несколько узловых СОА. Авторы отказались от использования реальной сети в пользу специального стенда. Задача синтеза фонового трафика решена при помощи соответствующего ПО. По сравнению с [90] существенно больше внимания уделено тестированию возможности восстановления фрагментированного трафика, а также способности обрабатывать сетевой трафик различной интенсивности. В работе [92] основное внимание сосредоточено на возможности использования СОА в условиях большого количества компьютерных атак при интенсивной нагрузке на сеть. Авторы вновь отказались от синтезированного трафика в пользу реального сетевого трафика, полученного в крупной корпоративной сети DePaul University. Данная сеть включала порядка 10 000 сетевых узлов, а интенсивность потока трафика на входном коммутаторе составляла от 5 до 7 тыс. пакетов в секунду при нагрузке 30–38 мегабит в секунду. Атакуемые узлы были внедрены в сеть DePaul University, а атаки проводились из сети Интернет. Методика сертификации СОА приведена в [83].

Авторы работы [93] тестировали системы обнаружения атак в сети, состоящей из десяти ЭВМ: двух «атакующих», трех «атакуемых», а также пяти ЭВМ, на которых было запущено ПО NetIQ's Chariot для генерации «фонового» трафика. Было реализовано в общей сложности 27 атак, включая попытки инвентаризации ресурсов, сканирование портов и организацию сетевых соединений «троянскими» программами. Кроме того, были предприняты попытки реализации «скрытых» атак, использующих альтернативные способы кодирования текста

и фрагментацию пакетов (ПО Fragrouter). Тестирование проводилось как без фонового трафика, так и с фоновым HTTP-трафиком различной интенсивности (40, 60 и 90 Мбит/с).

В работе [94] впервые было проведено тестирование активных систем — систем предупреждения атак (intrusion prevention system, IPS). Тестирование проводилось в действующей компьютерной сети, включавшей ЭВМ, расположенные в трех территориально распределенных частях экспериментальной лаборатории. Сеть была сконфигурирована так, чтобы быть максимально приближенной к сети Интернет по составу передаваемой информации. В работе [95] тестирование, как и в [94], проводилось в действующей корпоративной сети. В качестве атакующего воздействия выступало сканирование при помощи программ NMAP и Nessus, несколько атак были реализованы с использованием ПО Metasploit.

Работа [96] посвящена тестированию исключительно систем предупреждения атак. Тестирование проводилось по двум основным критериям: производительности и удобству использования. Системы предупреждения атак подключались к стенду, состоящему из двух устройств Spirent ThreatEx 2500, которые использовались для генерации атакующего воздействия, а также двух пар устройств Avalanche 2500 и Reflector 2500 того же производителя, которые генерировали фоновый сетевой трафик различной интенсивности. В тестах производительности в качестве фонового применялся сетевой трафик, в который входили пакеты наиболее распространенных протоколов: UDP, HTTP, FTP, SMTP, POP3 и DNS. На этапе оценки производительности измерялись две характеристики систем: пропускная способность (Мбит/с) и вносимая задержка (мс) распространения пакетов. В обоих случаях сначала измерения делались для трафика максимально возможной интенсивности без атак, а затем в этот трафик внедрялись атаки в различной пропорции (1 %, 4 % и 16 %), и измерения делались повторно. Тестирование TCP- и UDP-трафиком проходило раздельно.

В работах [97, 98] тест был проведен в действующей корпоративной сети, источником атакующего воздействия выступал специализированный программно-аппаратный комплекс Mu Dynamics Mu-4000.

В работе [100] рассмотрен стенд для тестирования систем предупреждения атак. Для генерации фонового трафика применялись устройства двух типов: программно-аппаратный комплекс, состоящий из пары Spirent WebAvalanche и WebReflector, для генерации веб-трафика и устройство Antara FlameThrower.

Логическим продолжением работы [100] является работа [101], посвященная тестированию коммерческих версий СОА Snort. Тестирование выполнялось на стенде, состоящем из двух атакуемых серверов, двух атакующих станций и ЭВМ с установленным ПО Fragrouter, которое использовалось для фрагментации сетевого трафика. Еще одна ЭВМ использовалась для генерации атак подмены MAC-адреса (ARP-спуфинг). Для создания потока «ложных» атак использовались программы Snot и Mucus, которые формируют пакеты на основе файла правил СОА Snort.

Работа [102] представляет собой обзор нескольких методик тестирования СОА, выделены два наиболее распространенных на тот момент подхода к тестированию. Первый заключается в создании небольшой закрытой сети и реализации атак в ее пределах. В этом случае роль фонового выполняет внутренний трафик данной сети. Второй подход предполагает воспроизведение предварительно записанного в крупной корпоративной сети трафика в тестовой среде. Этот подход требует интеграции атак в воспроизводимый трафик.

Технический отчет [103] представляет собой обзор известных работ по тематике тестирования СОА. В первой части отчета авторы предлагают перечень основных критериев тестирования систем обнаружения, во второй — дана краткая характеристика восьми работ, посвященных тестированию СОА, а в третьей — рассматриваются трудности, которые возникают при тестировании. Отдельное внимание уделено решению задачи синтеза фонового трафика. Выделены четыре возможные стратегии тестирования: тестирование без применения фонового трафика; использование реального сетевого трафика; использование реального трафика, из которого удалена персонифицированная информация; использование трафика, синтезированного с применением специального стенда. Авторами выделены достоинства и недостатки этих стратегий. Упоминаемая в отчете работа [104] посвящена тестированию СОА, ориентированных на защиту FTP-серверов.

Указывается, что количество атак было небольшим, а методы генерации фонового сетевого трафика и трафика атак были идентичны с использованными в [72]. Работа [105] выполнена корпорацией MITRE в интересах военно-морского флота США в 1997 году. Тестирование проходило в два этапа: на первом использовались относительно простые атаки, генерируемые программами типа SATAN; на втором этапе были дополнительно реализованы несколько более сложных и скрытых атак. Указывается, что фоновый сетевой трафик не применялся, то есть системы обнаружения тестировались без нагрузки. Упоминаемая в [103] работа NSS Group получила свое продолжение в виде методики сертификации СОА [106].

Работа [107] содержит обзор основных ошибок, которые делаются при тестировании систем обнаружения атак, а также некоторые рекомендации по их устранению.

На основе проведенного анализа работ в сфере тестирования ССЗИ и синтеза сетевого трафика можно сделать следующие выводы. С точки зрения сетевой СОА атака представляет собой множество упорядоченных во времени сетевых пакетов с определенным содержимым, поэтому подход к тестированию таких систем сводится к генерации сетевого трафика атакующего воздействия («сигнала») совместно с фоновым сетевым трафиком («шумом») и анализу отклика тестируемой СОА [72, 103]. Можно утверждать, что на данный момент сформировались два различных подхода к генерации тестового атакующего воздействия. Первый заключается в попытке воссоздания типичных условий функционирования СОА в рамках изолированной сети и последующего осуществления в ней реальных компьютерных атак [89, 108]. Несомненным преимуществом такого подхода является предельно высокая степень реалистичности атакующего воздействия, поскольку тестирование ведется с использованием действующих программных модулей, реализующих атаки. Программные модули, реализующие компьютерные атаки, обычно позволяют варьировать такие параметры атак, как IP-адреса атакующего и атакуемого, а также номера используемых TCP- и UDP-портов. Главным недостатком рассматриваемого способа тестирования является техническая сложность создания тестовой сети, состоящей из большого количества компьютеров с установленными на них уязвимыми ОС и прикладным ПО. Кроме того, возника-

ет необходимость восстановления начального состояния атакованного компьютера каждый раз после реализации направленной на него атаки, в противном случае станет возможным лишь однократное проведение каждой из атак. Отдельного внимания заслуживает задача обеспечения многократной повторяемости условий эксперимента — основного требования объективности теста. Самым очевидным способом ее решения является автоматизация процесса тестирования при помощи специализированного ПО, которое должно обеспечивать централизованное управление реализацией атак и восстановлением атакованных систем [89].

Второй подход к генерации атакующего воздействия заключается в применении специального экспериментального стенда, в состав которого входит генератор атакующего воздействия и тестируемый образец СОА. С помощью генератора осуществляется воспроизведение предварительно записанного массива сетевого трафика, который содержит как атакующее воздействие, так и фоновый сетевой трафик. Наличие различных массивов трафика, содержащих заранее записанные массивы сетевых пакетов разнообразных компьютерных атак, позволяет провести комплексное тестирование СОА, обеспечивая при этом как разнообразие вариантов атакующего воздействия, так и возможность многократного повторения процедуры тестового воздействия. Возможность повторения условий экспериментального тестирования востребована при проведении сравнительного тестирования ССЗИ. Кроме того, отсутствует необходимость применения в процессе тестирования информационных систем-«жертв» и необходимость восстановления их состояния после реализации атакующего воздействия. Для тестирования не только сетевых, но и узел-ориентированных СОА необходимо дополнительно организовать имитацию атакующего воздействия со стороны пользователей. Необходимость всестороннего комплексного тестирования СОА требует наличия максимально возможного количества вариантов реализуемых атак [89]. Вместе с тем представленный подход не позволяет варьировать параметрами (временными задержками, содержимым пакетов и т.п.) атакующего воздействия в процессе тестирования, так как требует модификации сформированных сетевых пакетов атакующего воздействия [106,108].

1.3.1.2. Особенности практической реализации средств тестирования

Один из первых практических проектов по тестированию — программа Intrusion Detection Evaluation, развернутая в 1998 году агентством DARPA [82]. Ее продолжением стал проект Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT), в рамках которого создан инструментарий для проведения тестирования в различных конфигурациях с эмуляцией работы пользователей [109].

Тестовый стенд DETER предназначен для проведения среднемасштабных экспериментов, связанных с компьютерной безопасностью [110], исследования осуществляются путем запуска интересующей программы в изолированной экспериментальной сети на основе виртуальных сетей, имеющих в своем составе различные ОС и системы безопасности.

Цель проекта Evaluation Methods for Internet Security Technology (EMIST) заключалась в разработке ПО и методики тестирования для различных форм сетевых атак и защитных механизмов. Получившийся в результате генератор сетевого трафика был сделан с помощью Scriptable Event System (SES), программы, позволяющей осуществлять контроль над большим количеством аппаратуры с центрального компьютера. Механизм работы этого генератора заключается в пошаговом выполнении заданного набора команд на центральном компьютере, с последующей отправкой на подчиненные компьютеры задания об отправке необходимых сетевых пакетов [111, 112].

Результаты проектов были использованы в исследовании [113] для экспериментов с атаками типа DDoS. Исследователи обратили внимание на недопустимое аномальное поведение фонового сетевого трафика при генерации. Кроме того, у исследователей возникли сложности с записью трафика в различных эмулируемых сетях для проведения оценки СОА, выявляющих аномалии.

RACOON является инструментом для генерации набора команд пользователей компьютерных сетей для проведения оценки работы сетевых СОА. Несмотря на то, что с помощью RACOON возможно создать различные наборы данных для проведения оценки СОА, данный инструмент не позволяет синтезировать реальные данные [114].

1.3.2. Тестирование телекоммуникационного оборудования

1.3.2.1. Принципы тестирования ТКО

Необходимость тестирования ТКО, прежде всего с точки зрения устойчивости к воздействию сетевых компьютерных атак типа «отказ в обслуживании», обусловлена тем, что выход из строя или нарушение штатного режима работы ТКО, обеспечивающего функционирование первичной сети, может привести к полному прекращению информационного взаимодействия между узлами сети, и, таким образом, к нарушению структурной целостности ИТС.

Общепринятым подходом при проведении оценки устойчивости ТКО к сетевым компьютерным атакам типа «отказ в обслуживании» является тестирование, в процессе которого производятся передача тестового СТ, имитирующего взаимодействие между конечными узлами сетей, и оценка параметров качества обслуживания, обеспечиваемого ТКО на участках между сетевыми интерфейсами ТКО. При этом производится выявление таких значений параметров тестового СТ, при которых качество обслуживания оказывается наихудшим. В качестве тестового может использоваться СТ, созданный с использованием следующих данных:

- образцов СТ реальной сети (сети-эталона);
- параметрического представления СТ сети-эталона;
- параметрического представления, созданного без использования каких-либо данных реальных сетей.

Независимо от реализации, принцип работы средств тестирования ТКО заключается в выполнении четырех основных операций:

- генерации тестового СТ;
- отправке сгенерированного СТ тестируемому образцу ТКО;
- захвате тестового СТ после его обработки ТКО;
- анализе переданного и захваченного СТ.

Стандарты сети Интернет RFC 2544 [42] и 3918 [43] описывают методики, используемые для измерения следующих характеристик, связанных с производительностью ТКО: пропускной способности, задержки передачи пакетов на канальном и сетевом уровнях, относительной доли потерь пакетов.

1.3.2.2. Стандарт RFC 2544

Методика, описанная в стандарте RFC 2544, предназначена для проверки способности оборудования к обработке служебных заголовков пакетов и определения максимальной интенсивности СТ, принимаемого ТКО, при которой не происходит потерь пакетов. Методика заключается в выполнении следующих шагов:

— устанавливается максимальная интенсивность передачи пакетов тестируемому образцу ТКО (в соответствии с его документацией);

— пакеты передаются тестируемому ТКО в течение определенного интервала времени, при этом отслеживается момент, когда количество потерянных в процессе обработки ТКО пакетов превысит заданный лимит;

— если превышение лимита произошло, то производится снижение интенсивности передачи данных и повторное выполнение предыдущего шага; иначе тест завершается, а текущая интенсивность передачи данных считается предельной для оборудования.

В стандарте RFC 2544 при описании задержек передачи данных используются термины *delay* и *latency*. Задержки передачи данных измеряются исходя из определений, приведенных в RFC 1242 [44]: *latency* обозначает задержку, связанную с функционированием тестируемого устройства, то есть временной интервал между приемом ТКО последнего бита пакета и завершением его отправки после обработки, а *delay* — задержки линии передачи, очереди в буфере устройства и т.п. Важным параметром, измеряемым в процессе тестирования, является джиттер, который определяется как среднее изменение разности межпакетных интервалов пары пакетов до и после обработки их тестируемым оборудованием. Измерение джиттера в соответствии с RFC 3550 [46] заключается в отправке последовательности помеченных пакетов с фиксацией времени их отправки и приема, а затем — анализе полученных временных интервалов.

Результатами тестирования являются: общее количество пакетов, переданных и полученных через все порты тестируемого оборудования; доля потерянных пакетов для каждого теста с различной длиной кадра; задержка передачи пакетов; джиттер; последовательность возникновения ошибок; ошибки в содержании пакета.

1.3.2.3. Стандарт RFC 2889

Методика, описанная в RFC 2889 [45], предназначена для оценки способности оборудования к обработке ситуаций, связанных с перегрузкой каналов передачи, и применима для тестирования как коммутаторов, так и маршрутизаторов. Тестирование заключается в выделении на исследуемом оборудовании четырех интерфейсов. При этом СТ первых двух интерфейсов направляется на третий, а одновременно один из них производит передачу пакетов на четвертый. Таким образом, происходит наблюдение за поведением тестируемого устройства в условиях нагрузки, превышающей его возможности. Результатами тестирования являются: планируемая и фактически полученная пропускная способность устройства; количество переданных и полученных пакетов; количество потерянных пакетов; количество коллизий; количество полученных служебных пакетов управления процессом передачи данных.

1.3.2.4. Стандарт RFC 3918

Цель методики, описанной в RFC 3918 [43], заключается в проверке способности маршрутизатора к обработке протоколов маршрутизации, то есть для определения пропускной способности и задержек, возникающих в устройстве при маршрутизации группового трафика и работе с несколькими потоками. Входными параметрами при проведении тестирования являются параметры протокола (IGP, PIM), параметры отправителя, параметры получателя (группа адресов), размеры пакетов, верхняя граница интенсивности передачи данных. Результатами теста являются следующие характеристики: максимальная пропускная способность на интерфейсе; количество потерянных пакетов; задержка передачи пакетов (максимальная, минимальная и средняя); количество ошибок пересылки пакетов.

1.3.2.5. Решения на основе эволюционно-генетического подхода

В рамках данного класса методик поиск сценария тестирования, приводящего к созданию критической нагрузки на тестируемое оборудование, сводится к решению задачи оптимизации значений параметров модели сценария тестирования. Численное решение данной задачи может быть затрудненно в связи с раз-

мерностью и видом оптимизируемой функции, которая в общем случае может быть нелинейной, разрывной, не дифференцируемой и многоэкстремальной.

Одним из подходов, позволяющим преодолевать указанные трудности, является эволюционно-генетический подход, который позволяет строить алгоритмы поиска оптимальных решений, называемые генетическими алгоритмами, на основе моделирования биологических механизмов популяционной генетики. Существует целый ряд важных работ, в частности, [48-53], авторы которых применяют аппарат генетических алгоритмов для построения сценариев тестирования. Общепринятым названием такого варианта решения рассматриваемой проблемы является термин *эволюционное тестирование* (*evolutionary testing*, *ET*). 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.

1.3.2.6. Выявление пороговых значений производительности при нагрузочном тестировании маршрутизаторов

При нагрузочном тестировании маршрутизаторов D-Link Dir320-NRU и TP-Link WR1043ND, проведенном с целью выявления влияния на пропускную способность маршрутизатора объема кэш-памяти и производительности центрального процессора (рисунок 1.5, рисунок 1.6), использовался специально сгенерированный UDP трафик, при этом фиксировалась максимальная скорость передачи данных, при которой не происходит потеря пакетов [295].

При оценке влияния объёма кэш-памяти устройства предполагается, что для ускорения процесса маршрутизации в кэш-памяти сохраняется информация о недавно маршрутизированных пакетах. При направлении очередного пакета в ту же сеть, в которую был направлен один из предыдущих, он отправляется на тот же интерфейс без анализа таблицы маршрутизации. Для оценки объёма кэша генерировался трафик, в котором варьировалось количество различных сетей, размер пакетов оставался фиксированным. Производительность маршрутизатора TP-Link

(объем кэш-памяти 64 кб) существенно уменьшается при вдвое большем количестве различных сетей, чем у маршрутизатора D-Link (объем кэш-памяти 32 кб).

Одним из важнейших показателей производительности является максимальное количество пакетов, которые устройство успевает маршрутизировать. Решение о том, куда отправлять тот или иной пакет, принимает центральный процессор, и для определения его производительности генерировался трафик, в котором варьировался размер пакета путем изменения количества полезной нагрузки. Количество передаваемых пакетов практически не зависит от размера полезной нагрузки, так как все время обработки пакета — это время обработки заголовков.

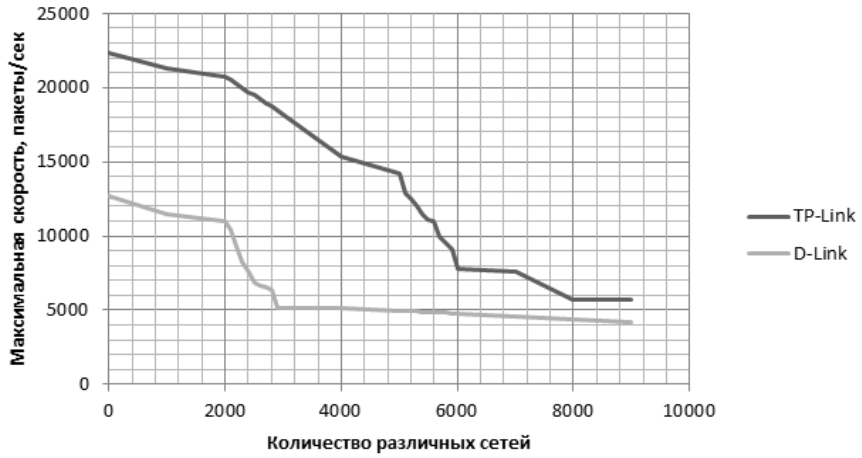

Рисунок 1.5. Зависимость пропускной способности маршрутизатора от количества различных сетей в трафике

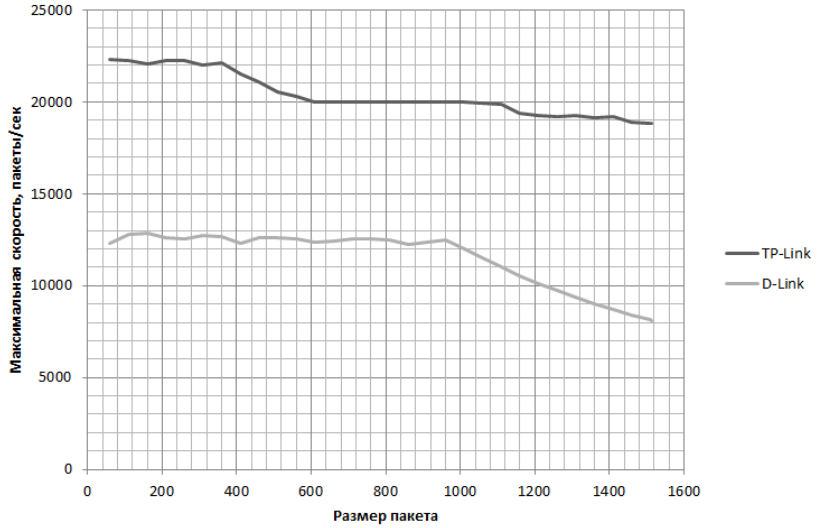

Рисунок 1.6. Зависимость пропускной способности маршрутизатора от размера полезной нагрузки в пакете

1.4. *Анализ моделей синтеза фонового сетевого трафика*

1.4.1. Параметры сетевого трафика

Для решения задачи тестирования ССЗИ необходимо синтезировать СТ идентичный реальному. Под синтезируемым СТ понимается искусственно созданный трафик с заданными математической моделью параметрами.

Одним из первых исследований, касающихся проблем моделирования и имитации сети Интернет, была работа Паксона и Флойда [131, 132].

В известных моделях [115-119] принято рассматривать сетевой трафик как динамический нестационарный процесс. Используется небольшое число параметров трафика (временные интервалы между пакетами, объем трафика в единицу времени и т.п.). Для генерации предлагается на основе имеющегося массива пакетов (вне зависимости от наполнения пакетов) создавать трафик, параметры которого идентичны реальному с точки зрения загруженности сетевых каналов.

Ряд работ по моделированию СТ [54, 115-119, 120, 121] показывает преимущество для моделирования СТ статистически самоподобных процессов по сравнению с традиционной Пуассоновской моделью. В [122, 123] модели самоподобия использовались для исследования зависимости от времени размеров сетевых кадров протокола Ethernet. В [124] описана процедура агрегирования для приведения исходных реализаций к эквидистантной (с постоянным шагом ΔT) шкале по оси времени. Для этого ось времени была разбита на интервалы ΔT, каждому из которых ставилось в соответствие отношение количества прошедшей за данный интервал времени информации (в байтах) к длительности интервала (в секундах). Получившиеся временные ряды были проанализированы, на основе чего было произведено измерение показателя Херста (H). Обнаружено, что для всех реализаций СТ $H > 0{,}5$, то есть трафик относится к классу персистентных процессов. Усредненное значение H для СТ $H \approx 0{,}8$. Зависимости коэффициента H от уровня агрегирования не выявлено.

В работах [123, 125] предлагается иной способ анализа СТ, основанный на суперпозиции нескольких независимых и имеющих одинаковое распределение ON/OFF–источников. Интервалы между ON– и OFF– периодами обладают эффек-

том Hoa (Noah effect), являющимся основой при моделировании самоподобного трафика [126]. Математическая модель СТ, построенная с использованием указанного математического аппарата, является адекватной реальному трафику [126] и позволяет использовать ее для анализа генерируемого трафика с целью сопоставления с СТ, функционирующим в компьютерных сетях.

В большинстве известных публикаций (в том числе [128-130]) по вопросам моделирования СТ в задачах тестирования сетевых устройств основными являются параметры, описывающие интенсивность трафика. При этом вне рассмотрения остаются вопросы, связанные с наполнением сетевых пакетов, что актуально в задачах тестирования сигнатурных СОА.

1.4.2. Модели генераторов сетевого трафика

Различают три вида моделей генераторов сетевого трафика по режиму работы: режим воспроизведения пакетов, режим источника сетевого трафика и режим имитации Web-сервера.

Режим воспроизведения пакетов заключается в генерации пакетов в сеть в соответствии со статистическими характеристиками трафика, наблюдаемыми в реальном канале. Такие генераторы, например, tcpreplay [133], применяются для экспериментов, в которых не учитывается влияние конфигурации сети на синтезируемый трафик [134-136]. Кроме того, часто используют воспроизведение на пакетном уровне в исследованиях, для которых необходимо синтезировать аномальный трафик [130, 137] (например, затопление SYN-пакетами), не зависящий от характеристик сети.

Предварительно записывается трафик, например, с помощью берклиевского пакетного фильтра (Berkeley Packet Filter - BPF) — ПО tcpdump [138, 139]. Базы данных образцов трафика содержат только заголовки протоколов (IP и TCP/UDP) и отметки времени прибытия пакетов. Специализированные аппаратные средства типа платформы DAG [140-142] могут извлекать заголовки и предоставлять отметки времени без вмешательства ОС, что повышает точность фиксации отметок времени. Также используются различные депозитарии pcap и DAG-файлов, например, архив Интернет-трафика [143] и PMA проект в NLANR [144].

Синтез сетевого трафика в режиме воспроизведения пакетов имеет ряд проблем, в частности существует проблемы воспроизведения СТ в высокоскоростных каналах связи ([146-147]), а также изменения массива трафика и структуры воспроизводимой сети, так как СТ является копией захваченного реального трафика.

Преимуществом является возможность генерации в соответствии с произвольной статистической моделью, выбранной на основе характерных признаков трафика, которые наиболее важных для тестирования, в том числе с учетом пульсации трафика и изменения во времени пропускной способности ([147-152]).

Синтез сетевого трафика, осуществляемый генераторами, работающими в режиме источника сетевого трафика, основан на поведенческой модели сетевых приложений, которые работают на конечных узлах сети и поддерживают соединение с использованием сетевых потоков ([158-163]). Генератор создает одно или несколько сетевых соединений и постоянно снабжает их данными для передачи, при этом обеспечивается реакция на изменения сетевой конфигурации и характеристики сети точно таким же образом, как и у конечных узлов существующих сетей. Основным недостатком является нереалистичность трафика вследствие одно направленности модели бесконечного источника.

В многочисленных генераторах трафика, имитирующих Web-сервер ([164-188]), осуществляется моделирование Web-трафика с помощью генерации синтетической нагрузки на Web-серверы. Существует несколько значимых моделей Web-трафика: параметрическая модель на основе законов производительности, реализующая принцип «мышей и слонов»; SURGE-модель, построенная на описании поведения каждого пользователя-клиента в виде последовательности загрузок гипертекстовых страниц и «времени обдумывания» между ними; модели, использующие для значимых параметров различные виды распределения (логнормальное, Парето, би-Парето и др.).

1.5. Анализ существующих методов тестирования с применением фонового сетевого трафика

1.5.1. Понятие фонового сетевого трафика

Сетевой трафик реальных компьютерных сетей рассматривается как совокупность атакующего воздействия и фонового трафика, не содержащего атак. Такой способ позволяет не только создавать основную нагрузку сетевых каналов, но и проводить обучение СОА, основанных на обнаружении аномалий, путем задания нормального поведения сети. При этом важно дать понятие нормального трафика. В работе [126] за основу берется предположение, что высоковероятные закономерности определяют нормальное течение событий, а нарушение закономерностей (аномальное) — атаку. Иной подход к определению нормального поведения СТ описан в работах [152,189] через совокупность критериев, которым он должен удовлетворять:

1) форматы пакетов и сессий, возникающих в процессе взаимодействия компонентов сети, должны соответствовать требованиям протоколов передачи данных и рекомендациям RFC. При этом не исключается возможность ошибок во время сетевого взаимодействия, которые могут возникнуть в рамках работы того или иного протокола;

2) логика взаимодействия компонентов компьютерных сетей на уровне синтезированных пакетов должна соответствовать имитируемому сетевому взаимодействию;

3) временные параметры СТ должны определяться той структурой и типом сети, в которой он циркулирует;

4) наличие количественных характеристик, описывающих пропускную способность: средняя скорость передачи данных, определяющая поток, который источник может поддерживать в течение длительного периода времени; пиковая скорость — определяет для сети максимальный трафик, который она в состоянии поддерживать; неравномерность — характеризует непостоянство трафика источника; количество пакетов в единицу времени, длина пакетов, время между посылками пакетов и др. характеристики, определяющие самоподобие СТ [190-191], как

например параметр Херста, значение которого для сетевого трафика находится в интервале строго более 0,5 и не превышает 1 [192];

5) содержимое области данных сетевых пакетов должно соответствовать характеристикам того протокола, к которому данный пакет относится. Причем предполагается, что в пакетах передается не абстрактный набор данных, а четко заданная информация. От содержимого области данных зависят не только количественные характеристики сетевого трафика, но и возможность ложных срабатываний СОА, что является одним из ключевых моментов при проведении тестирования;

6) по совокупности всех своих параметров СТ должен иметь фрактальную природу и обладать самоподобием.

Введенные критерии дают возможность формировать подходы к синтезу СТ, представляющего четко сформированные и логически обусловленные сессии пакетов в рамках сетевого соединения.

С целью синтеза фонового сетевого трафика, имитирующего штатное информационное взаимодействие между узлами моделируемой сети и не содержащего атакующих воздействий, А.С. Коллеровым была разработана матричная модель сетевого трафика [211, 302] на основе теории матриц, а также теории вероятностей и математической статистики.

1.5.2. Методы тестирования систем обнаружения атак с применением фонового сетевого трафика

Тестирование СОА осуществляется с использованием различных подходов:

- без использования фонового СТ,
- с применением массива реального СТ,
- с использованием реального СТ, не содержащего защищаемой информации,
- с применением генерируемого фонового СТ.

Тестирование без использования фонового СТ. В данном подходе СОА тестируется в сети, не содержащей иного трафика кроме тестовых сетевых атак. Данный подход легко позволяет определить критерий вероятности обнаружения атак, однако, не предоставляет возможности оценить вероятность ложных срабатываний. Легко можно выявить наличие сигнатур для тестовых атак и корректность их идентификации. Отрицательной стороной данного подхода является то,

что система, протестированная в идеальных условиях, может вести себя совершенно иначе в условиях повышенной сетевой нагрузки.

Тестирование с применением массива реального СТ. Подход заключается в отправке тестовых сетевых атак, внедренных в поток фонового СТ. При этом можно определить производительность СОА при различных объемах фонового трафика и, таким образом, проводить сравнительное тестирование различных СОА. Реальный СТ может содержать различные аномалии, что не позволит оценить вероятность ложных срабатываний. Недостатки данного подхода:

— так как реальный СТ содержит законодательно защищаемую информацию [11], то его захват и последующее воспроизведение невозможно;

— сложность тестирования вследствие необходимости хранения больших массивов трафика;

— так как тестовые атаки будут направлены против небольшого числа узлов-жертв, то интеллектуальные СОА могут настроиться на анализ трафика, направляемого только в тестовые узлы, игнорируя фоновый СТ и повышая свою производительность, в отличие от сигнатурных СОА;

— в связи с тем, что в реальном СТ могут содержаться аномалии, уникальные для определенного типа сетей, то при тестировании в более выигрышном положении окажутся те СОА, которые наибольшим образом ориентированы на конкретный тип сети;

— так как в используемом реальном СТ могут содержаться сетевые атаки, в том числе в скрытом виде, то сложно определить величину ложных срабатываний. Следовательно, требуется предварительный анализ трафика на наличие в нем сетевых атак, что должно быть выполнено с помощью иной доверенной СОА («ручной» анализ недопустим вследствие больших объемов СТ).

Тестирование с использованием СТ, не содержащего защищаемой информации. Данный подход состоит в том, чтобы, захватив реальный трафик, удалить из него (например, обнулением) содержимое полей данных сетевых пакетов, оставив только заголовки пакетов определенного уровня. Преимуществом является возможность воспроизведения такого трафика без нарушения законодательства.

Кроме того, удаление поля данных сетевых пакетов приводит, к удалению части атак, содержащихся в реальном трафике. Недостатками подхода являются:

— трафик с удаленным полем данных сетевых пакетов является абсолютно нереалистичным;

— автоматизированное удаление содержимого трафика в силу сложности и количества разнообразных протоколов может привести к непреднамеренно оставленному «мусору», содержащему защищаемые данные;

— внедряемые атаки должны соответствовать передаваемому фоновому СТ. При выполнении, например, атаки типа «отказ в обслуживании» на тестируемый узел следует контролировать отсутствие далее в фоновом трафике сетевых пакетов, отправляемых с данного узла.

Тестирование с применением генерируемого фонового СТ. В данном, наиболее часто применяемом подходе предлагается генерировать СТ с применением моделирования статистических свойств реального трафика. Известны [196-198] примеры программных и аппаратных комплексов, выполняющих генерацию трафика.

Преимущество подхода — в отсутствии в СТ охраняемой законом информации и неизвестных атак, а также в возможности многоразового повторения эксперимента в идентичных условиях. Недостатком подхода является необходимость моделирования разнообразных видов сетей.

1.5.3. Метод формирования содержимого сетевых пакетов на основе цепей Маркова

Метод формирования содержимого области данных сетевых пакетов с применением цепей Маркова с дискретным временем в задаче тестирования СОА подробно исследован в работах [211, 229, 230]. Цепь Маркова [228] задается множеством значений случайных величин, называемым пространством состояний, и матрицей переходных вероятностей между состояниями. По матрице переходных состояний определяется вероятность перехода из текущего состояния в следующее. Для генерации текста используется матрица переходов, при этом множество всех слов, знаков препинания и тегов является пространством состояний. Формирование переходной матрицы осуществляется на основе множества html-страниц, по которым производится оценка вероятности создания (составления) новой фра-

зы после последовательности уже созданных фраз. Произведенная цепью Маркова последовательность событий является набором слов, упорядоченных в единую html-страницу. Процесс поведения абстрактного пользователя сети при обращении к Web-серверу является Марковским [230].

Формирование страниц на Web-сервере предполагает расстановку рангов полученным страницам, что позволяет формировать модель посещения Web-сервера и предполагаемый маршрут перемещения посетителя по Web-сайту. Маршрут перемещения по сайту обусловлен двумя факторами: ссылками, находящимися на текущей странице, и временем, проведенным на странице [230]. Вероятность просмотра страницы зависит от количества ссылок на нее и от вероятности просмотра страниц, ссылающихся на нее.

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.

Таким образом, возможно применение цепей Маркова для наполнения области данных сетевых пакетов в модели взаимодействия пользователя с Web-сервером в применении к тестированию ССЗИ.

1.6. Анализ моделей формирования статической и динамической структуры сетевого взаимодействия

1.6.1. Модели построения сложных сетей для описания взаимодействия пользователей в современных сетях

Для моделирования структуры сложных сетей используется ряд моделей, позволяющих описывать взаимодействие между людьми:

- модель Эрдёша-Реньи (случайные графы) [199];
- модель Ваттса-Строгатца (сети «тесного мира») [200];
- модель Барабаши-Альберт (сети предпочтительного присоединения) [201].

Структура взаимосвязей абонентов сетей сотовой связи рассматривается как сеть простого вербального общения людей в реальном мире без применения каких-либо технических средств, так как для данных сетей определены некоторые структурные свойства: закон распределения степеней вершин близкий к Пуассо-

новскому; малая длина пути между вершинами; высокий коэффициент кластеризации; децентрализованная структура.

Модели Эрдёша-Реньи и Ваттса-Строгатца имеют децентрализованную структуру и близкий к Пуассоновскому закон распределения степеней вершин в графе, что позволяет использовать их при описании взаимодействия абонентов сетей сотовой связи.

Процесс генерации структуры социального графа предполагает создание первоначальной решетки с последующим, основанным на подходе генерации случайных чисел, созданием ребер, характеризующих связи, и присвоением ребрам и вершинам определенных весов. Особенностью социальных сетей является принцип предпочтительного присоединения, когда количество генерируемых соединений существенным образом зависит от веса узла (показательный закон распределения степеней вершин). Кроме того, характерными свойствами являются малая длина пути между вершинами и высокий коэффициент кластеризации. Указанные свойства наиболее полно представлены в модели Барабаши-Альберт, позволяет использовать данную модель при формировании структуры социальных графов с дополнениями:

— количество ребер n, соединяющих новую вершину с уже существующими в системе вершинами, определяется коэффициентом $C>1,5$, обозначающим соотношение количества ребер во всем графе к количеству всех вершин (среднее количество ребер на одну вершину);

— если количество ребер добавляемой вершины превышает 1, то показатель вероятности $П$ изменяется в зависимости от кластера вершины, к которой совершено присоединение первой: у вершин, инцидентных ей, данный показатель увеличивается, в то время как у остальных уменьшается:

$$П_{mod}(k_i)=П(k_i)\pm\frac{k_{min}}{\sum_{j=0}^{N}k_j} \quad (1)$$

где $П(k_i)$ – показатель вероятности, с которой новая вершина будет соединена с вершиной i в зависимости от ее степени k_i, $\sum_{j=0}^{N}k_j$ – сумма степеней всех вершин графа, k_{min} – минимальное значение степени вершины во всем графе.

1.6.2. Модель атакующего воздействия в терминах стохастических сетей Петри в задаче тестирования СОА

Применение стохастических сети Петри (англ. Generalized Stochastic Petri Nets) для решения задачи синтеза массивов атакующего воздействия подробно исследовано в работах [253-256]. В основе предложенной модели лежит утверждение о том, что комплексная атака состоит из последовательности элементарных атакующих воздействий — действий атакующего, выполняемых программными средствами и направленных на достижение конечной цели атаки. Атакующее воздействие рассматривается совокупность множества ЭТВ X и множество возможных исходов (последствий, результатов) атаки Y. Каждое ЭТВ x_k задает некоторую точку в n-мерном пространстве Y , характеризуется вектором $y_k = (y_1, y_2, \ldots, y_n)$, каждый элемент которого равен априорной вероятности, с которой данное ЭТВ приводит к указанному результату (n — общее количество возможных последствий атаки): $y_k = 0$ — *не приводит*; $0 < y_k < 1$ — *может приводить*; $y_k = 1$ — *всегда приводит*.

Конечная цель атакующего оценивается вектором $\boldsymbol{a} = (a_1, a_2, a_3, a_4)$, состоящим из четырех элементов: a_1 — сетевая разведка; a_2 — отказ в обслуживании; a_3 — захват ресурсов; a_4 — несанкционированный доступ. Считается, что злоумышленник может сделать предположение о наличии какой-либо уязвимости и попытаться реализовать атаку, не имея гарантий ее успешности. Вводится множество всех параметров системы Z, каждый из которых может принимать значения –1 («ложь») и +1 («истина»). Значения параметров, необходимые для реализации ЭТВ, характеризуются вектором $\boldsymbol{z}^I = (z_1, z_2, \ldots, z_M)^I$, каждый элемент которого может принимать три значения: 0 (параметр не влияет на реализацию ЭТВ), –1 (параметр должен иметь значение «ложь») или +1 (параметр должен иметь значение «истина»).

Знания злоумышленника о системе характеризуются парой векторов $\boldsymbol{z}^A$ и $\boldsymbol{z}^V$. Каждый элемент вектора $\boldsymbol{z}^A = (z'_1, z'_2, \ldots, z'_K)^A$ отражает степень знания злоумышленником соответствующего параметра системы и принимает два возможных значения: 0 (параметр не известен) или 1 (параметр известен). Вектор $\boldsymbol{z}^V = (z'_1,$

z'_2, …, $z'_K)^V$ отражает собственно знания или предположения (если значение параметра не известно) злоумышленника о значении параметров атакуемой системы.

Для создания динамической компоненты предложено использовать последовательность временных интервалов, соответствующих моментам передачи пакетов и состоянию ожидания линии связи. Введение понятия задержанного перехода сетей Петри делает возможным проследить порядок событий, происходящих в системе, и смоделировать их динамику. В работах [253-256] вводятся следующие виды задержек: межконцевая задержка распространения пакетов, время выполнения запроса сервером, программная задержка, задержка ввода команды и задержка оценки результата.

Вводятся два критерия оценки выбора каждого из ЭТВ при формировании вариативности атаки: степень соответствия ЭТВ конечной цели комплексной атаки и степень достоверности знаний злоумышленника о параметрах атакуемой системы, существенных для реализации ЭТВ. Линейная комбинация значений этих критериев используется для принятия решения о выборе того или иного ЭАВ, весовые коэффициенты характеризуют стратегию поведения злоумышленника.

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

Таким образом, модели на базе сетей Петри успешно используются для описания последовательности действий (ЭТВ), при этом содержат механизмы для организации управляемого ветвления и моделирования динамики системы, что позволяет их использовать для моделирования атакующего воздействия и формирования комплексных ситуационных задач при тестировании ССЗИ.

1.7. Анализ проблемы синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности

1.7.1. Декомпозиция параметров синтеза массивов условно-реальных данных для тестирования сетевых средств защиты информации

Ранее в главе 1 введены объекты тестирования — ССЗИ (СОА, ТКО, САЗ и ИАСБ), показана их роль в качестве элементов обеспечения безопасности ИТС, ИС и АСУ (рисунок 1.7), а также выделены основные характеристики, подлежащие тестированию с точки зрения возможности выявления комплексных компьютерных атак и уязвимостей ИТС, ИС и АСУ.

Для обеспечения безопасности объектов ИТС требуются надежные ССЗИ, гарантировать качество которых возможно на основе положительных результатов 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.

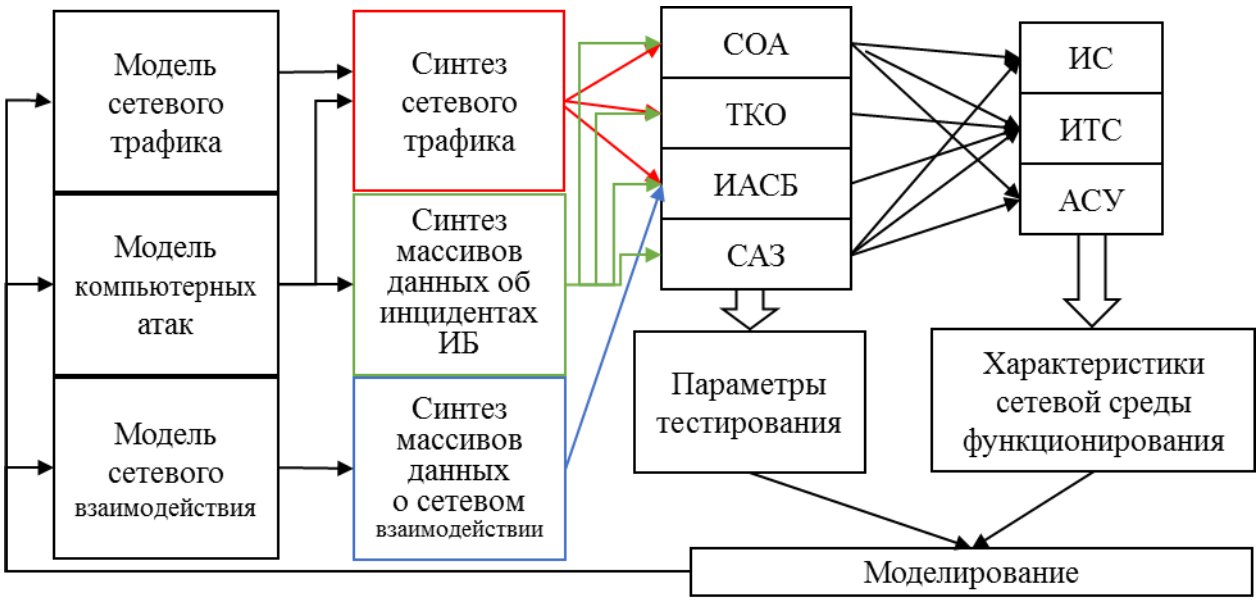

Рисунок 1.7. ССЗИ как объекты тестирования

В соответствии с функциональными задачами рассматриваемых ССЗИ выделяются три типа синтезируемых массивов условно-реальных данных: массивы се-

тевого трафика, массивы данных об инцидентах ИБ и массивы данных о сетевом взаимодействии пользователей ИТС.

Синтез массивов данных осуществляется на основе соответствующей модели и характеристик сетевой среды функционирования ССЗИ в ИТС, а также на основе параметров тестирования. На основе классификации ССЗИ, свойств каждого типа ССЗИ, характеристик, подлежащих тестированию, предложены параметры синтеза соответствующих массивов данных.

Основными параметрами синтеза массивов данных, которые применяются для тестирования СОА, ТКО, САЗ и ИАСБ, в дополнение к единым для всех массивов даты и времени событий являются параметры, представленные на схеме (рисунок 1.8).

Для массивов сетевого трафика:

— параметры IP-сессии;

— количественные статистические характеристики IP-сессии, рассчитываемые в единицу времени.

Для массивов данных об инцидентах ИБ:

— сведения об атакующем воздействии (атакующие, инструмент, доступ, этапы, источник / приемник, результат, цель);

— уязвимости, которые явились причиной инцидента ИБ.

Для массивов данных о сетевом взаимодействии пользователей ИТС:

— реквизиты абонента-источника соединения и принимающего соединение;

— тип соединения;

— количественные статистические характеристики соединения;

— параметры IP-сессии;

— идентификаторы базовых станций.

Представленные параметры являются основой для разработки модели ССЗИ как объекта тестирования, учитывающей при синтезе тестовых массивов параметры сетевого трафика заданной сетевой среды функционирования с учетом вариативности сетевых сред в ИТС.

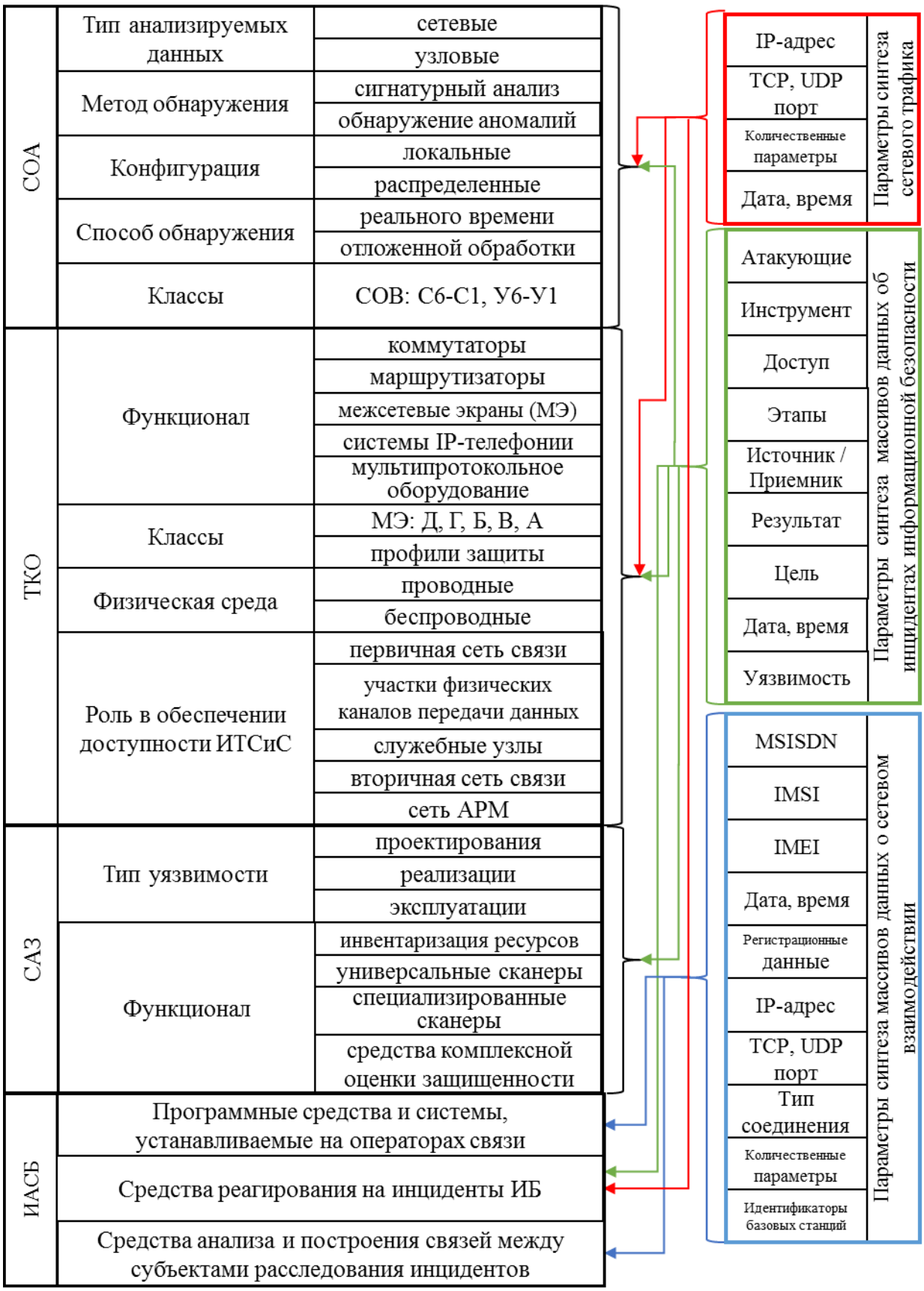

Рисунок 1.8. Классификация параметров синтеза массивов условно-реальных данных при тестировании ССЗИ

1.7.2. Критерии и параметры синтеза интерактивной сетевой среды для тестирования ССЗИ и расследования инцидентов информационной безопасности

Синтез как этап исследования системы предполагает разработку модели системы (включающую, в том числе выбор математического аппарата, моделирование, оценку модели по критериям адекватности), структурный и параметрический синтез) [257, 258]. В процессе структурного синтеза решаются три класса задач синтеза при проектировании системы: синтез структуры управляемой и управляющей систем и физической среды передачи информации. Для информационных систем наиболее распространенным является построение модели с использованием стандарта IDEF0 (разработанная функциональная модель в формате IDEF0 приведена далее в п. 4.1.2).

В общем случае структура киберполиона по расследованию инцидентов ИБ должна содержать следующие функциональные элементы:

– рабочие места обучаемых — могут быть распределены в рамках одного или нескольких компьютерных классов и лабораторий;

– информационные серверы — предназначены для хранения и обработки информационных массивов и запуска образов виртуальных машин, могут находиться в классах или быть вынесены в отдельное серверное помещение;

– рабочие места преподавательского состава — могут быть расположены в отдельной комнате либо размещены в классах;

– средства телекоммуникации — обеспечивают взаимодействие рабочих станций и информационных серверов. Средства телекоммуникации, обеспечивающие взаимодействие виртуальных систем, также могут быть виртуализированы;

– специализированные экспериментальные стенды — для проведения тестирования ССЗИ, могут быть распределены по лабораториям.

Основными объектами синтеза сетевой среды для тестирования ССЗИ и построения киберполигонов являются: фоновый сетевой трафик и сетевой трафик комплексного атакующего воздействия; данные о взаимодействии пользователей ИТС (биллинговая информация) и массивы биллинговой информации, содержа-

щие ситуационные задачи; уязвимости ИТС, интегрированные в совокупность образов уязвимых систем (таблица 1.3).

Таблица 1.3. Объекты синтеза сетевой среды для тестирования ССЗИ и построения киберполигонов по расследованию инцидентов ИБ

Объект синтеза	Тестирование ССЗИ				Расследование инцидентов ИБ			
	СОА	ТКО	ИАСБ	САЗ	Обнаружение КА	Аудит безопасности	Анализ инцидента ИБ	Выявление субъектов КА
Фоновый сетевой трафик	√	√	√	—	√	—	—	—
Сетевой трафик комплексного атакующего воздействия	√	√	√	—	√	—	√	√
Данные о взаимодействии пользователей ИТС	—	—	√	—	—	—	—	√
Массивы биллинговой информации, содержащие ситуационные задачи	—	—	√	—	—	—	√	√
Уязвимости ИТС в образах виртуальных систем	—	—	—	√	—	√	√	—

Таким образом, при синтезе интерактивной сетевой среды для тестирования ССЗИ и построения киберполигонов по расследованию инцидентов ИБ необходимо обеспечить:

— представление сетевой среды как совокупности фоновых и ситуационных массивов данных;

— наличие в составе массивов условно-реальных данных сетевого трафика и массивов данных о взаимодействии абонентов ИТС (биллинговой информации);

— наличие образов систем с заранее внедренными уязвимостями и реализованными инцидентами.

Основными требованиями к параметрам синтеза интерактивной сетевой среды при тестировании ССЗИ и построении киберполигонов по расследованию инцидентов ИБ являются (рисунок 1.9):

— вариативность сетевой среды;

— обеспечение комплексности ситуационных задач;

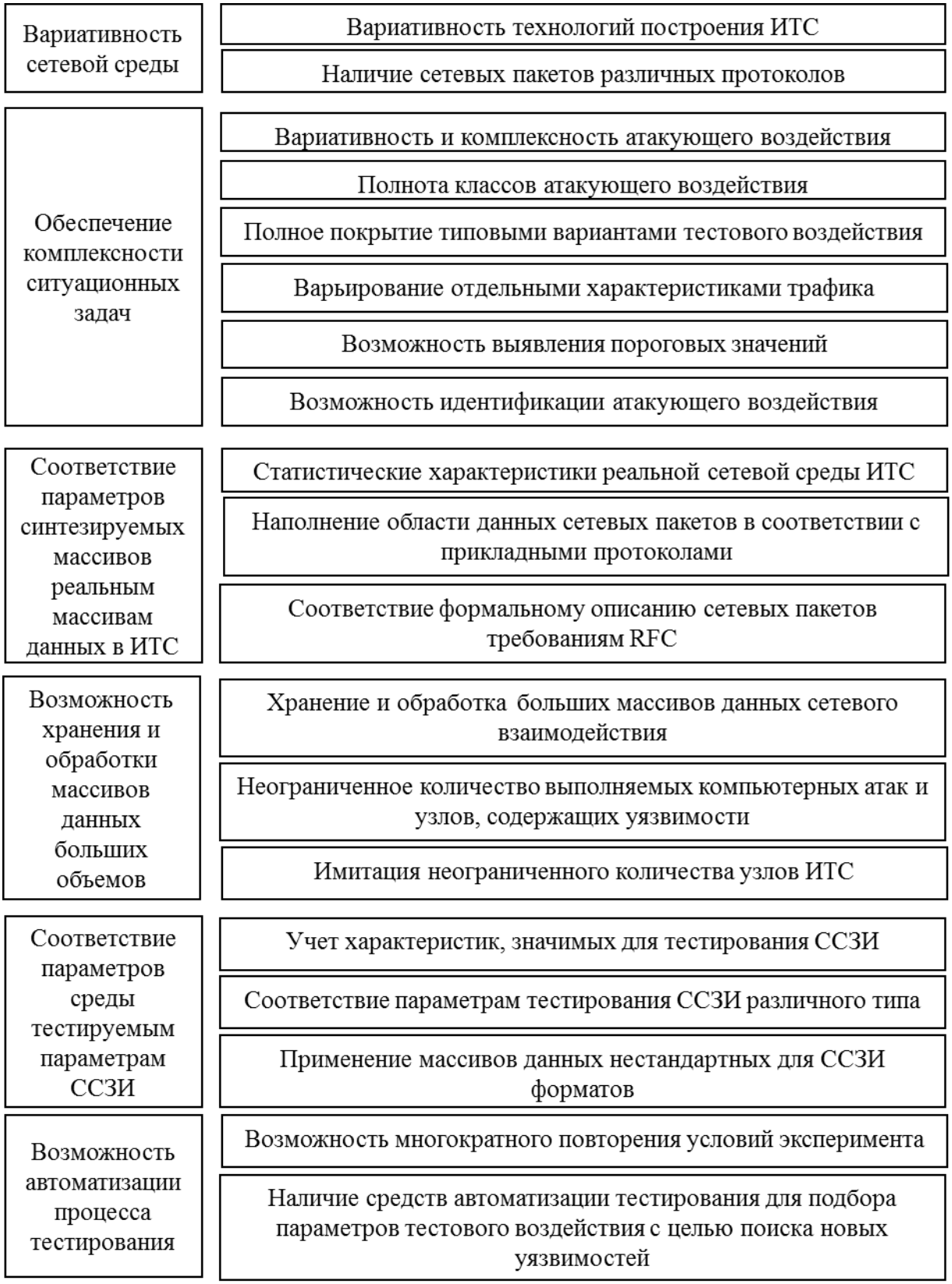

Рисунок 1.9. Ситематика требований к параметрам синтеза интерактивной сетевой среды

— соответствие параметров синтезируемых массивов реальным массивам данных в ИТС;

— возможность хранения и обработки массивов данных больших объемов;

— соответствие параметров среды тестируемым параметрам ССЗИ;

— возможность автоматизации процесса тестирования.

Критерием эффективности синтеза сетевой среды для тестирования ССЗИ и построения киберполигонов по расследованию инцидентов ИБ будем считать:

— создание комплексной учебной имитационной инфраструктуры для изучения методов расследования инцидентов ИБ, включающей совокупность информационных технологий и систем, имитирующих современные ИТС, и массивов учебных условно-реальных данных о сетевом взаимодействии, обеспечивающей вариативность ИТС и компьютерных атак;

— создание учебно-исследовательской имитационной инфраструктуры, позволяющей проводить тестирование ССЗИ для выявления уязвимостей и противодействия компьютерным атакам с целью обеспечения высокого уровня защищенности ИТС.

Проведенные систематизация и анализ современных технологий, методов и средств тестирования ССЗИ (рисунок 1.10), показали, что задача синтеза интерактивной сетевой среды относится к классу задач синтеза сложных систем, для которых в рамках имитационного моделирования применимы следующие математические методы, позволяющие учесть структуру и динамику сетевого взаимодействия объектов ИТС:

— эволюционно-генетический аппарат, широко используемый для решения задач оптимизации, в том числе может применяться в процессе подбора параметров массивов тестовых данных с целью выявления уязвимостей ССЗИ;

— алгоритмы сетей Петри, используемые для моделирования динамических дискретных систем, могут применяться для моделирования последовательности ЭТВ и синтеза динамической составляющей взаимодействия абонентов ИТС, где присутствует значительное количество активных объектов.

Кроме того, применяются теория вероятностей, математическая статистика, теория нечетких множеств и нечеткой логики, теория графов, теория матриц, модели сложных сетей.

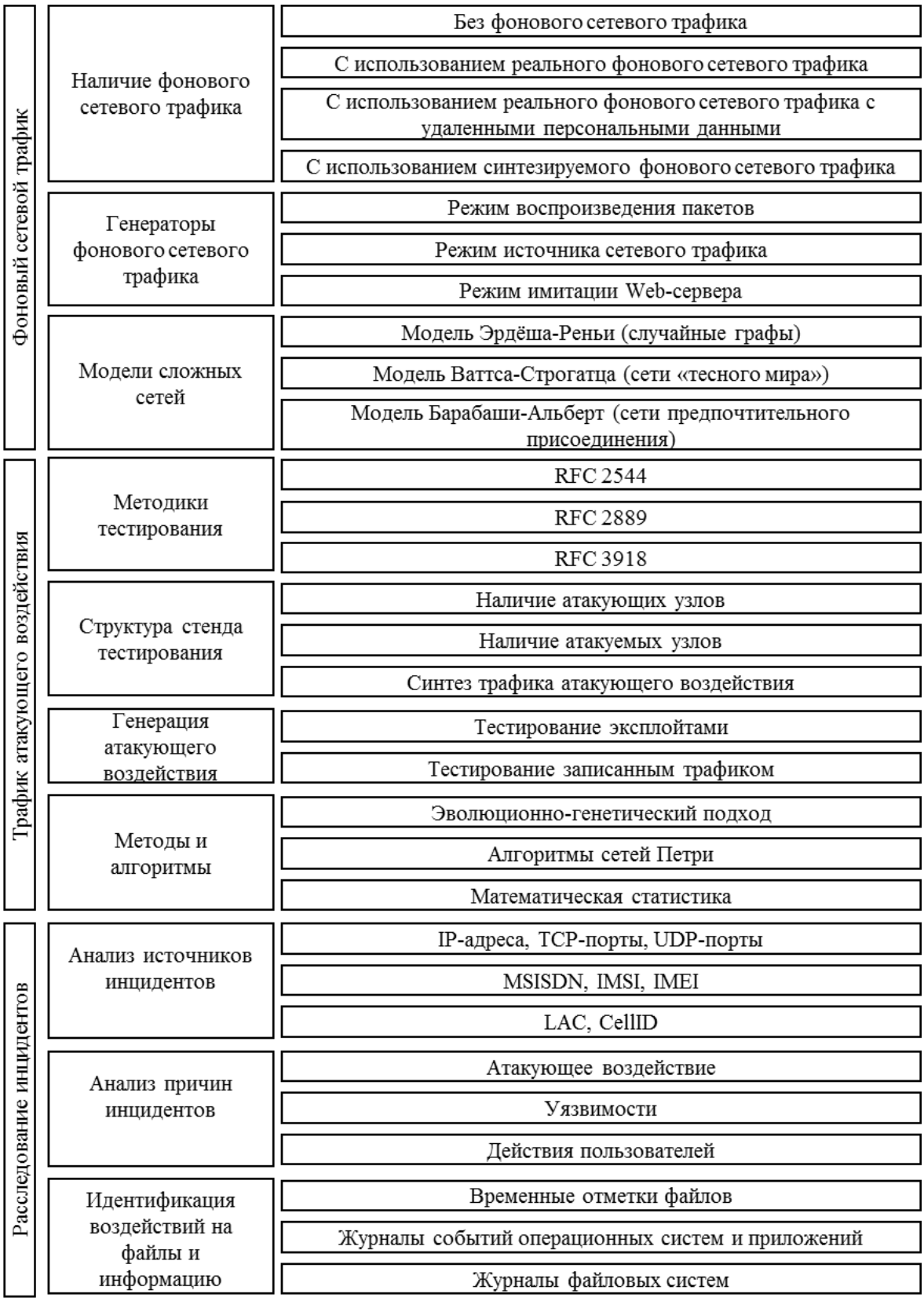

Рисунок 1.10. Систематика методов синтеза сетевой среды при тестировании ССЗИ

1.8. *Выводы по главе 1*

Глава 1 посвящена анализу ССЗИ и методов их тестирования. В ней даны понятие и систематика сетевых компьютерных атак. Компьютерная атака рассматривается как последовательность отдельных этапов, каждый из которых может быть выполнен несколькими возможными способами. Данная систематика позволяет при моделировании атакующего воздействия рассматривать комплексные атаки как совокупность элементарных атакующих воздействий. С целью дальнейшего обсуждения введено понятие и даны характеристики атак типа «отказ в обслуживании», направленных на ССЗИ, особенностью которых, является использование корректного сетевого трафика, соответствующего спецификациям используемых протоколов, параметры которого отличаются от штатного лишь количественно. Введены типы ССЗИ — СОА, ТКО, САЗ и ИАСБ как объекты тестирования. Показано, что все рассмотренные типы ССЗИ являются сложными интеллектуальными системами, в которых используются нетривиальные математические алгоритмы, проверка корректности реализации которых требует проведения тестирования различными наборами тестовых данных (трафика). В основе программных и программно-аппаратных ССЗИ лежит ПО, принимающее решение о том, является ли анализируемый ими поток данных атакующим воздействием или нет. Предполагается, что любое ПО имеет ошибки, особенно если речь идет о сложных многокомпонентных комплексах. Этими ошибками могут быть не только уязвимости реализации ПО, но и недостатки конфигурирования средств защиты. Ошибки в реализации и конфигурировании средств защиты являются одной из основных причин появления уязвимостей компьютерных систем, способствующих реализации угроз безопасности компьютерной информации.

Представлены основные типы СОА, приведены алгоритмы, лежащие в основе систем принятия решений СОА. Выделены параметры сетевого трафика, анализируемые СОА. ТКО рассмотрено как элемент ИТС. Приведены основные свойства маршрутизаторов и систем IP-телефонии. Уязвимость ТКО к атакам типа «отказ в обслуживании» определяется как его неспособность к обеспечению заданного требованиями ИТС уровня доступности обрабатываемой в ней информации. Данный уровень описывается совокупностью следующих параметров:

средней задержки при передаче пакета от отправителя получателю, джиттера и относительной доли потерь пакетов. Выделен отдельный тип ССЗИ — ИАСБ в контексте выявления и реагирования на инциденты информационной безопасности, дан обзор современных ИАСБ.

Представлен обзор известных технологий, методов и средств тестирования ССЗИ на примере СОА и ТКО. Рассмотрены известные реализации синтеза фонового сетевого трафика. Приведена классификация генераторов сетевого трафика, среди которых выделены категории генераторов, работающих в режимах воспроизведения пакетов, источника сетевого трафика, а также имитации Web-сервера.

Тестирование программных средств подразумевает наличие набора тестов, с помощью которых можно объективно оценить качество ПО. Тестирование проводится как в условиях натурного эксперимента, так и в условиях моделирования внешней среды. Имитация сетевой среды позволяет обеспечить высокую повторяемость результатов, возможность исследования большого количества вариантов и сценариев тестирования. При анализе известных подходов к тестированию ССЗИ выявлен ряд противоречий, требующих решения:

— для анализа наличия уязвимостей в ПО и конфигурировании ССЗИ явно недостаточным является выявление уязвимостей только с помощью универсальных сканеров безопасности. Проблема заключается в том, что большинство сканеров фактически атакующего воздействия не производят, и полученные с помощью них результаты не являются объективным доказательством наличия или отсутствия уязвимостей в реализации сетевых информационных систем;

— анализ защищенности сетевых систем необходимо проводить с применением так называемых эксплойтов — программ, выполняющих атакующее сетевое воздействие с использованием определенных уязвимостей. Ввиду большого количества подобных программ, имеющихся в сети Интернет как в исходном, так и в откомпилированном виде, не представляется возможным с помощью них выполнить всеобъемлющее тестирование сетевых средств в реальной сети;

— практически все программы-эксплойты относятся к категории вредоносных и могут привести, в частности к блокированию тестируемых систем;

— натурное тестирование образцов ССЗИ с применением образцов тестового

сетевого трафика является общепринятым и единственным эффективно реализуемым подходом к решению данной задачи. При этом тестирование в составе компьютерной сети защищаемого объекта может привести к нарушению ее работоспособности, поэтому оно должно производиться вне данной сети в специально подготовленной тестовой сетевой среде;

— возможность успешной реализации атак типа «отказ в обслуживании» в большинстве случаев оказывается взаимосвязана с рядом параметров сетевой среды функционирования ССЗИ, таких как количество взаимодействующих узлов, распределение узлов по сетям, подключенным к сетевым интерфейсам ССЗИ, и статистические распределения, которые определяют количество и структуру потоков сетевого трафика, генерируемого узлами. При этом существующие методики оценки защищенности ТКО не позволяют воспроизводить данные особенности в процессе тестирования ТКО с использованием синтезированного сетевого трафика.

Возможным решением указанных проблем является тестирование ССЗИ на специально разработанных стендах с применением моделей сетевой среды и атакующего воздействия. Во всех известных случаях организации стендов тестирования применялся одинаковый подход, заключающийся в выделении на стенде нескольких компьютеров-жертв с различными уязвимыми ОС и серверами приложений. Основными недостатками такого подхода, значительно усложняющими организацию стенда, являются следующие:

— значительное количество узлов-жертв атак. В связи с тем, что каждая сетевая атака обычно использует определенную уязвимость в программном коде конкретной версии ОС или серверного приложения, то для успешного проведения атаки необходимо устанавливать уязвимые версии ОС в уязвимых конфигурациях. Для каждой уязвимой версии ОС необходимо иметь на стенде отдельный компьютер. Проведение значительного количества разнообразных атак требует одновременной установки на стенде большого количества ОС и приложений различных версий;

— значительное количество атакующих узлов. Каждая сетевая атака так или иначе привязана к типу и версии ОС атакующего, следовательно, необходимо дополнительно оснащать стенд требуемым количеством атакующих узлов. Кроме

того, имитация многоузлового воздействия также требует значительного количества атакующих узлов;

— ограничения по количеству атак. Ограничения по количеству компьютеров-жертв и атакующих узлов приводят к наложению ограничений и по количеству различных атак, применяемых для тестирования. Это объясняется сложностью подбора готовых к выполнению программных модулей и сценариев атак, актуальных для ограниченного количества жертв;

— сложность автоматизации запуска атакующего воздействия. Стандартная процедура тестирования выглядит как последовательный запуск программных модулей, реализующих атаки. В том случае, когда требуются несколько компьютеров с различными ОС, достаточно сложно осуществить синхронизацию запуска атакующих приложений, так как для реализации ряда атак требуется вмешательство человека-оператора. Кроме того, выполнение некоторых атак, например, приводящих к блокированию сетевых служб или узлов, требует перезагрузки компьютеров-жертв, которая занимает продолжительное время и также должна быть инициирована оператором. В частности, атаки, приводящие к получению полномочий администратора, требуют не только перезагрузки компьютера, но, зачастую, и удаления следов использования этих полномочий (удаления вновь созданных пользователей, закрытия свободного доступа к разделам жесткого диска и пр.). Следовательно, циклическое автоматизированное выполнение такого рода атак становится затруднительным;

— сложность регистрации момента осуществления атаки. При ручном запуске атак на выполнение достаточно сложно точно зафиксировать момент, в который была предпринята попытка ее реализации. Следовательно, при анализе файла-журнала СОА также будут возникать проблемы с отнесением той или иной его записи к реализованным атакам.

В связи с указанными выше недостатками известного подхода в организации атакующего воздействия, был разработан новый подход, существенно отличающийся от решения, описанного выше. Предлагаемый подход к организации атакующего воздействия в задаче тестирования ССЗИ основан на формировании базы данных тестовых атак в виде массивов сетевого трафика.

Синтез трафика должен базироваться на математической модели сетевой среды функционирования ССЗИ, которая должна учитывать при синтезе 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.

Таким образом, проведенные систематизация и анализ современных технологий, методов и средств тестирования 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) показали актуальность решения следующих научных задач:

— 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;

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

— разработка алгоритма, обеспечивающего автоматизацию процесса выявления пороговых параметров устойчивости ССЗИ на примере ТКО к компьютерным атакам типа «отказ в обслуживании»;

— разработка моделей, алгоритмов и программного обеспечения синтеза массивов фоновых данных для тестирования СОА, ТКО и ИАСБ с обоснованием методов анализа реалистичности синтезируемых тестовых массивов;

— создание единого научно-методического инструментария имитационного моделирования при синтезе интерактивной сетевой среды для компьютерных полигонов;

— разработка алгоритмов и программных средств для создания учебно-научного компьютерного полигона для тестирования ССЗИ и расследования инцидентов информационной безопасности.

2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ НАУЧНО-МЕТОДИЧЕСКОГО ИНСТРУМЕНТАРИЯ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРИ СИНТЕЗЕ ИНТЕРАКТИВНОЙ СЕТЕВОЙ СРЕДЫ ДЛЯ КОМПЬЮТЕРНЫХ ПОЛИГОНОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. *Структура и компоненты комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности*

Как было показано в п. 1.1.1, для решения задач по:

— отработке практических навыков выявления компьютерных атак, расследованию инцидентов информационной безопасности, внедрения превентивных мер по предупреждению компьютерных атак;

— тестированию ССЗИ на реализацию функциональных возможностей, защищенность и наличие уязвимостей

техническая инфраструктура киберполигона в сфере информационной безопасности должна обеспечивать, в том числе:

— средства моделирования типовых пользовательских операций при работе в информационных системах;

— средства моделирования действий внешнего и внутреннего нарушителей, реализующие автоматические компьютерные атаки в зависимости от инфраструктуры компьютерной сети.

Для решения поставленной в диссертации научной проблемы разработан научно-методический инструментарий проектирования компьютерных полигонов в сфере информационной безопасности 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 информационной безопасности на объектах ИТС и ИС.

В основе разработанного научно-методического инструментария лежит представленный ниже комплексный метод синтеза интерактивной сетевой среды

для компьютерных полигонов, призванный обеспечить комплексность и вариативность тестового воздействия на ССЗИ (рисунок 2.1).

Комплексный метод предусматривает воздействие на тестируемый образец ССЗИ комбинации двух видов массивов данных: фонового и атакующего, для синтеза каждого из которых разработан собственный метод.

Метод синтеза массивов фоновых данных основан на модели интерактивной сетевой среды функционирования (далее — ССФ) ССЗИ (п. 2.2.2), матричной модели хранения статистических характеристик ССФ ССЗИ (п. 2.2.3) 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 (п. 2.3.1.2), динамическую модель комплексной атаки с применением алгоритмов сетей Петри (п. 2.3.1.3) и эволюционно-генетические алгоритмы для синтеза массивов атакующего воздействия (п. 2.3.2).

Имитационно-статистический метод синтеза массивов условно-реальных данных (п. 2.4.2) о взаимодействии пользователей ИТС основан на пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС (п. 2.4.1).

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.

Рисунок 2.1. Схема компонентов комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности

Процесс тестирования ССЗИ предполагает развертывание на специальном учебно-научном компьютерном полигоне ряда компонентов, входящих в состав экспериментальных стендов (рисунок 2.2).

Тестирование ССЗИ осуществляется по трем основным направлениям:

— выполнение требований к производительности ССЗИ, предъявляемых нормативными документами;

— выявление уязвимостей в программном обеспечении ССЗИ;

— корректность реализации аналитических алгоритмов и методик, встроенных в ССЗИ.

Результатом тестирования является отчетная документация, формируемая в том числе автоматизированным способом.

Процесс тестирования ССЗИ осуществляется в изолированной сетевой среде, максимально приближенной к условиям функционирования ССЗИ с учетом вариативности параметров современных компьютерных сетей. 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 в рамках сравнительного или сертификационного тестирования.

Тестовая среда, формируемая в соответствии с ССФ, должна соответствовать сетевой среде, наблюдаемой в реальных условиях.

Тестовый сетевой трафик генерируется в соответствии с выбранной моделью ССФ и состоит из двух компонентов: фоновый сетевой трафик (массив фоновых данных) и сетевой трафик атакующего воздействия (ситуационный массив данных). При генерации тестирующего массива происходит комплексирование фонового и атакующего массивов в единый массив, который подается на экспериментальном стенде на вход в тестируемый образец ССЗИ.

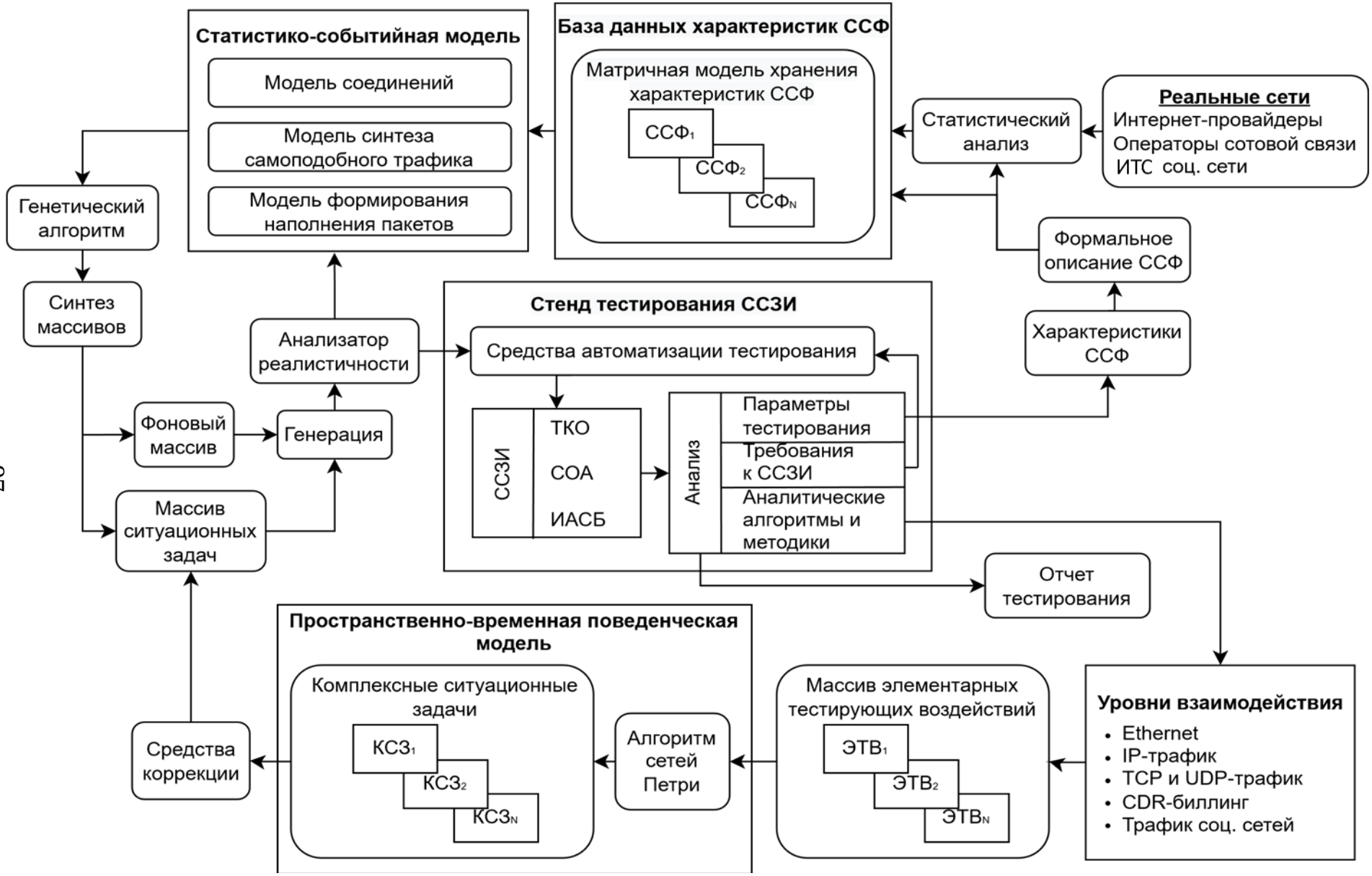

Рисунок 2.2. Схема взаимодействия компонентов метода синтеза интерактивной сетевой среды

Возможно изменение соотношения фонового и атакующего трафика в процессе тестирования с целью выявления граничных условий производительности ССЗИ.

Фоновый массив по статистическим характеристикам должен соответствовать трафику в реальных компьютерных сетях. Критерием соответствия синтезированного трафика реальному является его самоподобие. Для формирования фонового массива проводится анализ характеристик ССЗИ, подлежащих тестированию, и выбор характеристик такой ССФ, которая должна удовлетворять параметрам тестирования (рисунок 2.3). С целью осуществления повторяемости эксперимента фоновый трафик (массив) должен генерироваться по определенным закономерностям, учитывающим условия тестирования.

Рисунок 2.3. Формирование банка данных характеристик ССФ

Синтез трафика должен осуществляться на основе ранее сохраненных параметров реального трафика. Ввиду больших объемов информации неэффективно хранить сгенерированные массивы сетевого трафика для различных вариантов компьютерных сетей в силу значительного разнообразия их характеристик. Целесообразно осуществлять запись значимых для последующего синтеза характеристик трафика для их компактного хранения, для чего применяется матричная модель хранения характеристик внешней среды.

Для накопления соответствующих характеристик в виде базы данных заранее осуществляется съем статистики с реальных компьютерных сетей. При этом могут использоваться процедуры анализа сетевого трафика, статистические характеристики могут быть получены в сетях операторов связи, что не противоречит ФЗ «О связи».

Для реализации возможности синтеза трафика, идентичного ССФ ССЗИ в условиях конкретной ИТС, осуществляется выделение статистических характеристик с различных ИТС, где предполагается применение образцов ССЗИ. Полученный при этом банк данных характеристик ИТС формируется в виде набора матриц. Накопленная база данных статистических характеристик сетевых сред позволяет имитировать ИТС различных конфигураций. Каждая матрица представляет собой статистическое распределение одной из значимых характеристик внешней среды. При этом содержимое пакетов не анализируется и не хранится. Далее синтез массивов осуществляется на основании характеристик, заложенных в матричной структуре, с применением выбранной статистической модели и осуществляется на основе событий, инициируемых соответствующей моделью соединений, которая также отличается для различных видов ИТС и тестируемых ССЗИ.

При синтезе фонового трафика (рисунок 2.4) учитываются как статистические распределения потока пакетов, так и наполнение области данных прикладных протоколов высокого уровня. Формирование области данных обеспечивается на основе алгоритмов, применяющих марковские цепи для генерации массивов текстовых строк. Особенностями фонового сетевого трафика являются:

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

— соответствие формальному описанию сетевых протоколов, принятому в соответствующих рекомендательных документах типа RFC;

— соответствие с точки зрения самоподобия сетевому трафику реальных компьютерных сетей;

— соответствие особенностям тестирования ССЗИ определенного типа.

Далее проводится анализ реалистичности сформированного тестового массива. В качестве основного показателя соответствия синтезируемых массивов реальному трафику используется общепринятое свойство самоподобия телетрафика, для измерения степени соответствия используется показатель Херста.

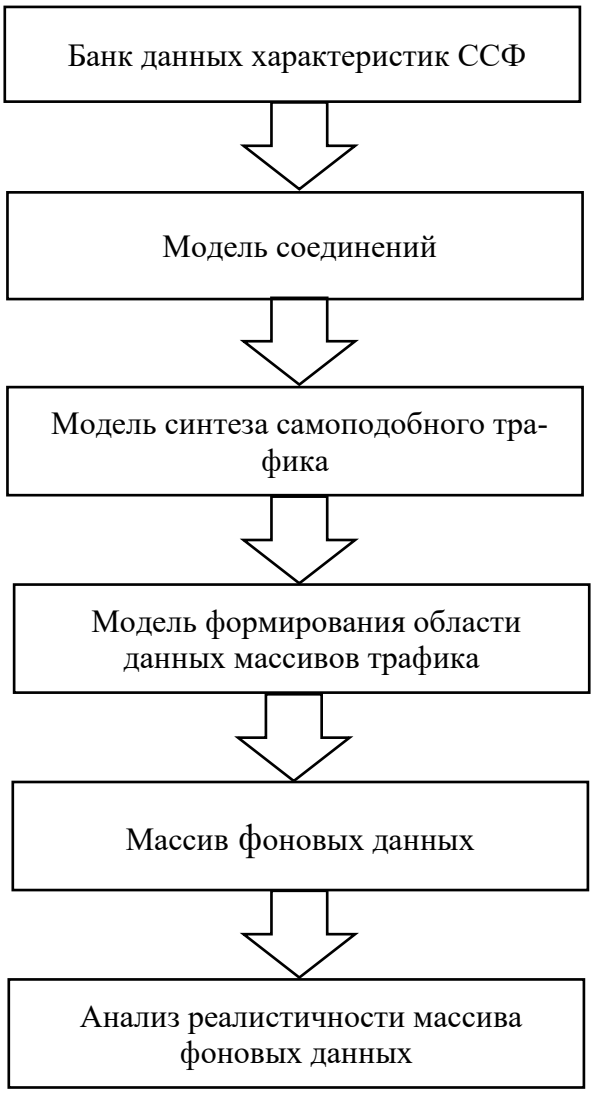

Рисунок 2.4. Формирование массива фоновых данных

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, позволяющий на основе исходной статистической модели осуществить варьирование отдельными характеристиками трафика.

Ситуационный (атакующий) массив данных содержит набор тестовых задач, предназначенных для выявления особенностей аналитической обработки ССЗИ различных пороговых значений и комбинаций в анализируемых данных. Атакующее воздействие рассматривается как совокупность характеристик сетевой среды, обладающая определенными закономерностями или сигнатурами.

Как и в случае с массивом фоновых данных, массив атакующего воздействия хранится в компактном в виде как набор характеристик сетевой среды. Атакующее воздействие (ситуационные задачи) предназначено для реализации двух видов тестов: тесты на анализ корректности реализованных в ССЗИ аналитических алгоритмов и методик и тесты на производительность аналитических комплексов. Для анализа корректности реализованных алгоритмов и методик выделяются типовые аналитические методики (типовые атаки), для каждой формируется набор ситуационных задач (тестов). Синтез атакующих (ситуационных) массивов данных осуществляется на основе алгоритмов сетей Петри, где ситуационные задачи (атаки в случае тестирования СОА) представляют собой формируемую по определенным правилам последовательность элементарных тестовых со-

бытий, распределенных по времени. Для хранения типовых элементарных воздействий применяются шаблоны, содержащие, например, набор пакетов сетевой атаки.

Исходный массив типовых элементарных воздействий формируется путем анализа известных атак на ИТС и ИС, на основе известных сценариев атакующего воздействия, кроме того, может формироваться аналитиком, проводящим тестирование.

На основе пространственно-временной модели и алгоритмов сетей Петри формируется совокупность ситуационных задач.

Особенностями трафика атакующего воздействия являются:

— полное покрытие всеми вариантами тестового воздействия всех видов сетевых компьютерных атак (всех видов ситуационных задач), характерных для тестируемого типа ССЗИ;

— представление всех классов атакующего воздействия;

— присутствие (необязательное) в атакующем трафике нестандартных сетевых пакетов, не удовлетворяющих требованиям стандартов RFC.

Система комплексирования позволяет объединять данные фонового массива и массива ситуационных задач по пространству (как адресному, так и географическому) и времени. Объединенный массив проходит анализ на самоподобие, после чего осуществляется его передача на соответствующий стенд, где функционирует средство автоматизации тестирования (рисунок 2.5).

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 выходу ССЗИ из устойчивого состояния работы, либо к нарушению его функциональных возможностей.

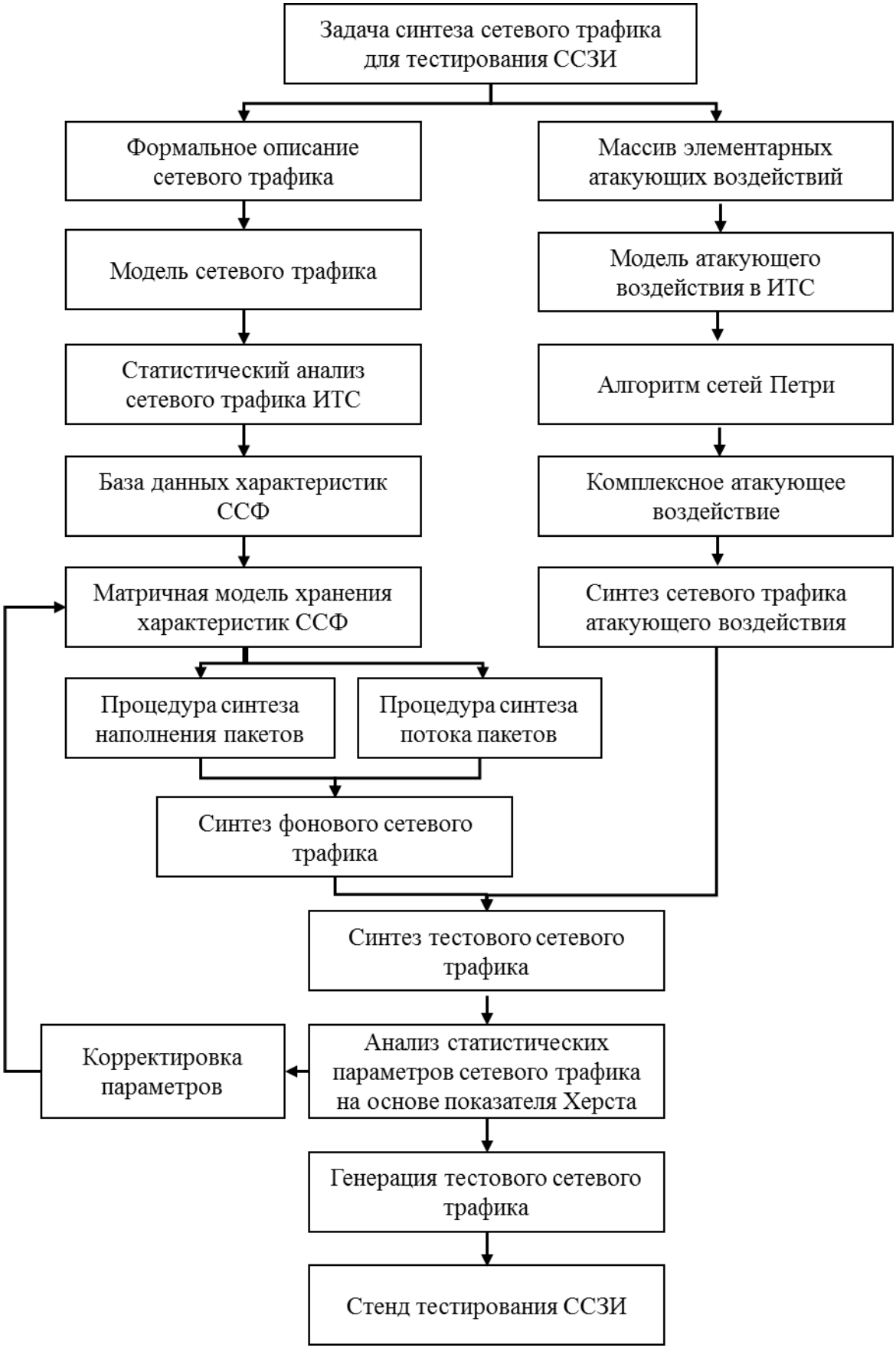

Рисунок 2.5. Схема синтеза сетевого трафика

С целью поиска новых уязвимостей ССЗИ к определенным сочетаниям параметров внешней среды целесообразна автоматизация процесса тестирования как поиск граничных (пороговых) значений атакующего воздействия.

Автоматизированная методика тестирования ССЗИ предназначена для выявления граничных 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» (рисунок 2.6).

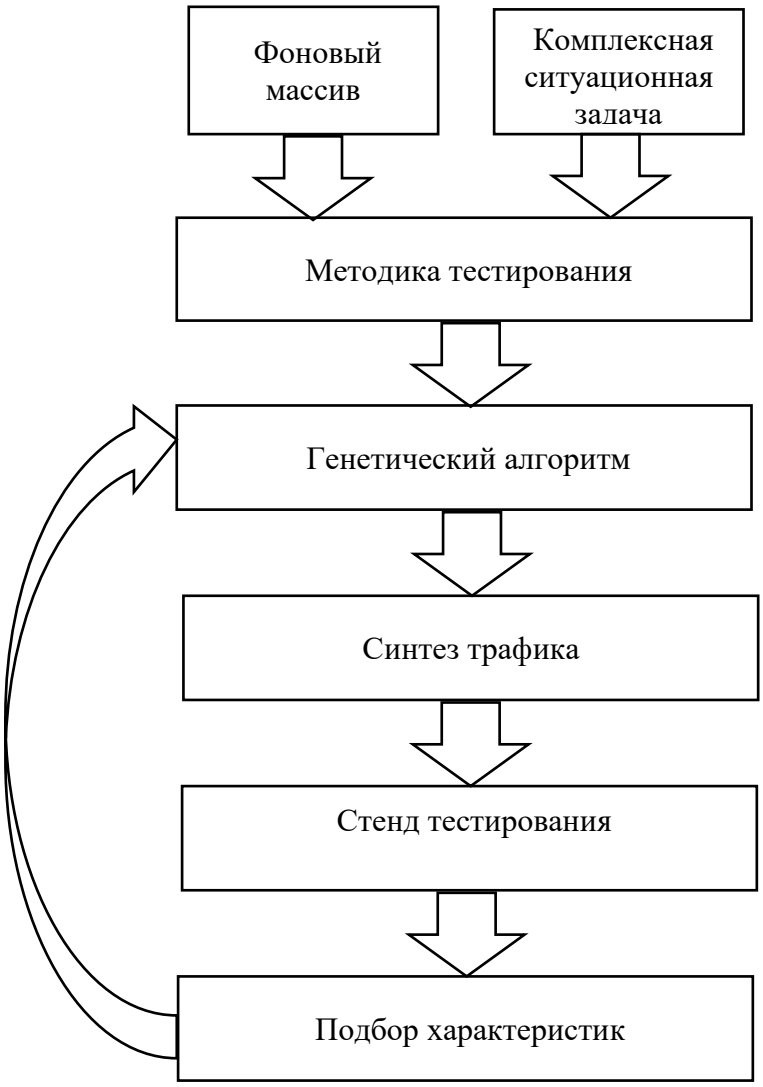

Рисунок 2.6. Автоматизация тестирования

Корректировка параметров сетевого трафика на основе применения генетического алгоритма реализуется при автоматизированном тестировании ТКО, что

позволяет на основе оптимизации переборных операций параметров сетевого трафика выявлять ранее неизвестные уязвимости (рисунок 2.7).

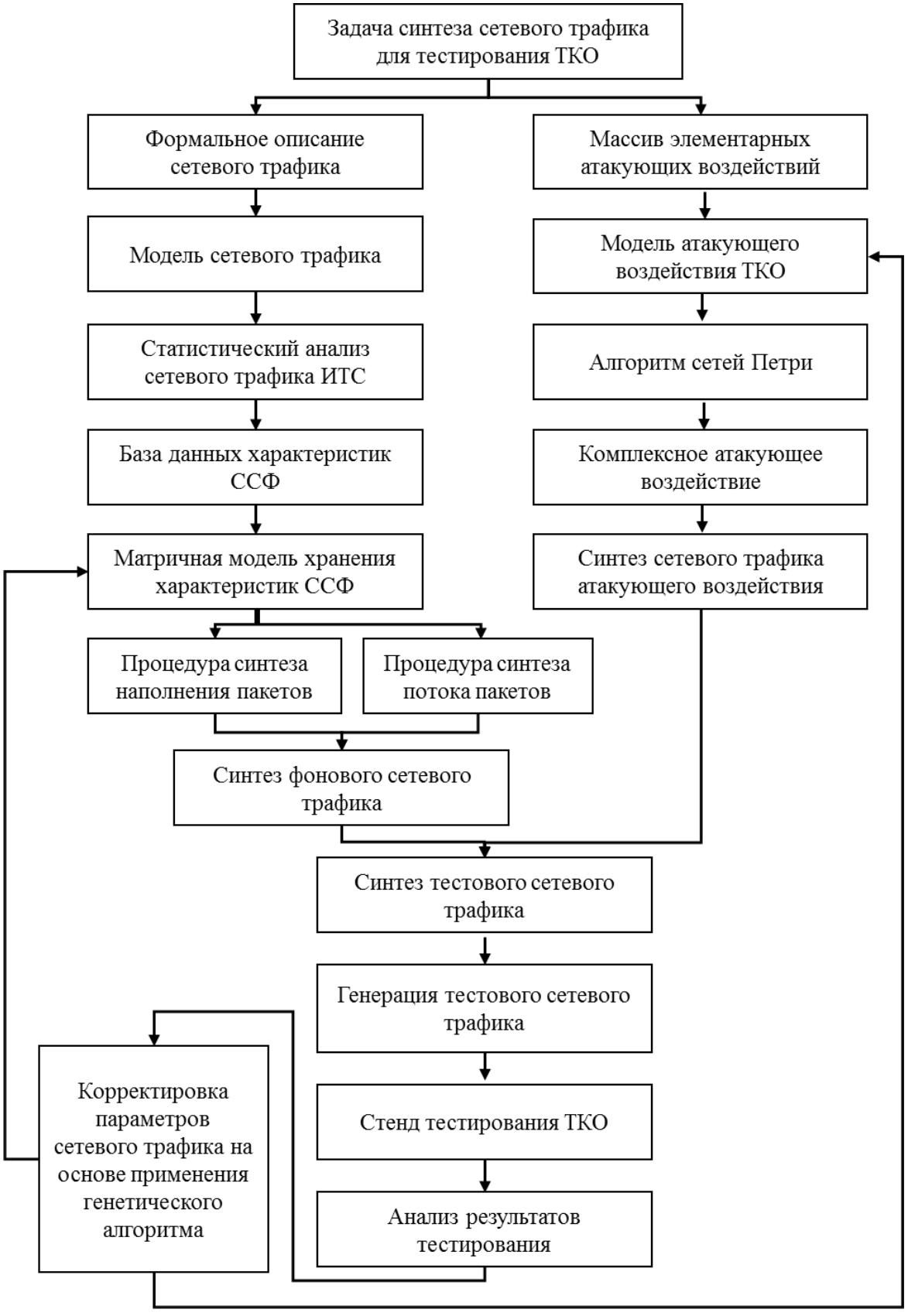

Рисунок 2.7. Схема синтеза сетевого трафика для автоматизированного тестирования ТКО

Для каждого ССЗИ разрабатывается уникальная методика тестирования, основанная на требованиях нормативных документов к данному виду ССЗИ.

Тестирование осуществляется с применением учебно-экспериментальных стендов, обеспечивающих:

— воздействие на тестируемое ССЗИ массивов фоновых данных (фонового трафика), по статистическим характеристикам соответствующему трафику в реальных компьютерных сетях, генерирующемуся по определенным закономерностям, учитывающим условия тестирования и вид ССЗИ;

— имитацию атакующего воздействия путем воспроизведения записанного трафика комплексной атаки, сформированной в автоматизированном режиме с применением алгоритмов сетей Петри, что позволяет снять ограничения по количеству выполняемых атак, обеспечивая их вариативность, адаптивность и повторяемость;

— автоматическую замену IP-адресов источника и назначения в воспроизводимых пакетах, что позволяет имитировать неограниченное количество узлов атакующих и уязвимых систем и полностью воссоздавать обмен сетевыми пакетами между атакующим и атакуемым узлами;

— упрощение процесса автоматизации атакующего воздействия и уменьшение числа узлов, используемых на стенде, за счет применения специально разработанного ПО тестирования;

— возможность идентификации атакующего воздействия и регистрации событий, связанных с атаками.

В случае большой вычислительной сложности алгоритмов синтеза тестовых данных либо больших объемов массивов данных применяется технология параллельных вычислений на кластере, представляющем собой совокупность серверов и ПЭВМ в стандартном исполнении [284].

В следующих разделах каждый из элементов предлагаемого комплексного метода моделирования интерактивной сетевой среды для построения компьютерных полигонов в сфере информационной безопасности рассматривается подробно.

2.2. *Методы, модели и алгоритмы синтеза массивов фоновых данных*

2.2.1. Метод синтеза массивов фоновых данных

Метод синтеза фоновых массивов данных, предназначенных для тестирования ССЗИ, представляется совокупностью элементов процесса синтеза массивов фоновых данных, включая синтез фонового сетевого трафика IP-сетей (рисунок 2.8), синтез массивов фоновых данных о взаимодействии абонентов сетей операторов сотовой связи, синтез массивов данных о взаимодействии пользователей в социальных сетях:

– формальное описание массивов фоновых данных с учетом структуры и размера моделируемой сети, а также характеристик массивов тестовых данных, значимых для тестирования ССЗИ;

– методы формирования значений векторов статистических характеристик массивов данных, позволяющие получать входные данные для построения матрицы статистических характеристик в зависимости от вида ССЗИ и перечня значимых характеристик;

– матричное представление статистических характеристик массивов данных, позволяющее хранить статистические характеристики, значимые для тестирования ССЗИ;

– процедура синтеза массивов данных на основе матрицы статистических характеристик с учетом модели сетевой среды функционирования ССЗИ;

– процедура синтеза области данных сетевых пакетов, основанная на применении теории марковских цепей;

– процедура оценивания реалистичности синтезируемого массива данных.

Модели сетевой среды функционирования для комплексов СОА и ТКО и должны коррелировать с моделями сетевой среды для комплексов и ИАСБ на уровне пространства IP-адресов.

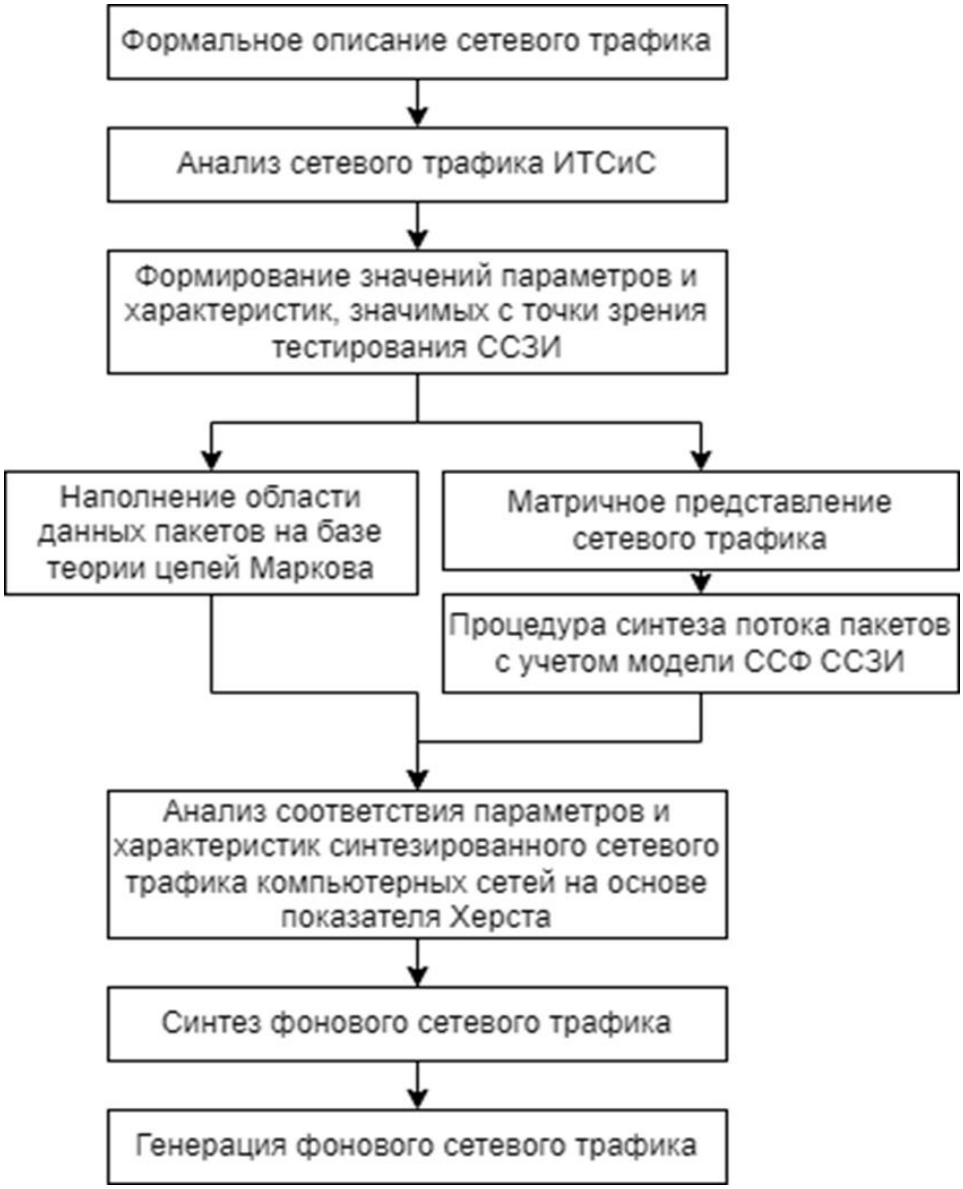

Рисунок 2.8. Схема метода синтеза фонового сетевого трафика

2.2.2. Модель интерактивной сетевой среды функционирования ССЗИ

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. Под топологией понимается распределение узлов между подсетями рассматриваемой сети. Харак-

теристиками сетевого трафика являются вероятностные распределения как потоков данных между узлами сети, так и распределения пакетов внутри потоков.

Основными классифицирующими признаками сетевых пакетов являются:

— идентификатор протокола a_k,

— IP-адреса узлов источника s_k и получателя d_k,

— номера портов (для протоколов транспортного уровня) или типы генерируемых сообщений (для протоколов управления сетью), где n_p — предельное значение данного параметра, принимаемое равным наибольшему номеру порта транспортного уровня — 65535: узла источника — $ps_k = \overline{\{1, n_p\}}$ и узла получателя — $pd_k = \overline{\{1, n_p\}}$,

— время отправки ts_k и приема tr_k пакета,

— задержка передачи пакета $z_k = tr_k - ts_k$,

— длина пакета l_k.

Каждый пакет k описывается в виде кортежа его характерных свойств, области определения которых задаются множествами:

$$k = \langle a_k, s_k, d_k, ps_k, pd_k, ts_k, tr_k, z_k, l_k \rangle \in K. \qquad (2.1)$$

Идентификатор протокола $a_k \in Y = \{1, \ldots, 255\} \subset \boldsymbol{N}$, длина пакета $l_k \in L = \{1, \ldots, MTU\} \subset \boldsymbol{N}$ (MTU — Maximum Transmission Unit, максимальный размер блока в байтах).

Каждый пакет k является элементом потока p, который в свою очередь принадлежит множеству всех возможных потоков P. Каждый из потоков p определяется параметрами, характеризующими логическое соединение между взаимодействующими сетевыми узлами:

— объем потока b (сумма длин пакетов l);

— момент времени начала потока τ;

— разность межпакетных интервалов i-х отправленного и принятого пакетов $t_{p,i}$:

$$t_{p,i} = (tr_i - tr_{i-1}) - (ts_i - ts_{i-1}). \qquad (2.2)$$

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

— средняя задержка передачи пакетов $\bar{z}$:

$$\bar{z} = \frac{\sum_{i=1}^{k} z_i}{k}, \quad (2.3)$$

— средняя разность межпакетных интервалов $\overline{t_p}$

$$\overline{t_p} = \frac{\sum_{i=1}^{k} t_{p,i}}{k}, \quad (2.4)$$

— среднеквадратическое отклонение разности межпакетных интервалов (джиттер), $\sigma(t_p)$

$$\sigma(t_p) = \sqrt{\frac{\sum(t_{p,i} - \overline{t_p})^2}{k-1}}. \quad (2.5)$$

Топология моделируемой сетевой среды описывается с помощью параметров: множество узлов сетей *H*, множество сетей *W*, множество *Y* сетевых интерфейсов, n_h, n_w, n_y — количество узлов, сетей и сетевых интерфейсов. Адреса источника и получателя $s_i, d_i \in H = \{1, \ldots, n_h\} \subset \boldsymbol{N}$ находятся в области *H* узлов моделируемой сети, сеть состоит из n_h узлов.

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 своими функциями распределения (далее — ФР). Определены векторы следующих статистических характеристик:

— не связанных с направлениями передачи данных:

$$C_0 = <F_h, F_f>, \quad (2.6)$$

где F_h — ФР вероятности события генерации трафика конечными узлами потока, F_f — ФР длительности сетевых сессий внутри потока;

— связанных с направлениями передачи:

- от узла-инициатора к взаимодействующему узлу:

$$C_1 = <F_{l1}, F_{t1}>, \quad (2.7)$$

- от взаимодействующего узла к узлу-инициатору:

$$C_2 = <F_{l2}, F_{t2}>, \quad (2.8)$$

где F_{li} — ФР размера пакета (длины), F_{ti} — ФР промежутка времени между началами передач двух последовательных пакетов.

Таким образом, поток P может быть описан выражением:

$$P = <a, s, d, ps, pd, b, \tau, \bar{z}, \sigma(t_p), C_0, C_1, C_2>. \quad (2.9)$$

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

Модель M интерактивной сетевой среды функционирования ССЗИ, используемая для синтеза тестового сетевого трафика, может быть представлена следующим выражением:

$$M=<H, W, Y, <P_i>^n_{i=1}, F_g, F_c>. \quad (2.10)$$

Разработанная модель M интерактивной сетевой среды функционирования ССЗИ 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.

2.2.3. Матричная модель хранения статистических характеристик сетевой среды функционирования ССЗИ

Синтез тестовых массивов данных осуществляется на основе статистических характеристик реальных ИТС, хранящихся в виде базы данных параметров сетевого трафика. В силу больших объемов информации и разнообразия ИТС, а также невозможности хранения содержимого пакетов в образцах трафика реальных сетей применяется метод хранения характеристик сетевой среды в виде набора матриц. Каждая матрица представляет собой статистическое распределение одной из значимых характеристик сетевой среды. Сетевой трафик делится на потоки, соответственно свойства сети определяются совокупными характеристиками всех сетевых потоков. 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. Особенностью матричного представления является возможность опера-

ций анализа характерных свойств потоков с помощью стандартных матричных операторов.

В соответствии с моделью сетевой среды функционирования ССЗИ для матриц характеристик сетевого трафика и составляющих их векторов используются следующие обозначения (для f потоков):

идентификатор протокола: $A = (\vec{a}_i) = (a_{ij}) \in \mathbf{R}^{f \times 255}$;

адрес узла источника: $S = (\vec{s}_i) = (s_{ij}) \in \mathbf{R}^{f \times n}$;

адрес узла получателя: $D = (\vec{d}_i) = (d_{ij}) \in \mathbf{R}^{f \times n}$;

порт источника: $PS = (\vec{ps}_i) = (ps_{ij}) \in \mathbf{R}^{f \times n}$;

порт получателя: $PD = (\vec{pd}_i) = (pd_{ij}) \in \mathbf{R}^{f \times n}$;

моменты времени начала потока: $T = (\vec{\tau}_i) = (\tau_{ij}) \in \mathbf{R}^{f \times q_\tau}$;

объем потока: $B = (\vec{b}_i) = (b_{ij}) \in \mathbf{R}^{f \times q_b}$

длины пакетов: $L = (\vec{l}_i) = (l_{ij}) \in \mathbf{R}^{f \times q_l}$;

задержка передачи: $Z = (\vec{z}_i) = (z_{ij}) \in \mathbf{R}^{f \times q_z}$.

Общей характеристикой сетевого трафика является матрица, состоящая из выставленных в ряд блоков в виде вышеуказанных матриц [193]:

$$F = \langle A, S, D, PS, PD, T, B, L, Z \rangle \in \mathbf{R}^{f \times \Sigma}, \qquad (2.11)$$

где $\Sigma = 255 + 2n + q_\tau + q_b + q_l + q_z$ (q — шаг дискретизации). Трансформируя и изменяя эти матрицы и их компоненты можно изменять результаты работы модели.

Наполнение матриц характеристик сетевого трафика значениями для конкретной ИТС производится на основе анализа дампа трафика. Дамп представляет собой набор сетевых пакетов, зафиксированных в предполагаемом месте установки ССЗИ. Алгоритм определения характеристик трафика сформирован на основе описания векторов характеристик (рисунок 2.9). После построения матриц, описывающих свойства потоков трафика, осуществляется формирование структуры трафика на основе алгебраических выражений. Дополнение векторов характеристик сетевого трафика производится путем разработки метода определения значений этих характеристик и формирования соответствующей матрицы. В таком случае весь алгоритм не изменяется, а происходит добавление новых шагов. Матрица идентификаторов потоков представляет собой совокупность векторов-указателей, содержащих значение 1 в индексе идентификатора протокола.

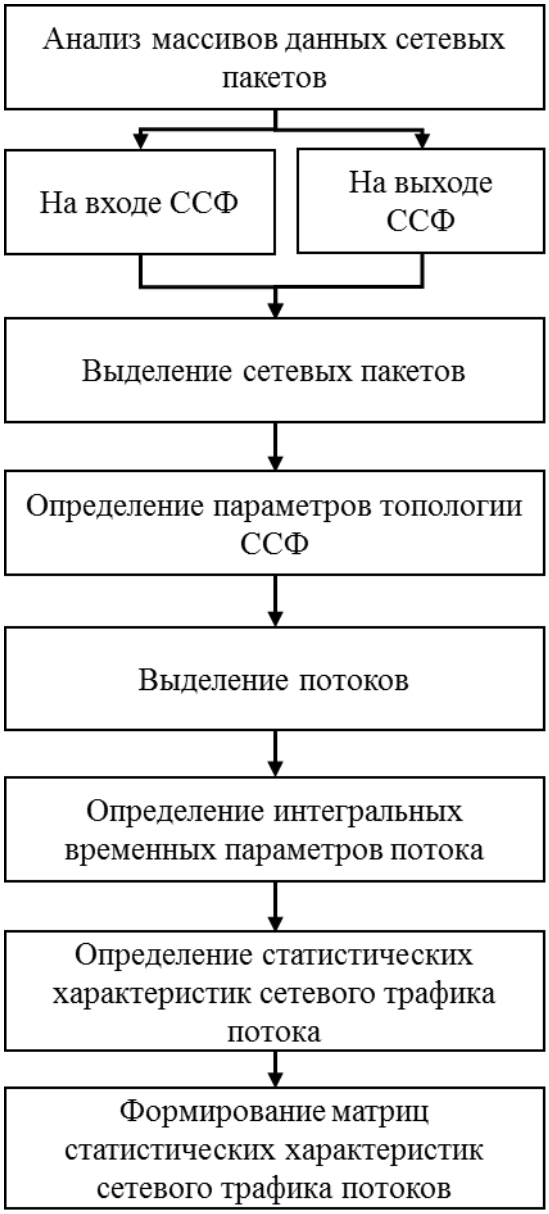

Рисунок 2.9. Схема алгоритма определения значений характеристик сетевого трафика

В связи со значительной вариативностью объемов потоков для их матричного хранения применяется функция квантования:

$$\Phi_{size}(b) = \max\left\{1, q_b\left(\frac{b-1}{b_{\max}-1}\right)^{\alpha}\right\}. \qquad (2.12)$$

Здесь $b_{\max}$ — максимальный объем потока в трафике, α — нелинейный коэффициент масштабирования, который позволяет сглаживать функцию квантования для широкого диапазона значений (от нескольких байт до гигабайт).

Для хранения моментов времени начала потоков используется отображение на ряд временных указателей $\{1,...,q_\tau\}$ с помощью функции квантования:

$$\Phi_{start}(\tau) = \max\left\{1, q_\tau\left(\frac{\tau}{\tau_{\max}}\right)\right\}. \qquad (2.13)$$

Сумма векторов моментов времени начала потоков дает гистограмму, показывающую распределение времени начала потоков.

В векторе-гистограмме распределений длин пакетов элемент l_{ij} представляет количество пакетов длиной j байт в i-ом потоке. Аналогично хранятся задержка канала передачи (вычисляется как средняя величина для отдельного потока) и частота потерь в канале передачи.

Хранение интервалов времени между пакетами Δt_{ij} осуществляется путем отображения на ряд временных указателей $\{1,...,q_g\}$ с помощью функции квантования (β — коэффициент масштабирования сглаживающей функции для диапазона от микросекунд до нескольких тысяч секунд):

$$\Phi_{time}(\Delta t) = \max\left\{1, q_g\left(\frac{\Delta t - \Delta t_{\min}}{\Delta t_{\max} - \Delta t_{\min}}\right)^{\beta}\right\}. \qquad (2.14)$$

Общее число исходящих потоков для каждого узла задается вектором $S^T\mathbf{1} \in \mathbf{R}^n$ (S^T — транспонированная матрица, 1 — вектор-столбец, состоящий из единиц, размерностью f), а общее число потоков получателей $D^T\mathbf{1} \in \mathbf{R}^n$. Число потоков между каждой парой узлов является произведением $S^T D \in \mathbf{R}^{n\times n}$. Причем элемент $(S^T D)_{ij}$ показывает число потоков, исходящих от узла i к узлу j.

Таким образом, матричная модель представляет собой характеристику каждого потока в виде совокупности векторов, позволяет анализировать ряд характерных свойств потоков с помощью стандартных матричных операторов.

2.2.4. Алгоритм синтеза фонового сетевого трафика

Алгоритм синтеза фонового сетевого трафика основан на преобразовании матрицы статистических характеристик трафика и состоит из пяти этапов (рисунок 2.10).

Этап 1. Выбор матрицы статистических характеристик сетевого трафика.

Этап 2. Формирование топологии синтезируемой ССФ.

Этап 3. Формирование интегральных временных параметров сетевых потоков.

Этап 4. Синтез сетевых пакетов с учетом статистических характеристик сетевых потоков и наполнение области данных сетевых пакетов, основанное на модели работы Web-сервера.

Этап 5. Оценка адекватности дампа сетевого трафика с использованием показателя Херста.

На этапе синтеза потоков пакетов происходит преобразование имеющейся матрицы характеристик сетевого трафика F (2.11) с использованием функций деквантования с учетом продолжительности тестирования. Генерация последовательности пакетов для потока f заключается в выборе случайным образом значений в соответствии со строкой матрицы f с характеристиками, описанными через вектор f_C. Выбор значения индекса $x \in \{1,...,q_c\}$, где q_c — максимальное значение определенной характеристики трафика, осуществляется случайным образом в соответствии с заданным распределением f_C.

С целью синтеза области данных сетевых пакетов рассматривается Web-трафик как информационный обмен между Web-сервером и пользователем, осуществляемый путем отправки запросов и обработки ответов в виде передачи Web-страниц, содержащих статические и динамические компоненты.

Алгоритм синтеза области данных сетевых пакетов предполагает автоматизированное, определяемое требуемыми характеристиками информационного обмена формирование запросов к Web-серверу и передаваемых дан-

ных, позволяющее динамически изменять структуру Web-сервера в ходе тестирования.

Рисунок 2.10. Схема алгоритма синтеза фонового сетевого трафика

Алгоритм синтеза области данных сетевых пакетов реализуется цепью Маркова с дискретным временем. Для генерации текста используется матрица переходов, при этом множество всех слов, знаков препинания и тегов является пространством состояний. Формирование переходной матрицы осуществляется на основе множества html-страниц, по которым производится оценка вероятности создания (составления) новой фразы (включая конструкции языка гипертекстовой разметки) после последовательности уже созданных фраз. Модуль формирования страниц на Web-сервере производит расстановку рангов полученным страницам, определяя предполагаемый маршрут перемещения посетителя по Web-сайту и модель посещения Web-сервера. Рассмотренная модель взаимодействия с Web-сервером позволяет

генерировать запросы к страницам в зависимости от начальных условий, матрицы переходов и наполнения сервера.

На этапе генерации потоков пакетов применяется следующий алгоритм синтеза потоков пакетов:

1. Случайный выбор пары узлов источника s и получателя d.
2. Выбор объема потока b:

$$\Phi_{size}(b) = \max\left\{1, (b_{\max} - 1)\left(\frac{x}{q_b}\right)^{\frac{1}{\alpha}}\right\}. \quad (2.15)$$

3. Выбор используемых в потоке длин пакетов l согласно гистограмме и выбранному объему потока b.
4. Выбор интервалов времени между пакетами Δt с учетом средней величины задержки $\overline{z}$:

$$\Phi^{-1}_{time}(\Delta t) = \Delta t_{\min} + (\Delta t_{\max} - \Delta t_{\min})\left(\frac{\Delta t}{q_g}\right)^{\frac{1}{\beta}}. \quad (2.16)$$

5. Вычисление средних значений длин пакетов и интервалов времени между пакетами $\overline{l}$ и $\overline{\Delta t}$, средней продолжительности потока $\overline{t_f}$:

$$\overline{t_f} = b\frac{\overline{\Delta t}}{\overline{l}}. \quad (2.17)$$

6. Выбор момента времени начала потока τ (сумма $\tau + \overline{t_f}$ меньше либо равна продолжительности генерации):

$$\Phi^{-1}_{start}(x) = \tau_{\max}\frac{x}{q_\tau}. \quad (2.18)$$

7. В выбранный момент времени начала потока τ происходит отправка первого пакета.
8. Выбор и отправка следующего сетевого пакета.
9. Процесс продолжается до окончания времени генерации, либо до момента времени окончания всех потоков. Последний пакет, вне зависимости от распределения, переносит оставшееся количество байт.

На завершающем этапе производится оценка адекватности дампа сетевого трафика с использованием показателя Херста, заключающаяся в сравне-

нии значений показателя Херста для исходного и сгенерированного трафиков. При наличии показателя в интервале от 0,5 до 1 считается, что синтезированный трафик соответствует трафику реальных ИТС [124, 192].

2.2.5. Процедура анализа реалистичности тестовых массивов условно-реальных данных

Одно из требований, предъявляемых к фоновому СТ, является сходство статической и динамической составляющих синтезированного СТ и трафика существующих компьютерных сетей. В основе современных компьютерных сетей лежит коммутация пакетов, пакеты по сети поступают на конечные узлы не по отдельности, а пачками. Трафик имеет выраженный характер пульсации, что повышает вероятность перегрузок в узлах сети, которые вызывают потери и задержки при передаче пакетов. Однако, в мультисервисных сетях, к которым относятся компьютерные сети, число событий на заданном промежутке времени зависит от предыдущих отдаленных событий. Трафик компьютерной сети обладает свойством самоподобия, то есть выглядит качественно одинаково при любых масштабах временной оси, характеризуется высоким пик-фактором (отношение пиковой интенсивности процесса поступления пакетов на обслуживание к его среднему значению). Наличие этих свойств у синтезированного СТ является одним из аргументов при оценке его сходства с реальным [54, 147]. Характеристикой наличия самоподобия является показатель Херста H (Hurst parameter), значения которого находятся в диапазоне от 0,5 до 1 (рисунок 2.11).

Рисунок 2.11. Связь между параметрами фрактальных процессов

Равенство этого коэффициента 0,5 указывает на отсутствие самоподобия, а близость к 1 — на проявление фрактальных свойств. Существующие исследования в области фракталов и самоподобия СТ [124, 192, 194, 195] указывают на значение показателя Херста в диапазоне от 0,68 (аудио трафик) до 0,8 (трафик потокового видео).

Для вычисления показателя Херста при анализе реалистичности СТ используется метод *R/S*-анализа [192, 194, 195], где R − размах накопленного отклонения выбранной фрагмента траектории, попадающего во временной интервал $[L_{min}, L_{max}]$ (с математической точки зрения − временного ряда (ВР)), S − математическое ожидание фрагмента анализируемого ВР.

Анализируемый ВР x_k разделяется на N смежных интервалов длиной L, на каждом из которых вычисляются:

- средние значения ВР:

$$\bar{x} = \frac{1}{L} \sum_{i=1+(n-1)L}^{nL} x_i \, ; \tag{2.19}$$

- математическое ожидание фрагмента анализируемого ВР, попадающего в данный временной интервал:

$$\sigma_n = \left[\sum_{i=1+(n-1)L}^{nL} (x_i - \bar{x}_n)^2 \right]^{0,5} ; \tag{2.20}$$

- накопленные отклонения соответствующих фрагментов ВР:

$$X_n = \sum_{i=1+(n-1)L}^{nL} (x_i - x_n) \, ; \tag{2.21}$$

- значение размаха накопленного отклонения:

$$[R_{max}]_n = \max(X_n) - \min(X_n) \, ; \tag{2.22}$$

- отношения накопленных отклонений к математическому ожиданию данного фрагмента ВР:

$$[R/S]_n = [R_{max}]_n / \sigma_n \, ; \tag{2.23}$$

- по ансамблю значений среднее значение отношения накопленных отклонений к математическому ожиданию соответствующего фрагмента ВР:

$$\left[\overline{R/S}\right]_N = \frac{1}{N}\sum_{i=1}^{N}[R/S]_n. \quad (2.24)$$

Метод оценки адекватности СТ заключается в сравнении значений показателя Херста для исходного и сгенерированного трафиков. Оценка соответствия реализуется с помощью вычисления значений показателя Херста для каждой из множества $i = 1, N$ пар образцов синтезированного и исходного СТ. Если значения отличаются незначительно, то можно говорить о наличии у синтезированного трафика фрактальных свойств.

Таким образом, сравнение синтезированного трафика с исходной реализацией осуществляется с помощью вычисления показателя Херста, который выступает показателем «пульсации» СТ. Анализ литературы позволяет выделить интервал значений этого параметра от 0,5 до 1, который наблюдается в существующих компьютерных сетях.

2.3. *Методы, модели и алгоритмы синтеза атакующего воздействия и ситуационных задач*

2.3.1. Модель формирования атакующего воздействия, основанная на теоретико-графовом подходе и применении стохастических сетей Петри

2.3.1.1. Графы атак при моделировании уязвимых систем

Граф атак — это граф, представляющий всевозможные последовательности действий нарушителя для достижения угроз (целей). Такие последовательности действий называются трассами (путями) атак, где под атакой понимается использование нарушителем уязвимости [277]. В контексте сетей Петри уязвимости узлов сети являются взвешенными вершинами, переходы — выполнение элементарных атак, где элементарная атака представляется множеством условий (предусловий), необходимых для реализации атаки с использованием определенной уязвимости, и множеством следствий (постусловий) — изменений состояния сети вследствие использования уязвимости и реализации атаки.

Условия и постусловия описываются в терминах общей система оценки уязвимостей системы CVSS (Common Vulnerability Scoring System) [235], предназначенной для проведения оценки защищенности ИТС на основе метрик по шкале критичности от 0 до 10. Метрики защищенности CVSS позволяют оценивать защищенность компьютерной сети и ее компонентов с различной степенью детализации и с учетом разнообразных аспектов. Основными метриками CVSS являются метрики «вектор атаки», «сложность доступа» и «требуемый уровень привилегий» (ранее — «аутентификация»), которые характеризуют условия применения уязвимости. Базовая метрика «вектор атаки» (Attack Vector, AV) отражает то, при каком виде доступа уязвимость может быть обнаружена атакующим и использована; метрика «сложность доступа» (Access Complexity, AC) определяет, насколько сложно провести атаку на систему путем использования уязвимости; метрика «требуемый уровень привилегий» (Privileges Required, PR) определяет, сколько уровней аутентификации

и авторизации должен пройти злоумышленник прежде, чем он получит возможность использовать уязвимость в системе. Каждая уязвимость описывается интегральной оценкой критичности атакующего воздействия Base Score (принимает значения от 0 до 10) с учетом воздействия уязвимости на конфиденциальность, целостность и доступность информации. Для наделения вершины графа весом (в относительной интервальной шкале [0,1]) вводятся следующие характеристики оценивания, предложенные в [277]:

– *C(h)* — критичность узла *h*, определяется по трехуровневой шкале, исходя из назначения узла;

– *S(a)* — уровень критичности атакующего воздействия *a*, рассчитывается с использованием обобщенной оценки критичности атакующего действия *(Base Score (a))* CVSS;

– *M (a,h)* — размер ущерба, вызванного реализацией атакующего действия с учетом уровня критичности атакуемого узла;

– *AC (a)* — сложность доступа для атакующего действия *(Access Complexity (a)),* рассчитывается на основе данных, заложенных в CVSS;

– *R(t)* — степень возможности реализации угрозы *t*;

– *RL (t)* — уровень риска реализации угрозы *t*;

– *SL(h)* — уровень защищенности анализируемого узла*;*

– *SL* — уровень защищенности сети в целом.

Размер ущерба *M (a,h)*, вызванного успешной реализацией атакующего воздействия, находится в зависимости от критичности атакуемого узла *C (h)* и от общего уровня критичности атакующего воздействия *S (a)*.

Критичность узла определяется по трехуровневой шкале (высокая, средняя, низкая) исходя из назначения узла и выполняемых им функций. Наивысший уровень критичности узла означает угрозу блокирования ресурсов всей сети при условии нарушения работы узла вследствие использования уязвимостей злоумышленниками. Далее в сторону уменьшения уровня критичности идут рабочие серверы, функционирование которых (каждого по отдельности) является важной составляющей успешного функционирования ИТС. Для рабочих станций обычно устанавливается низкий уровень критич-

ности, так как нарушение их функционирования незначительно влияет на работоспособность ИТС в целом. В качестве исходных данных для построения графа используются данные о топологии имитируемых ИТС, включая данные о количестве узлов, их назначении (степени критичности), наличии сетевых служб (открытых портов) и перечне имитируемых уязвимостей. В процессе формирования графа атак применяется ряд операций, предложенных в теоретико-графовом подходе к задачам количественного анализа защиты информации в компьютерных системах [254].

2.3.1.2. Теоретико-графовая модель распространения атакующего воздействия в иерархической системе уязвимых объектов

Синтез атакующего воздействия осуществляется в два этапа — на первом этапе формируется статический граф атакующего воздействия, на втором — его динамическая составляющая. Конечной целью моделирования является синтез последовательности пакетов для генерации и имитации комплексного атакующего воздействия. При этом комплексная компьютерная атака должна быть представлена совокупностью элементарных 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 моделируемых ИТС и ИС и временных интервалов. Характеристиками имитируемых ИТС и ИС являются диапазоны IP-адресов, функциональность узлов с точки зрения сетевого взаимодействия, имитируемая сетевая инфраструктура, соответствие уязвимостей ИТС и ИС элементарным тестирующим воздействиям (далее — ЭТВ), имеющимся в тестовой базе.

С целью моделирования начальных условий для формирования атакующего воздействия, а также формирования траектории развития компьютерной атаки в моделируемой уязвимой системе применена теоретико-графовая модель распространения атакующего воздействия в иерархической системе уязвимых объектов. Модель базируется на ранее разработанном теоретико-

графовом подходе к задачам количественного анализа защиты информации в компьютерных системах [254].

Синтез (проектирование) комплексного атакующего воздействия в иерархической системе уязвимых объектов системы основан на исходных параметрах, которые представляются в виде двудольного графа *G (A, H, E)* (рисунок 2.12). Комплексные компьютерные атаки представляются в виде множества вершин *A* одной доли графа, а атакуемые узлы имитируемой уязвимых ИТС — в виде множества вершин *H* другой доли графа. Множество ребер (дуг) такого графа *E* выражает степень реализуемости компьютерной атаки по отношению к атакуемому узлу.

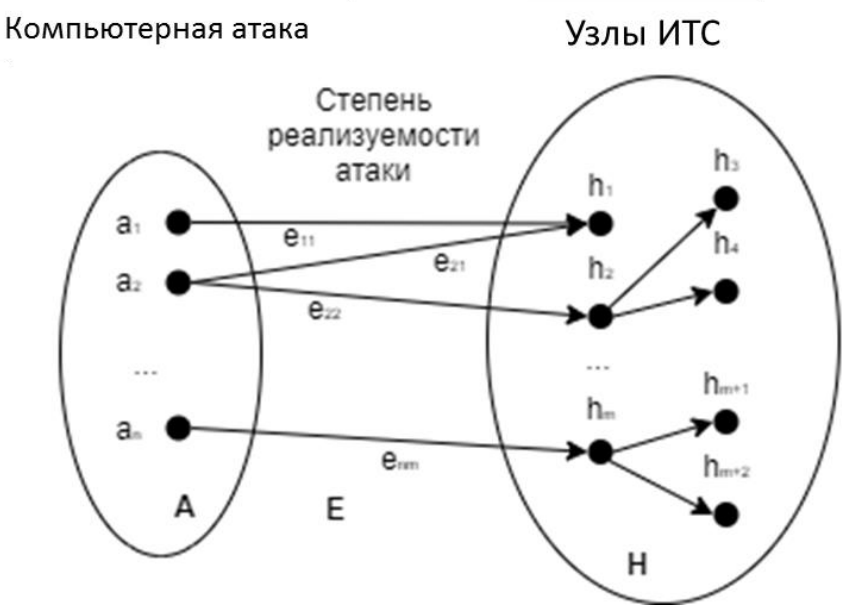

Рисунок 2.12. Граф комплексного атакующего воздействия

Граф *G (A, H, E)* комплексного атакующего воздействия будем считать вершинно и реберно взвешенным. Веса вершин компьютерных атак a_k характеризуют потенциальную реализуемость компьютерной атаки по отношению ко всем узлам *H* имитируемых ИТС и определяются как триплет чисел $a_k(a_k^{(1)}, a_k^{(2)}, a_k^{(3)})$. Параметры $a_k^{(1)}$, $a_k^{(2)}$ и $a_k^{(3)}$ выражают вес компьютерной атаки с точки зрения воздействия на конфиденциальность ($a_k^{(1)}$), целостность ($a_k^{(2)}$), и доступность ($a_k^{(3)}$) информации на атакуемых узлах. Веса узлов ИТС h_m характеризуют потенциальную уязвимость узла ко всему множеству компьютерных атак из *A*. Веса узлов ИТС также определяются тройкой чисел

$h_m(h_m^{(1)}, h_m^{(2)}, h_m^{(3)})$, где $h_m^{(1)}$ — уязвимость узла к воздействию на конфиденциальность, $h_m^{(2)}$ — целостность, $h_m^{(3)}$ — на доступность информации.

Веса ребер $e_{km}(e_{km}^{(1)}, e_{km}^{(2)}, e_{km}^{(3)})$ определяют степень реализуемости атаки k по отношению к узлу m. Степень реализуемости компьютерной атаки измеряется от 0 до 10 в зависимости от усредненной интегральной оценки критичности атакующего воздействия Base Score с учетом воздействия уязвимости на конфиденциальность ($e_{km}^{(1)}$), целостность ($e_{km}^{(2)}$) и доступность информации ($e_{km}^{(3)}$). Все веса представляют собой неотрицательные вершины.

Конечный граф атакующего воздействия является двудольным – компьютерная атака, узел ИТС, степень реализуемости атаки, при этом комплексная атака осуществляется зачастую путем воздействия на удаленный узел не напрямую, а посредством иных узлов. Атакующее воздействие сначала может быть реализовано на один (или несколько) узел сети, над которым нарушитель может получить управление, далее атака будет развиваться с этого узла. При таком воздействии формируется иерархическая структура ИТС (с точки зрения атакующего), граф перестает быть двудольным.

При этом возможность распространения атаки зависит от ряда условий, прежде всего от возможностей, полученных нарушителем на предыдущем этапе. Таким образом, итоговая возможность совершения атаки на узел складывается из возможности прямой и опосредованной атак. В результате проявляется вариативность учета уязвимости узлов ИТС. Вариативность еще более усиливается при использовании технологий доменной архитектуры или удаленного доступа, когда ряд узлов являются доверенными для остальных элементов ИТС, однако доверенные узлы могут иметь уязвимости и быть подвержены атакам. Каждая комплексная компьютерная атака из множества A в моделируемой системе представлена подмножеством ЭТВ I, имеющихся в тестовой базе атакующего воздействия в виде массивов сетевого трафика. Каждое ЭТВ из множества I использует одну или несколько уязвимостей из множества V.

Каждая уязвимость в соответствии с метрикой стандарта CVSS воздействует на конфиденциальность CI, целостность II и доступность информации

AI в определенном соотношении, а также характеризуется способом доступа *AV*, сложностью доступа и реализации атаки *AC*, необходимостью аутентификации *Au*, что позволяет рассматривать уязвимость как кортеж: *V = <AV, AC, Au, CI, II, AI>*. Каждая уязвимость из множества *V* присутствует в определенном программном обеспечении и операционных системах, т.е. соответствует некоторому подмножеству в множестве программного обеспечения *En*. Каждый узел ИТС из множества *H* имеет набор программного окружения, соответствующий элементам множества *En*, кроме того, каждый узел может иметь связь с другими узлами сети, разрешенную наличием соединения и политикой межсетевого экранирования, определяемую наличием сервиса *S* или клиентского ПО *K*. Каждый сервис и клиент из множеств *S* и *K* ориентирован на использование определенного TCP/UDP порта из множества портов *P*.

Рассматривая моделируемую ИТС как 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 $G(A, I, V, En, H, S, P, E^{AI}, E^{IV}, E^{VEn}, E^{HEn}, E^{HH}, E^{SP}, E^{HS})$.

Множество дуг графа *G* представляют прямоугольные матрицы:

– 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 (клиента);

– E^{SP} — использование сервисом TCP/UDP-порта.

Необходимость учета взаимной сетевой достижимости узлов ИТС приводит к тому, что граф комплексного атакующего воздействия *G* перестает удовлетворять условию дольности, доля *H* графа, представляющая узлы ИТС, если редуцировать дуги, соединяющие ее вершины с вершинами доли E^{HEn}, является графом типа «лес». Для решения задачи на основе матрицы E^{HH} взаимной сетевой достижимости узлов ИТС строится итоговая матрица

достижимости узлов по отношениям структурной вложенности E^{HHR}. Вычисление матрицы E^{HHR} осуществляется на основе степеней матрицы E^{HH} по выражению:

$$E^{HHR} = E^{HH} + (E^{HH})^2 + (E^{HH})^3 + \ldots + (E^{HH})^n, \qquad (2.25)$$

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 $G(A, I, V, En, H, S, P, E^{AI}, E^{IV}, E^{VEn}, E^{HEn}, E^{HH}, E^{SP}, E^{HS})$ 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 компьютерной атаки к узлу. В графе G_{ij} множества вершин и дуг представляют собой подмножества соответствующих вершин и дуг графа G (рисунок 2.13).

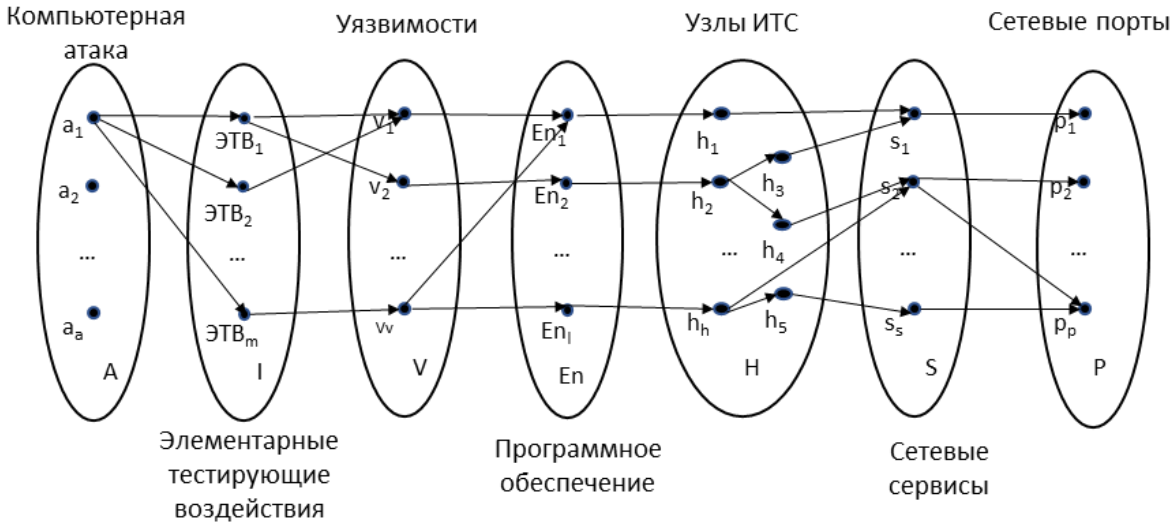

Рисунок 2.13. Граф воздействия комплексной атаки на узел ИТС

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 пользователя к ресурсу.

В процессе определения смежных вершин последовательно анализируется совокупность матриц графа G на наличие элементов, отличных от 0 (наличие связи), перечень таких вершин фиксируется. При построении путей анализируется зафиксированный перечень вершин, и вершины последовательно добавляются в новый граф G_{ij} с учетом вариативности путей воздействия комплексной компьютерной атаки.

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 ЭТВ (путей развития атаки в графе G_{ij}) с применением алгоритмов сетей Петри. На основе данной формализации возможно получить ряд соотношений, позволяющих вычислять степень уязвимости узлов с учетом сочетания возможности прямой атаки на узел, а также опосредованной атаки, проводимой через иерархию узлов в сети.

Матричные операции позволяют рассчитывать возможности атакующих при наличии взаимосвязи между узлами ИТС, а также при наличии на узлах сети уязвимостей, которые могут быть использованы злоумышленниками. Расчеты количественных параметров предоставляют возможность строить графы атак, что особенно важно при проектировании комплексного атакующего воздействия.

2.3.1.3. Динамическая модель комплексной атаки с применением алгоритмов сетей Петри

Модель компьютерной атаки, применяемая для синтеза сетевого трафика атакующего воздействия, отражает как статическую, так и динамическую (последовательность пакетов ЭТВ и временных интервалов) составляющие трафика.

Синтез атакующих (ситуационных) массивов данных осуществляется на основе алгоритмов сетей Петри, где ситуационные задачи (атаки в случае тестирования СОА) представляют собой формируемую по определенным

правилам последовательность элементарных событий, распределенных по времени. Для задачи синтеза массивов атакующего воздействия используются обобщенные стохастические сети Петри (англ. Generalized Stochastic Petri Nets) [215-222, 253] — сети Петри со случайными задержками, в которых помимо переходов со случайными задержками существуют также мгновенные переходы.

Статическое состояние атакующего воздействия, определяющее множество позиций сети Петри (фишек) и множество переменных состояния, формируется на основе теоретико-графового подхода. Позициями (фишками) сети Петри являются ЭТВ.

С переходами рассматриваемой сети Петри связаны два типа событий: изменение состояния модели и генерация очередного Ethernet-кадра атакующего воздействия, при этом используется база данных компьютерных атак, содержащая сетевой трафик, записанный в ходе реализации известных компьютерных атак. Выбор перехода сети Петри основывается на весовых коэффициентах, присвоенных уязвимостям, используемым при атакующем воздействии, в соответствии с CVSS.

Компьютерная атака развивается во времени, значительная часть временных задержек носит стохастический характер, определяемый, в частности, временем передачи сетевых пакетов между атакующим и атакуемым. Переход сети Петри выбирается исходя из значения задержки, которое формируется как совокупность задержек при передаче пакета из одной точки компьютерной сети в другую, при ответе сервера на поступивший запрос, при вводе атакующим очередной команды или запуске очередного эксплойта с учетом времени реакции атакующего для оценки результата предыдущего действия. Величина задержки при передаче пакета является случайной и зависит от пропускной способности маршрутизатора и количества пакетов, поступающих на обслуживание в единицу времени [222-224]. Величины задержек и временных интервалов определяются на основе статистической модели имитируемой ИТС, хранящейся в базе данных характеристик ИТС, представленной в п. 2.2.3. Выбор ЭТВ, являющегося элементом комплексной

атаки, осуществляется на основе графа атакующего воздействия «атака-узел» G_{ij}, учитывающего факты вхождения ЭТВ в комплексные атаки, использования ЭТВ уязвимостей, воздействия уязвимостей на программное окружение, наличие программного обеспечения на узлах ИТС, сетевую структуру ИТС, наличие открытых TCP/UDP-портов и сетевых сервисов (рисунок 2.14).

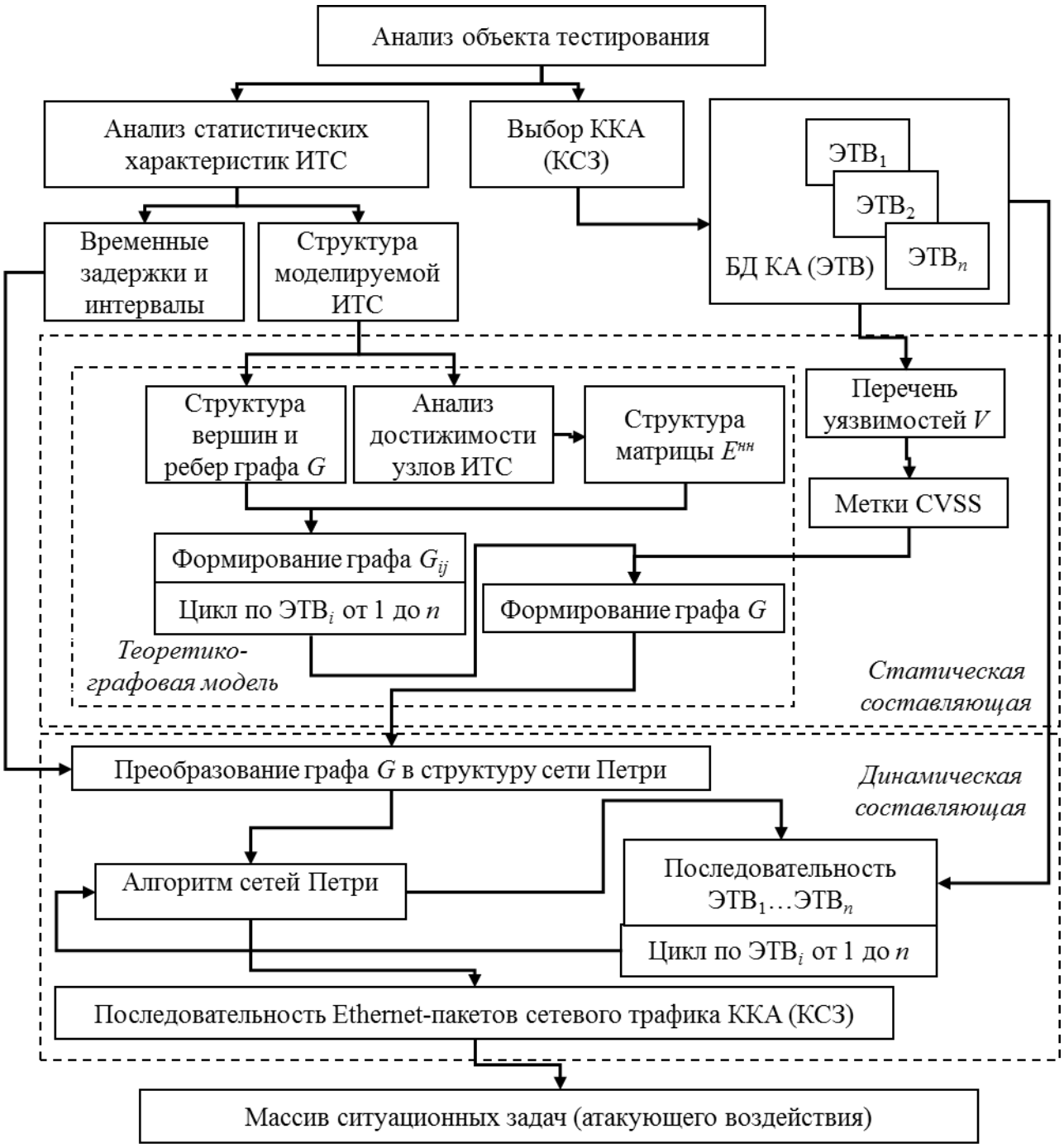

Рисунок 2.14. Схема процесса синтеза массива атакующего воздействия

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.

Предложенная динамическая модель комплексной атаки предполагает альтернативное развитие атаки, а также случайный характер синтезируемых задержек. Задача выбора ЭТВ – многокритериальная задача принятия решения в условиях неопределенности. После того как ЭТВ выбрано, оно должно быть реализовано, причем результатом должен стать сетевой трафик, используемый затем для тестирования СОА.

В качестве модели сетевого трафика ЭТВ также используется стохастическая сеть Петри. Пространство состояний модели определяется множеством позиций и множеством переменных состояния. Текущее состояние модели, то есть фаза ЭТВ, описывается расстановкой фишек в позициях сети и конкретными значениями переменных состояния. При формировании содержимого пакета используется база данных реализации известных компьютерных атак, содержащая пакет сетевого трафика атакующего воздействия и реакции узла-жертвы. Структура сети Петри определяет алгоритм атаки. Многоальтернативность действий атакующего и случайный порядок событий моделируется при помощи взвешенных переходов, находящихся в состоянии конфликта (имеющих общие входные позиции).

Представленная модель комплексной атаки, применяющая аппарат сетей Петри для придания динамики и многоальтернативности имитируемого тестового воздействия, позволяет описывать:

– алгоритм проведения комплексной компьютерной атаки с учетом выбора альтернатив ее проведения с учетом элемента случайности;

– динамическую составляющую ЭТВ как совокупность детерминированных и (или) случайных задержек, зависящих как о свойств сетевой среды, так и от моделируемого поведения нарушителя.

Таким образом, совокупность статической теоретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов и динамической модели комплексной атаки с при-

менением алгоритмов сетей Петри позволяет реализовать управляемый процесс синтеза сетевого трафика комплексных компьютерных атак. Полученный сетевой трафик может многократно использоваться для тестирования, в том числе сравнительного, различных систем обнаружения атак.

2.3.2. Эволюционно-генетический подход к синтезу массивов атакующего воздействия

В соответствии с моделью сетевой среды *M*, представленной в п. 2.2.1, осуществляется формирование образцов трафика для тестирования ТКО, процедура подробно описана в [268 и 278]. Совокупность параметров трафика для тестирования ТКО может быть представлена в виде вектора ψ в общем пространстве параметров тестового сетевого трафика Ψ. Одна из задач ТКО — обеспечение передачи информации с обеспечиваемой степенью доступности информации $\omega \in \Omega$, которая может быть нарушена атакующим воздействием атака типа «отказ в обслуживании». Соответственно, тестирование ТКО с применением данных образцов позволяет определить соответствие между параметрами тестового трафика и обеспечиваемой ТКО доступностью.

Процесс выявления уязвимости ТКО к атакам типа «отказ в обслуживании» представляет собой поиск сочетаний параметров сетевого трафика атакующего воздействия, к которому ТКО оказывается уязвимо. Такой процесс является задачей переборного типа, которая может быть сведена к задаче отыскания экстремумов многомерной функции $\omega(\psi)$ и решена с применением алгоритмов поиска оптимальных решений. Одним из вариантов решения которой является применение генетических алгоритмов [55].

При разработке генетического алгоритма в рамках эволюционно-генетического подхода необходимо определить [56] параметры особи (входные и выходные); функцию приспособленности особи; механизм скрещивания; механизм мутации; механизм селекции; условия завершения генетического алгоритма.

Параметры особи. В качестве входных параметров особи рассматри-

вается совокупность параметров модели сетевой среды функционирования ССЗИ M (п. 2.2.1), описывающей топологию моделируемой сети и структуру циркулирующего в ней сетевого трафика: H, W, Z, $\langle G_i \rangle_{\mathrm{i}=1}^{n_g}$, F_g, F_c.

В качестве выходных параметров используются элементы вектора ψ, описывающего сетевой трафик в соответствии с предложенной моделью и результаты тестирования образца ТКО: $<n_h, n_w, n_z, p_s, p_{tcp},\ p_{\mathrm{udp}},\ p_{icmp},\ \overline{n_f},\ \sigma(n_f),\ \overline{t_f},\ \sigma(t_f), \overline{l_{p,}}, \sigma(l_p), \overline{t_p}, \sigma(t_p), \overline{t_d}, \sigma(\delta t_p), q>$.

Результаты тестирования образца ТКО определяют обеспечиваемую ТКО доступность информации $\omega \in \Omega$ и отражают успешность применения данного сетевого трафика как потенциальной реализации атаки типа «отказ в обслуживании»

Структура вектора ψ:

— количество узлов n_h, сетей n_w и сетевых интерфейсов n_z;

— относительная доля p_s пакетов, сгенерированных узлами-инициаторами соединений;

— относительные доли потоков протоколов TCP p_{tcp}, UDP p_{udp} и 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 $\sigma(t_p)$);

— 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.

Входные параметры особи представлены в виде хромосомы — структуры, определяющей взаимное расположение множества генов. Ген — структурная единица хромосомы, ответственная за формирование альтернативных значений внутренних признаков особи, в качестве которой используется последовательность бит заданной длины, кодирующая значение определенного признака. Генотип особи — представление значений параметров модели се-

тевой среды функционирования ССЗИ M в виде последовательности бит (бинарной строки). Множества H и W модели задают количество моделируемых узлов и сетей, а также принадлежность узлов сетям, представлены в виде матрицы A_{hw}, где значение элемента $\alpha_{i,j} = 1$ означает принадлежность узла j к сети i, а значение $\alpha_{i,j} = 0$ — ее отсутствие.

Участок ϕ_1 хромосомы χ, отражающий содержание параметров H и W модели, является последовательностью целых чисел, записанных в двоичной системе счисления, где $\alpha_{i,j}$ является битом $(i-1)$ гена j:

$$\phi_1 = \langle \chi_{1,j} \rangle_{j=1}^{n_h}, \forall j: \left(\chi_{1,j} = \sum_{i=1}^{n_w} 2^{i-1}\, \alpha_{i,j}\right). \quad (2.26)$$

Данный участок хромосомы имеет длину $n_w n_h$ бит.

Параметр Y особи определяет количество сетевых интерфейсов ТКО и то, какие моделируемые сети к ним подключены. Данный параметр может быть представлен в виде матрицы A_{WY}, где значение элемента $\alpha_{i,j} = 1$ означает подключение (непосредственное или через промежуточные сети) сети j к сетевому интерфейсу i ТКО, а значение $\alpha_{i,j} = 0$ — его отсутствие. Таким образом, участок ϕ_2 хромосомы, отражающий содержание параметра Y модели, может быть представлен как последовательность целых чисел, записанных в двоичной системе счисления:

$$\phi_2 = \langle \chi_{2,j} \rangle_{j=1}^{n_w}, \forall j: \left(\chi_{2,j} = \sum_{i=1}^{n_y} 2^{i-1}\, \alpha_{i,j}\right). \quad (2.27)$$

Данный участок хромосомы имеет длину $n_w n_Y$ бит.

Для представления функции распределения вероятности генерации потока F_g и количества генерируемых потоков в секунду F_c используется участок ϕ_3 хромосомы, включающий два гена, каждый из которых содержит бинарное представление функции распределения:

$$\phi_3 = \langle F_g,\, F_c \rangle. \quad (2.28)$$

Массив групп потоков $\langle G_i \rangle_{i=1}^{n_g}$ представляется участком ϕ_4 хромосомы, каждый из генов которой является описанием группы потоков G_i в виде би-

нарной строки. Количество бит, выделенных параметрам a, s_i, d_i, $p_1 p_s$, p_d, определяется предельными значениями количества типов потоков, узлов сетей, и возможных номеров портов транспортного уровня. Общее количество групп потоков равно n_g.

Таким образом, хромосома χ особи генетического алгоритма представляет собой последовательность участков χ_1-χ_4:

$$\chi = \langle \phi_1, \phi_{2,} \phi_{3,} \phi_4 \rangle. \tag{2.29}$$

Критерий оптимальности решения. Особенностью генетического алгоритма, реализованного для решения задачи тестирования ТКО, является необходимость многокритериальной оптимизации. В процессе тестирования ТКО выявляются области пространства параметров сетевого трафика, где по крайней мере один из параметров доступности информации превышает заданный порог. Для определения оптимальности решения при проведении размножения и селекции производится ранжирование популяции $\{\mu_i\}_{i=1}^{n_\mu}$ по значениям параметров доступности информации $\{\omega_i\}_{i=1}^{n_\mu}$ в последовательность γ:

$$\gamma = \langle \gamma_i \rangle_{i=1}^{n_\mu}, \ \gamma_i = \left| \cup_{j=1}^{3} \{ \mu_k \mid \forall k : \omega_{i,j} > \omega_{k,j} \} \right|, \tag{2.30}$$

где γ_i — ранг особи, определяющийся как количество особей популяции, которым соответствуют меньшие значения всех параметров доступности информации, и равный наибольшему индексу особи μ_i в массивах:

$$\begin{cases} \Gamma_1 = \langle \mu_i \mid \forall i > j : \overline{t_d}(\mu_i) \geq \overline{t_d}(\mu_j) \rangle_{i=1}^{n} \\ \Gamma_2 = \left\langle \mu_i \mid \forall i > j : \sigma\left(\delta t_p(\mu_i)\right) \geq \sigma\left(\delta t_p(\mu_j)\right) \right\rangle_{i=1}^{n} \\ \Gamma_3 = \langle \mu_i \mid \forall i > j : q(\mu_i) \geq q(\mu_j) \rangle_{i=1}^{n} \end{cases}. \tag{2.31}$$

Критерием оптимальности решения функции приспособленности $fit(\mu_i)$ для особи $\mu_i \in \mu$ является ее ранг:

$$fit(\mu_i) = \gamma_i \, . \tag{2.32}$$

Механизм селекции. Для выделения особей, переходящих в следующее поколение в процессе выполнения генетического алгоритма, использует-

ся механизм элитного отбора, заключающийся в построении популяции следующего поколения из лучших особей текущего. Быстрая сходимость, обеспечиваемая элитным отбором [55], скомпенсирована применением аутбридинга в процессе выбора родительских пар особей для скрещивания, а также механизмом скрещивания, повышающим вероятность мутации для особей-потомков схожих родительских особей.

Механизм скрещивания. Механизм скрещивания выполнен комбинацией инбридинга (наименьшие различия генотипов особей с целью сохранения наиболее удачных особей) и аутбридинга (наибольшие различия генотипов для увеличения разнообразия и избегания преждевременной сходимости) [55]. Мерой различия особей является расстояние Хэмминга между бинарными строками, представляющими генотипы особей.

Для скрещивания применена процедура двухточечного кроссинговера хромосом родительских особей путем случайного выбора двух точек разрыва r_1 и r_2 родительских хромосом, генотип дочерних особей определяется следующим образом:

$$\chi_c = \langle \chi_{c,i} \rangle_{i=1}^{n}, \text{где } \chi_{c,i} = \begin{cases} \chi_{p1,i}, & \text{если } i < r_1 \text{ или } i > r_2 \\ \chi_{p2,i}, & \text{если } r_1 \leq i \leq r_2 \end{cases}, \qquad (2.33)$$

где χ_c, χ_{p1}, χ_{p2} — генотипы соответственно дочерней особи и ее родительских особей.

Достоинством двухточечного кроссинговера является возможность передачи дочерней особи оптимальных сочетаний генов, находящихся в средней части хромосомы родительской особи, без отбора неоптимальных сочетаний генов на ее концах.

Механизм мутации. Механизм мутации предназначен для исключения преждевременной сходимости популяции к локальным экстремумам за счет увеличения вероятности мутации для особей, имеющих слабо отличающихся родителей. Предложен метод сальтации, заключающийся в выборе 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 произво-

дится замена значений бит генотипа на противоположные. В результате формируется измененный генотип $\dot{\chi}$:

$$\dot{\chi} = \langle \dot{\chi}_\imath \rangle_{i=1}^{n} \ : \ \dot{\chi}_\imath = \begin{cases} \chi_i \, , & \text{если } i \notin \{j_0 j_1\} \\ \chi_i \oplus 1 \, , & \text{если } i \in \{j_0 j_1\} \end{cases}. \qquad (2.34)$$

Мутация выполняется лишь для особей, сгенерированных на текущем шаге работы генетического алгоритма, причем вероятность мутации p_{mut} определяется в соответствии с расстоянием Хэмминга между ее родительскими особями:

$$p_{mut} = 1 - \frac{D(\dot{\chi}_{\text{p0}}, \dot{\chi}_{\text{p1}})}{|\dot{\chi}_{\text{p0}}|} \, , \qquad (2.35)$$

где $\dot{\chi}_{\text{p0}}$, $\dot{\chi}_{\text{p1}}$ — бинарные строки генотипов родительских особей.

Численность популяции. Одним из важных параметров генетического алгоритма, влияющих на его быстродействие, является численность популяции. Предлагается отказ от фиксированных значений и подбор оптимальных значений непосредственно в процессе выполнения генетического алгоритма на каждом из циклов эволюции [60-61].

Применяются стратегия элитного отбора, которая подразумевает перенос особей из предыдущего поколения популяции в следующее, и адаптивный алгоритм, подразумевающий изменение размера популяции на основе анализа динамики изменения максимальных и средних значений параметров доступности информации, соответствующих особям популяции генетического алгоритма. Проводится анализ вектора максимальных значений $\widehat{\omega}$ и вектора средних значений $\overline{\omega}$ с целью принятия решения об увеличении или сокращении численности популяции. Если ни один из элементов вектора максимальных значений не увеличил в течение шага работы алгоритма своего значения, то для увеличения скорости поиска новых решений, не являющихся комбинацией существующих, производится увеличение. В то же время, если ни один из элементов вектора средних значений не увеличил своего значения, то для увеличения быстродействия алгоритма численность уменьшается.

Условием завершения генетического алгоритма является окончание введенного при запуске временного интервала работы [62].

В рамках генетического алгоритма (рисунок 2.15) использованы следующие функции и процедуры:

– RandomM — процедура инициализации с помощью генератора случайных чисел особи генетического алгоритма — вектора μ_i, которому взаимно однозначно соответствует бинарное представление χ_i;

– D — функция расстояния Хэмминга между представлениями χ_i особей;

– Crossover — процедура скрещивания особей путем двухточечного кроссинговера со случайным выбором границ областей обмена битами соответствующих бинарных представлений;

– Mutation — процедура мутации особи методом сальтации ее бинарного представления с вероятностью, определяемой отношением расстояния Хэмминга между ее родительскими особями и длиной бинарного представления, обеспечивающая защиту от преждевременной сходимости популяции.

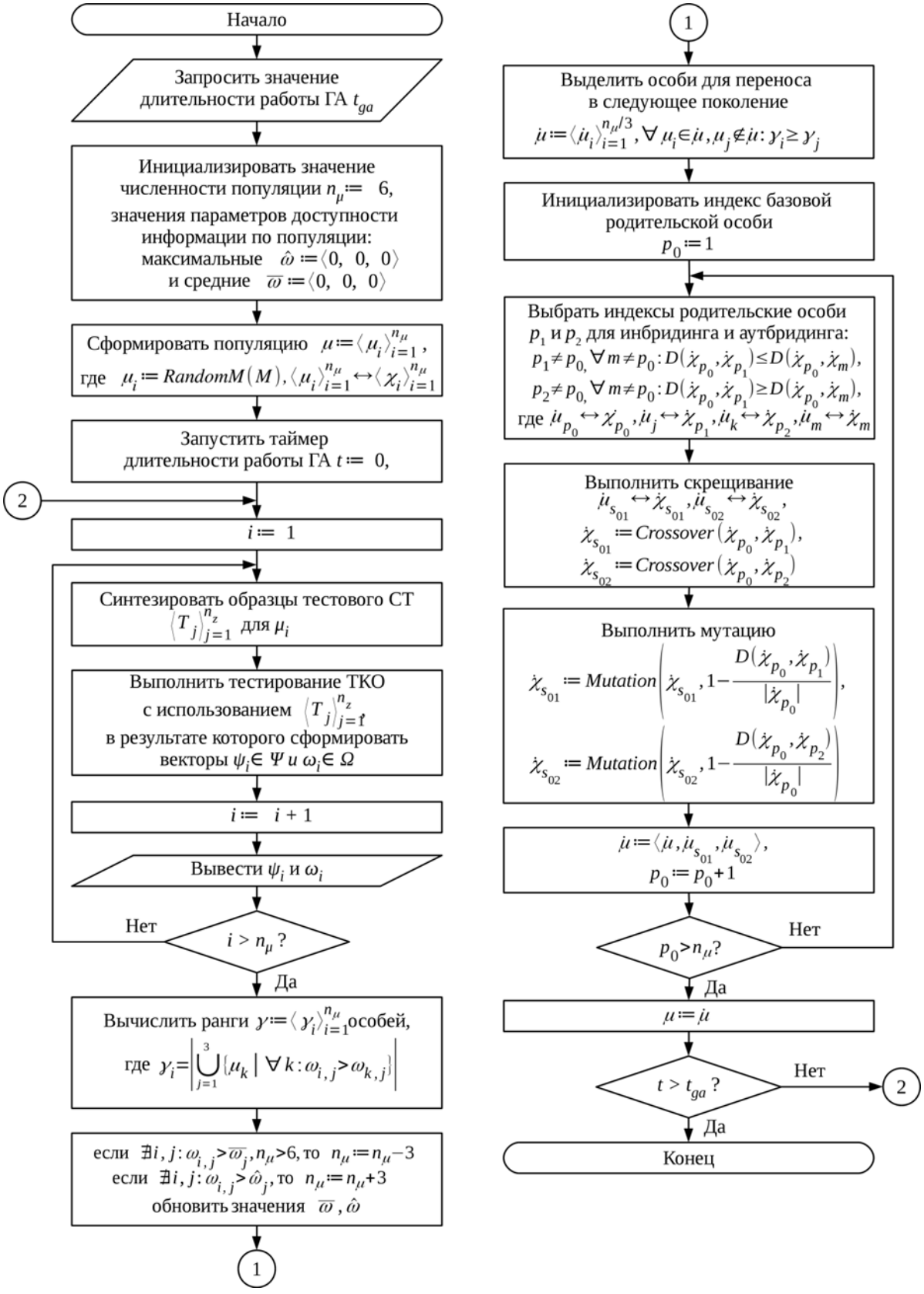

Рисунок 2.15. Схема генетического алгоритма

2.4. *Имитационно-статистический метод синтеза массивов условно-реальных данных о взаимодействии пользователей ИТС*

2.4.1. Пространственно-временная статистико-событийная модель взаимодействия пользователей ИТС

С целью синтеза массивов условно реальных данных о взаимодействии пользователей ИТС с учетом статистических, социальных, геопространственных и временных аспектов разработана пространственно-временная статистико-событийная модель взаимодействия пользователей ИТС [265, 267, 260, 286]. В состав модели входят модель перемещений *MSH*, модель соединений *MS* и модель взаимодействия в социальных сетях *MI* (рисунок 2.17).

Модель перемещений *MSH* описывает движение абонентов сетей сотовой связи относительно базовых станций, на которых осуществляется регистрация абонентских терминалов. Координаты базовых станций задаются параметрами LAC и CellID (см. п. 1.2.6.2) в рамках имитируемого населенного пункта, который представляется квадратом, состоящим из массива клеток (рисунок 2.16), в каждом из которых представлены одна или несколько базовых станций.

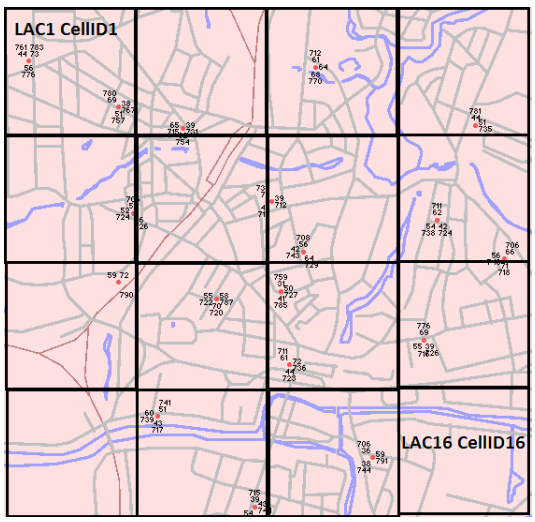

Рисунок 2.16. Имитация населенного пункта в терминах базовых станций операторов сотовой связи

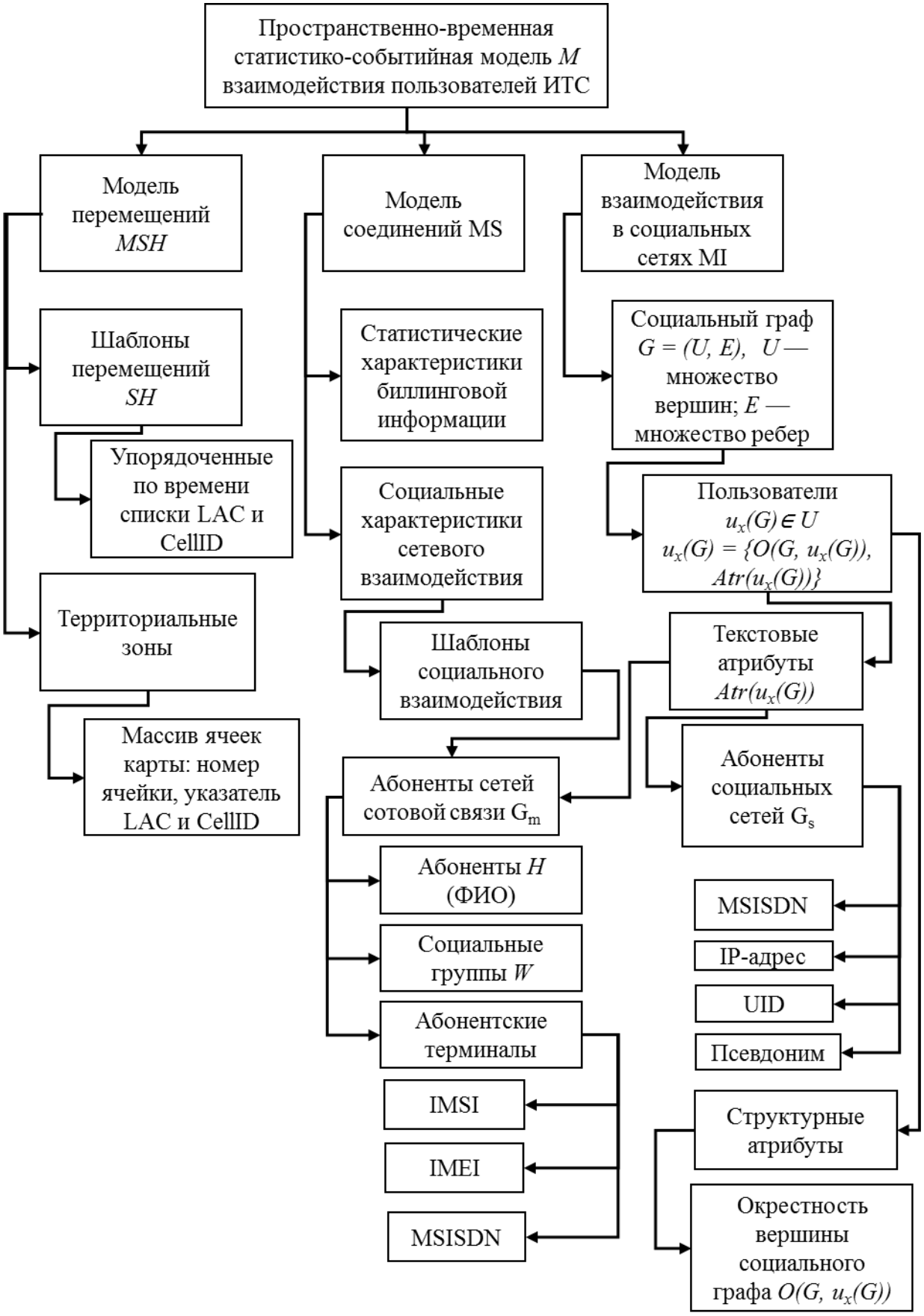

Рисунок 2.17. Схема компонентов пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС

В рамках модели для описания перемещений при создании ситуационной задачи создаются шаблоны, содержащие упорядоченные по времени позиции, характеризующиеся положением базовых станций (LAC и CellID), позволяющие поставить в соответствие абонентам временные метки их пребывания в различных территориальных зонах. Статистические и социальные характеристики сетевого взаимодействия описываются моделью соединений *MS*, основанной на шаблонах социального взаимодействия абонентов *H* ИТС в рамках социальных групп *W* и абонентской базы, объединяющей имитируемые персональные данные абонентов и сведения об абонентских терминалах.

Для описания взаимодействия абонентов в социальных сетях предложена модель *MI*, где совокупность абонентов ИТС представлена социальными графами[1]. Абонент *x* в моделируемой ИТС, описываемой с помощью социального графа *G*, обозначается $u_x(G) \in U$. Для описания вершины графа $u_x(G)$ используются атрибутивные компоненты (атрибуты) учетных записей объекта в ИТС, которые можно разделить на две категории: текстовые и структурные.

Набор текстовых атрибутов представляет собой вектор параметров $Atr(u_x(G))$, описывающих его различные характеристики. Структурные атрибуты, представляющие систему взаимоотношений между пользователями ИТС, описываются как окрестность[2] $O(G, u_x(G))$ вершины социального графа. Рассмотренные параметры позволяют описать пользователя ИТС: $u_x(G) = \{O(G, u_x(G)), Atr(u_x(G))\}$. Основными текстовыми атрибутами учетной записи u_x пользователя в сети сотовой связи (граф G_M) являются: $IMSI(u_x(G_M))$ — номер SIM-карты, $IMEI(u_x(G_M))$ — IMEI (номер аппарата), $MSISDN(u_x(G_M))$ — MSISDN (номер телефона), $surname(u_x(G_M))$, $name(u_x(G_M))$, $secname(u_x(G_M))$ — фамилия, имя и отчество пользователя. 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),

[1] ***Социальный граф*** — граф $G = (U, E)$, узлами U которого являются социальные объекты (пользователи, абоненты), а ребрами E — социальные связи между ними.

[2] ***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.

IP($u_y(G_S)$) — IP-адрес, *UID($u_y(G_S)$)* — идентификатор пользователя, *nickname($u_y(G_S)$)* — его текстовый псевдоним.

Процесс синтеза массивов биллинговой информации заключается в последовательном формировании записей *D* в формате CDR, каждая запись соответствует событию сетевого взаимодействия, среди которых выделяются события регистрации абонентских терминалов на базовых станциях *T*, голосовые сообщения *C*, СМС-сообщения *S* и события *G* Интернет-соединений (GPRS-трафика) (рисунок 2.18).

При формировании массива соединений *Y*, объединяющего массивы звонков и СМС-сообщений, учитываются статистические характеристики биллинговой информации:

– $K_0 = \langle F_{time}, F_{dur}, F_n, F_a \rangle$ — не связанные с адресацией соединения, описываемые функциями распределения: 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 — функция распределения выбора получателей соединения, а F_t — функция распределения 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 $\langle Y_i \rangle_{i=1}^{n_Y}$ и описывается выражением:

$$Y_i = \langle A, h_1, h_2, K_0, K_1 \rangle. \quad (2.36)$$

Модель соединений *MS* определяется выражением:

$$MS = \langle H, W, \langle Y_i \rangle_{i=1}^{n_Y} \rangle. \quad (2.37)$$

В модели взаимодействия пользователей в социальных сетях *MI* учитываются множества абонентов оператора сотовой связи *H* и социальных групп *W*, а также массив взаимодействия в социальных сетях *YI*, являющийся совокупностью информационных сообщений трех типов: публичное сообщение, публичное направленное сообщение и приватное сообщение,

содержащее информацию исключительно для одного получателя.

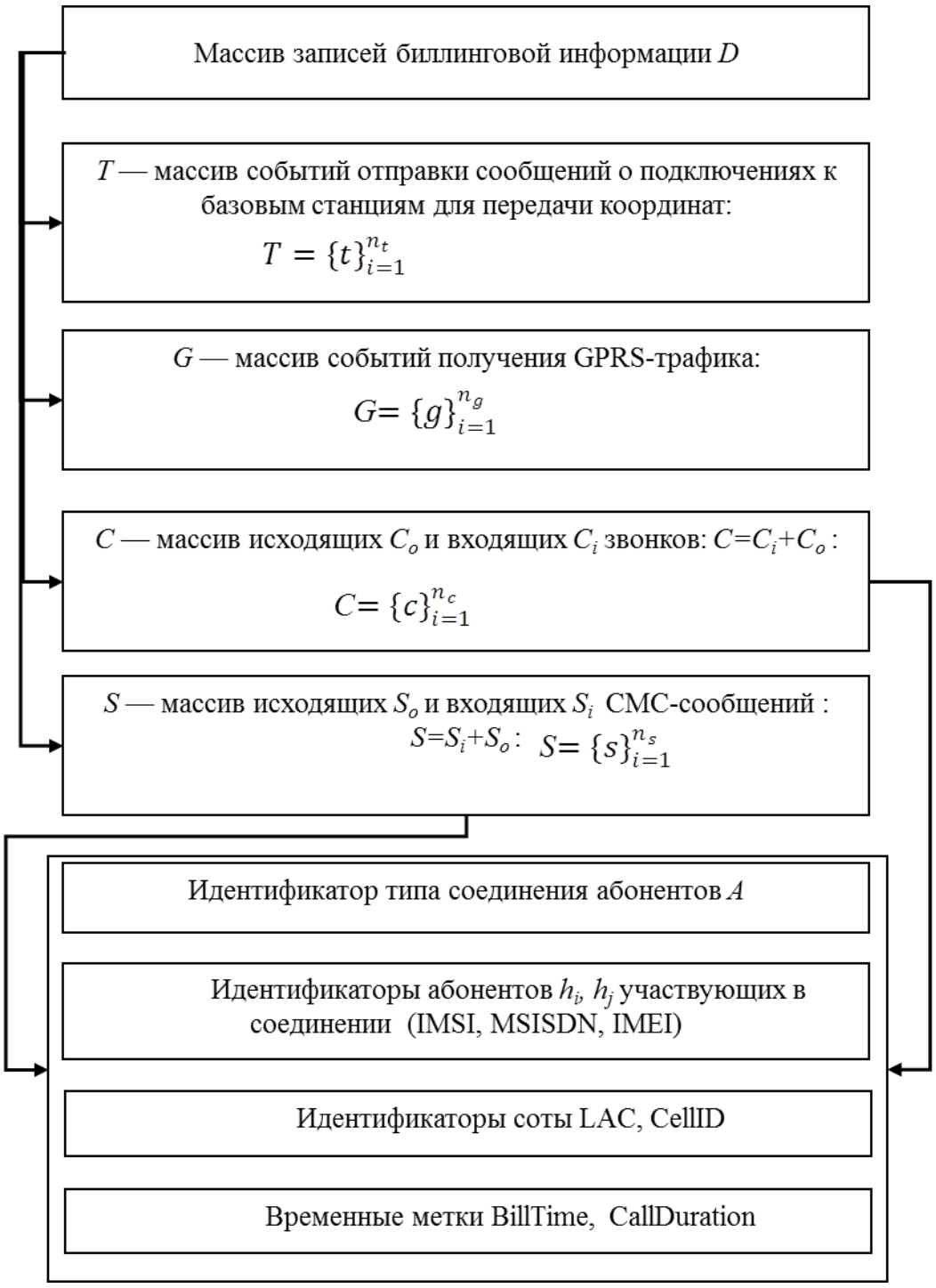

Рисунок 2.18. Схема синтеза массивов биллинговой информации (n_t — количество перемещений, n_g — подключений, n_c, n_{co} и n_{ci} — звонков, n_s, n_{si} и n_{so} — сообщений)

С учетом перемещений абонентов по заданным шаблонам пространственно-временная статистико-событийная модель M взаимодействия абонентов ИТС описывается выражением:

$$M = \langle MS, MSH, MI \rangle. \quad (2.38)$$

В ИАСБ в процессе анализа сетевого взаимодействия пользователей загружаются, в том числе данные, поступающие от операторов сотовой связи как в формате CDR, так и в иных табличных либо граф-ориентированных форматах. Основными источниками данных являются службы сотовой связи и службы социальных сетей (рисунок 2.19).

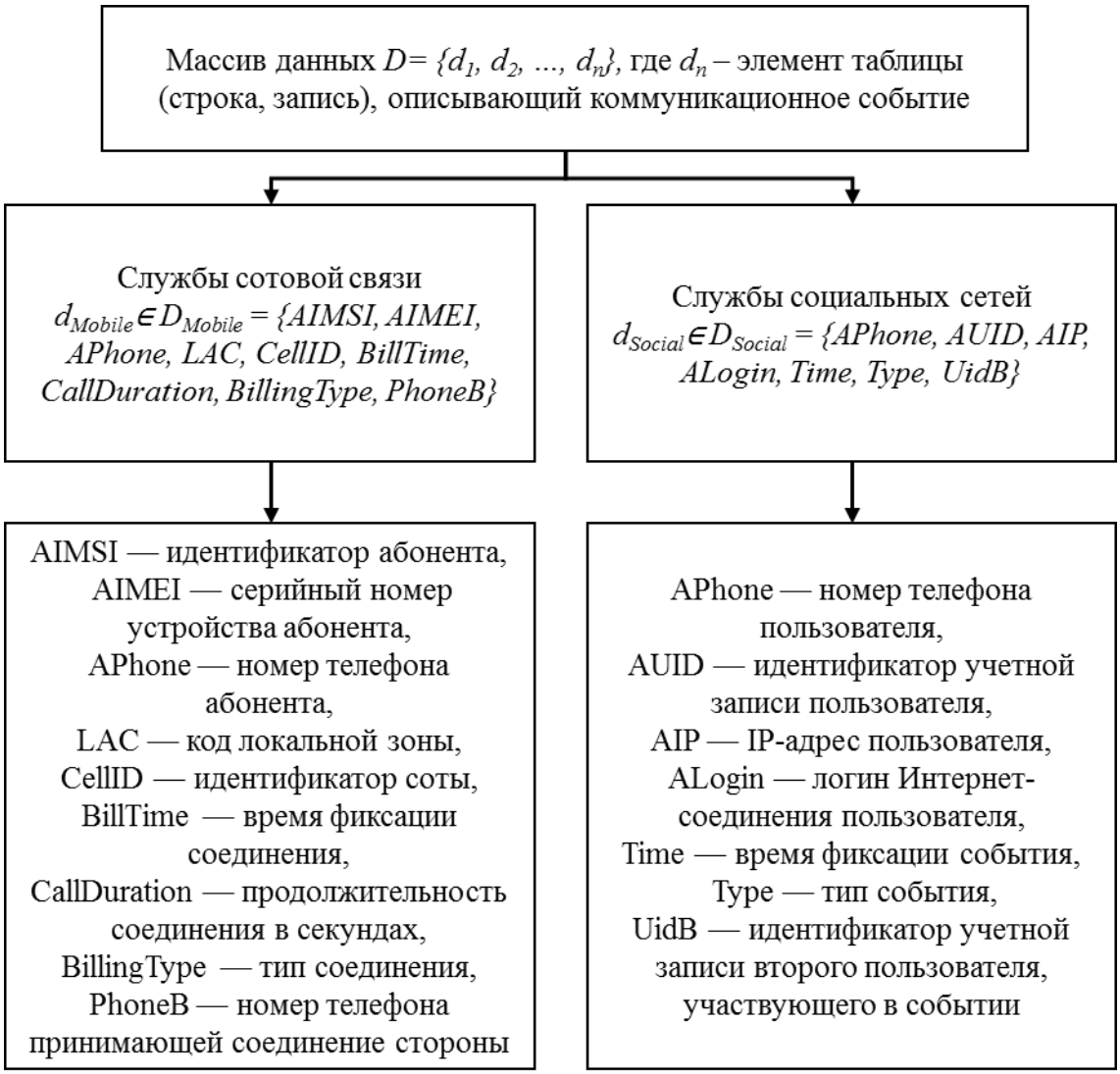

Рисунок 2.19. Структура массивов данных, описывающих коммуникационные события

Для тестирования аналитических алгоритмов и методик в структуре массива данных должны быть представлены фоновые и ситуационные компоненты: $D = D_{task} \cup D_{feed}$,,где D_{task} – ситуационные задачи и D_{feed} – фоновые события (рисунок 2.20).

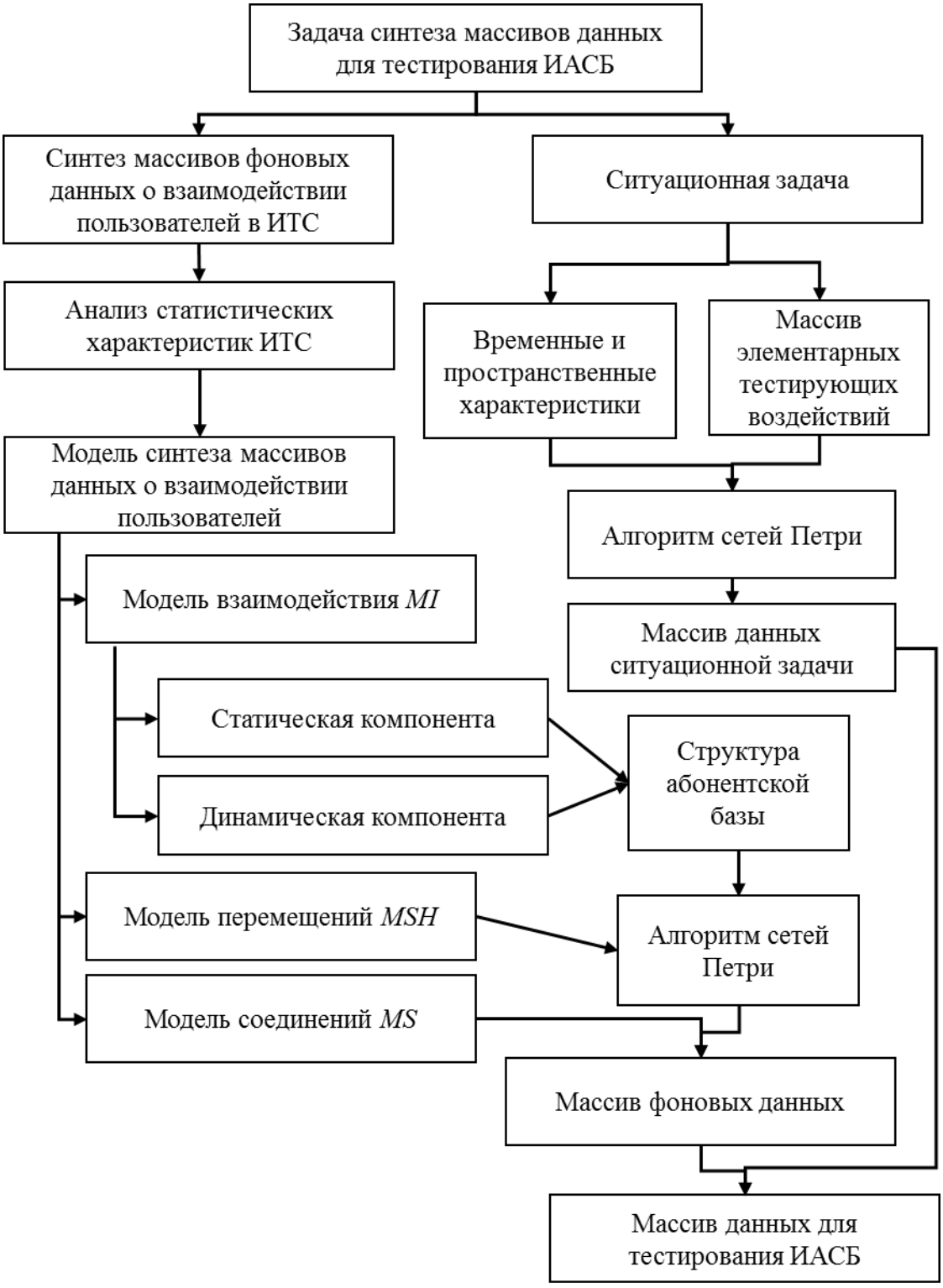

Рисунок 2.20. Схема синтеза массивов данных для тестирования ИАСБ

Ситуационная задача предназначена для анализа корректности выявления взаимодействия пользователей, описывается шаблоном взаимодействия пользователей G_t. Ситуационная задача — это задаваемое оператором множество взаимодействий между абонентами, определяемое характерными

признаками. Фоновый массив биллинговой информации — это множество записей о совершенных событиях, описывающее поведение большого количества абонентов, не задействованных в ситуационной задаче. Синтезируемый фоновый массив должен повторять реальный по статистическим характеристикам, к которым относятся:

– распределения длительности событий;

– распределения количества событий по дням недели и отдельно по каждому часу внутри каждого дня;

– распределения типов событий в общем массиве событий, совершенных за день и отдельно за каждый час этого дня.

Массив фоновых данных имитирует социальную активность в целом и содержит события пользователей, подчиняющиеся статистическим законам реальных сетевых сервисов.

Для формирования различных полей записей d_{Mobile} и d_{Social} в рамках пространственно-временной статистико-событийной модели M взаимодействия абонентов ИТС используются статистические распределения следующих групп параметров:

— событийные (поля *BillingType*, *Type*);

— социальные (поля *PhoneB*, *UIDB*);

— пространственные (поля *LAC, CellID*);

— временные (поля *Time*, *CallDuration*).

2.4.2. Имитационно-статистический метод синтеза массивов условно-реальных данных на основе модели взаимодействия пользователей ИТС с применением аппарата сетей Петри

Метод синтеза массивов условно-реальных данных о взаимодействии пользователей ИТС (опубликован в [261, 259, 260]) основан на предложенной пространственно-временной статистико-событийной модели взаимодействия пользователей ИТС и представлен последовательными этапами формирования статических и динамических компонентов с использованием различных математических подходов, имитирующими различные параметры про-

цесса взаимодействия пользователей на основе статистических распределений требуемых показателей в реальных ИТ-сервисах, и принципов моделирования сложных сетей (рисунок 2.21).

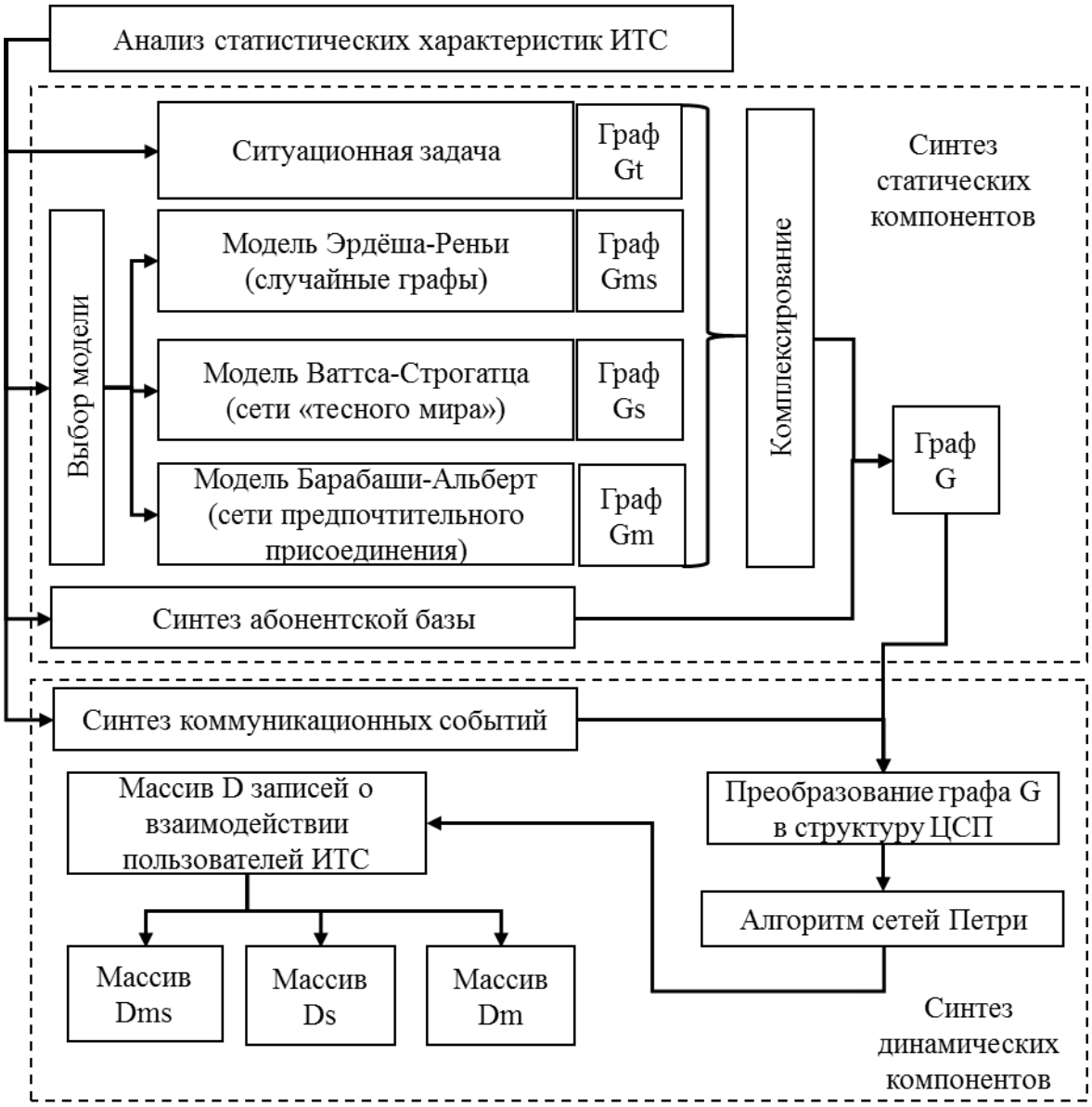

Рисунок 2.21. Схема синтеза статических и динамических компонентов массивов условно-реальных данных о взаимодействии пользователей ИТС

Основными являются этапы формирования статических и динамических компонентов коммуникационных событий:

1. Формирование статических компонентов записей d_{Mobile} и d_{Social}, к которым относятся персональные идентификаторы пользователей (*AIMSI*,

AIMEI, APhone, AUID, AIP, ALogin) и структура их взаимосвязей внутри ИТС (в том числе информация о социальных группах).

2. Генерация динамических компонентов коммуникационного события (тип, участники, место, время начала и продолжительность) на основе существующих социальных связей пользователей.

Процесс формирования статических компонентов основывается на композиции известных моделей сложных сетей, выбор которых осуществляется по результатам анализа статистических характеристик, полученных в результате анализа сетей операторов сотовой связи и социальных сетей.

Процесс формирования статической структуры графа G_M начинается с генерации регулярной решетки со степенью вершин K. Затем происходит выбор случайным образом соседних вершин с распределением значений вершин и ребер (модель Барабаши-Альберт).

Процесс формирования статической структуры социального графа G_S происходит в соответствии с моделью Эрдёша-Реньи (п. 1.6.1), начинается с генерации случайного графа G_{MS}, структурного ядра графа G_S , затем в граф последовательно добавляются вершины в соответствии с моделью Ваттса-Строгатца.

После создания статической структуры осуществляется процесс формирования динамических компонентов массивов условно-реальных данных, основанный на применении алгоритмов цветных сетей Петри (ЦСП).

В качестве вершин и переходов ($p_k \in P$, $t_k \in T$) сети Петри используются вершины и дуги созданных графов G_M, G_S и G_t. В целях моделирования коммуникационных событий различных типов (подключение к базовым станциям, GPRS-трафик, исходящие и входящие звонки и СМС-сообщения, публичные и приватные сообщения) и учета дополнительных параметров (например, время и продолжительность коммуникационного события) введена раскраска меток сети в различные цвета (рисунок 2.22).

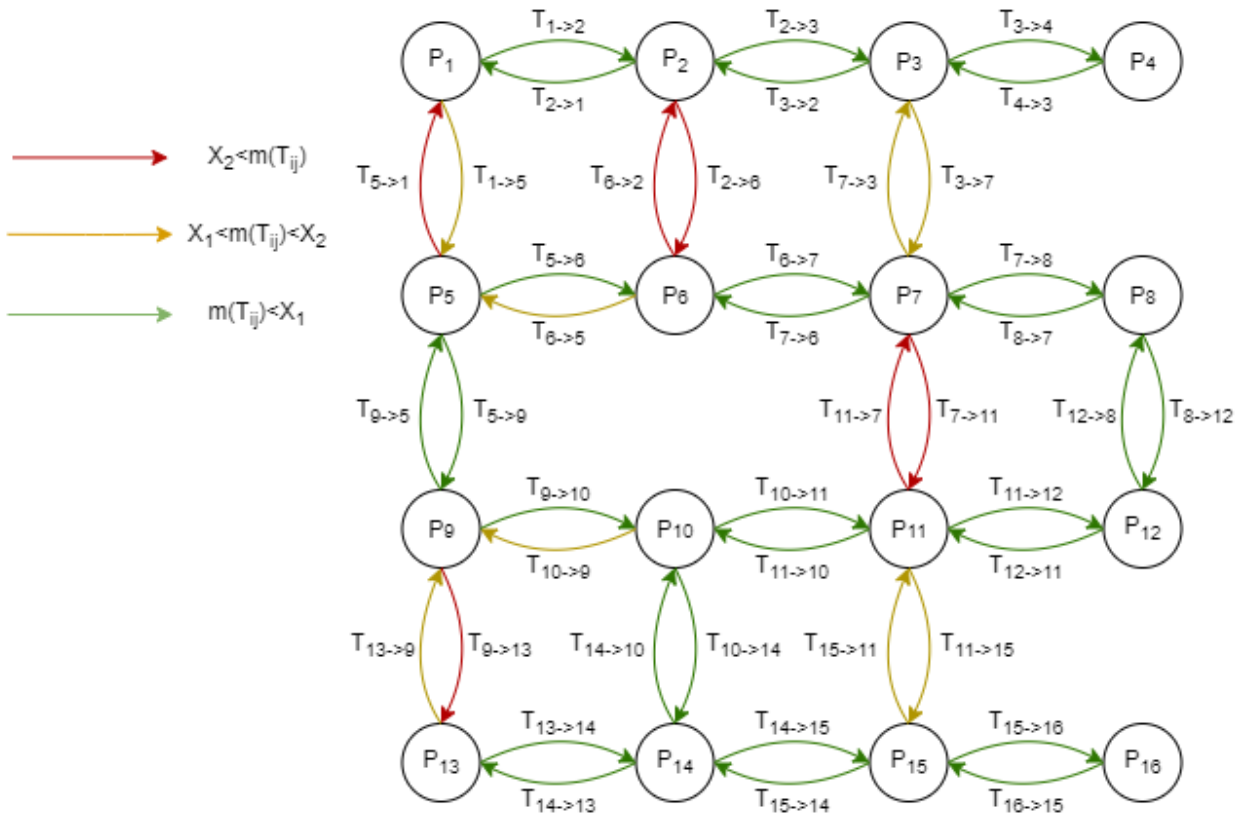

Рисунок 2.22. Пример сети Петри, используемой в модели перемещений *MSH*

Результатом выполнения всех циклов процессов формирования статических и динамических компонентов являются синтезированные массивы D_{Mobile} и D_{Social} требуемого формата. Соединения абонентов генерируются на основе абонентской базы.

База абонентов (база принадлежности) сетей операторов сотовой связи представляет собой совокупность персональных данных абонентов и номеров соответствующих им абонентских терминалов. База абонентов формируется на основании списков фамилий, мужских и женских имен (на русском языке) в порядке уменьшения частоты их появления. Описание каждого абонента хранится в отдельной строке. Каждый абонент имеет уникальный номер, социальную группу и социальную роль (которые определяют интенсивность коммуникационных событий абонента), номер оператора связи, которому он принадлежит, уникальные значения IMSI, IMEI и MSISDN. Для каждого пользователя происходит генерация уникального идентификатора участника социальной сети UID (рисунок 2.23).

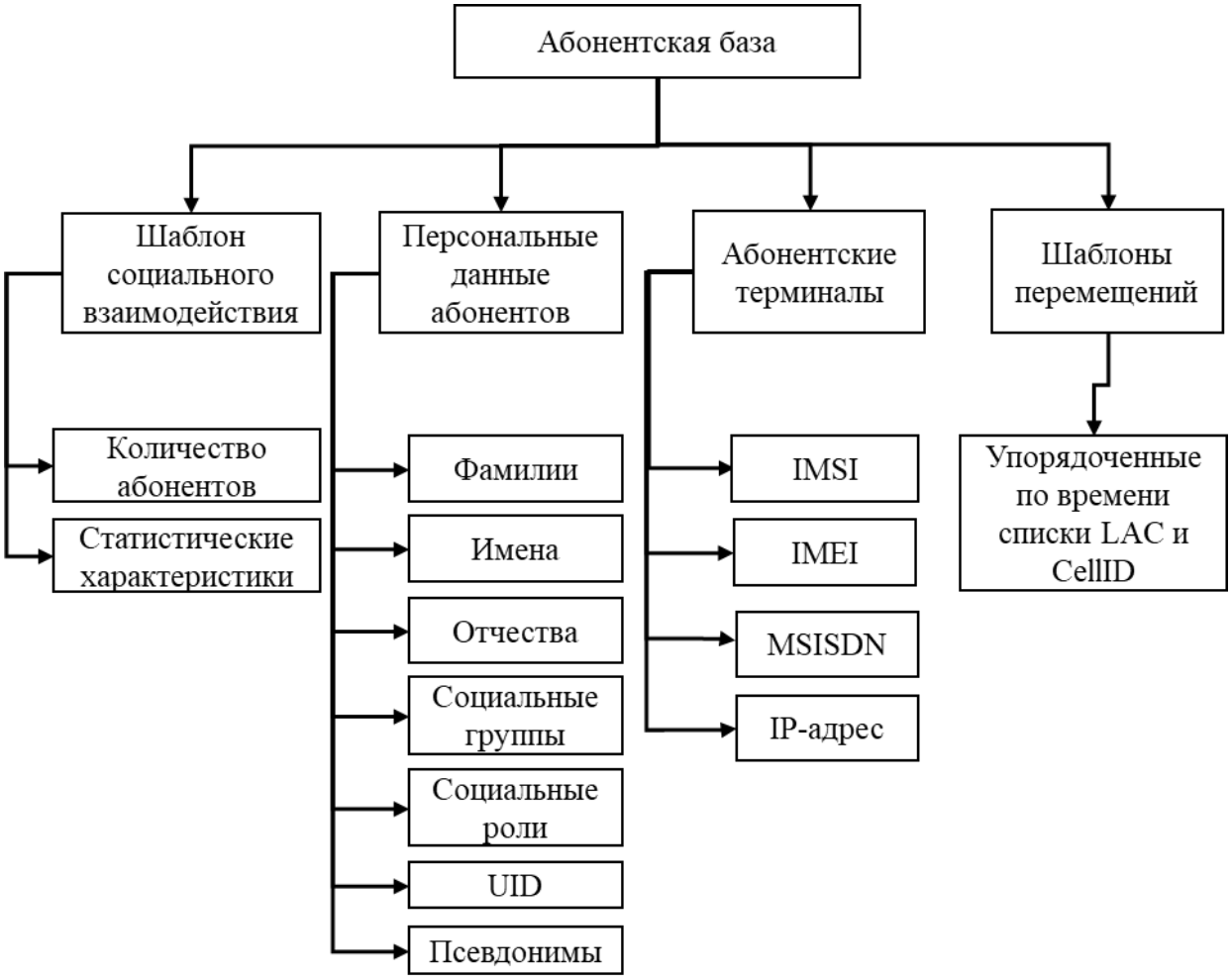

Рисунок 2.23. Схема компонентов абонентской базы

При синтезе соединений абонентов сетей операторов сотовой связи отдельно формируются массивы соединений, соответствующие ситуационной задач, и массивы фоновых данных. При этом используются абонентская база, файлы, описывающие базовые станции выбранной местности, статистические распределения видов событий по времени и продолжительности, заранее сгенерированный массив ситуационных задач.

При синтезе фоновых массивов поочередно для каждого из абонентов с учетом назначенных шаблонов перемещения и шаблонов социального взаимодействия происходит генерация событий — записей в массиве биллинга. Для каждого типа коммуникационного события используются статистические характеристики, определяющие количественные и временные параметры (рисунок 2.24).

Рисунок 2.24. Схема процедуры синтеза записей коммуникационных событий

Формируются исходящие коммуникационные события для каждого коммутатора отдельно в виде отдельных строк в массиве записей.

После создания исходящего события формируется соответствующее ему входящее событие для выбранного абонента-получателя на той базовой станции, на которой в момент события зарегистрирован получатель в соответствии с шаблоном перемещений.

После синтеза массива фоновых данных происходит интеграция массивов исходящих событий, входящих событий, событий регистрации с массивом данных ситуационной задачи, сортировка объединенного массива по времени и разделение массивов в отдельные файлы, описывающие коммутационные события на каждом отдельном коммутаторе, принадлежащем соответствующему оператору сетей сотовой связи (рисунок 2.25).

Рисунок 2.25. Схема синтеза массивов данных биллинговой, распределенных по коммутаторам операторов сетей сотовой связи

В процессе сортировки создается дополнительный массив структур, состоящий из двух полей: номера события в исходном массиве и времени совершения события, которые сортируется по увеличению времени совершения события методом выбора.

2.4.3. Алгоритм построения оптимального неповторяющегося маршрута абонентов при синтезе массивов данных биллинговой информации в терминах модифицированных стохастических сетей Петри

Модель перемещений *MSH* имитирует перемещения абонентов заданном временном интервале в рамках населенного пункта. Для создания траекторий перемещений абонентов предлагается применение алгоритмов сетей Петри. В терминах сетей Петри точки геопозиции имитируемого населенного пункта представлены множеством узлов P: $P = \{p_i\}_{i=1}^{n_p}$, и переходов $T = \left\{\{t_i\}_{j=1}^{n_{ti}}\right\}_{i=1}^{n_p}$ (где n_p — количество узлов, n_{ti} — переходов на узле p_i, t_{ij} — переход от узла $p_{i.}$ к узлу $p_{i.}$). Возможность перемещения абонента из одного из одного узла в другой определяется наличием между узлами связывающих переходов (путей). Каждый переход t_{ij} обладает весом $m(t_{ij})$, имеющим смысл количества абонентов, перемещенных по нему на предыдущем шаге. Решение о выборе способа перемещения принимается в два этапа (рисунок 2.26).

На первом этапе производится выбор принципиально реализуемых способов перемещения от точки p_i к точке p_{i+1} с учетом необходимых временных параметров пребывания абонента в конкретной точке карты (узле графа). Эти знания могут быть получены путем анализа состояния графа топологии шаблонов перемещений T с учетом их загруженности (веса перехода). На втором этапе из общего массива возможных способов перемещения от точки p_i к точке p_{i+1} выбирается предпочтительный, минимизируя общее время перемещения (максимизируя время нахождения в точке, соответствующее величине $|t_{i2}-t_{i1}|$). Для этого каждый возможный исход перемещения оценивается перемещающимся с позиции достижения конечной цели (промежуточного пункта p_i).

Рисунок 2.26. Схема создания динамической модели перемещения абонентов в терминах сетей Петри

Ограничением является то, что перемещающийся может просчитывать ситуацию только на два шага вперед (вероятность загруженности пути на длительное время в общем случае не всегда возможно предсказать). Следовательно, перемещающийся, находящийся на узле p_i, может рассматривать в качестве возможных вариантов первого шага узлы, непосредственно связанные с узлом p_i, а в качестве перспективного направления движения — узлы, непосредственно связанные с соседними для p_i узлами. Следует заметить, что после выполнения первого шага переход «по плану» к следующему мо-

жет оказаться невозможным (на нем может отсутствовать фишка) или нерациональным (вследствие того, что другие абоненты во время выполнения первого шага описываемого абонента прошли именно через этот переход).

Узлы сети p_i моделируют квадраты карты населенного пункта. Длина каждой стороны карты — k квадратов, всего на карте квадратов k^2, $n_p = k^2$. Каждый из внутренних квадратов (не являющийся частью внешней стороны) имеет 4 перехода на соседние. Каждый переход — однонаправленный (условие сети Петри), поэтому всего для таких квадратов имеется $4(k-1)^2$ переходов. У каждого внешнего квадрата, кроме 4 угловых, имеются по 3 перехода на остальные (у угловых — по два). Поэтому всего у внешних квадратов $12(k-2)+8 = 12k-4$ перехода.

Каждый переход моделирует путь. В случае если вес перехода меньше заданного критического, то путь доступен. При выборе перехода для дальнейшего движения также учитывается его вес. Если вес больше критического, то фишка на переходе отсутствует, и пройти по нему нельзя, пока фишка не появится (путь загружен). При этом гарантируется, что, если изначально фишка на переходе была (т.е. критический вес был больше 0), то через шаг после исчезновения фишки с перехода она снова там появится: если переход закрылся, значит, по нему не будет движения, и его вес за этот шаг увеличиваться не будет. Шаг пройдет, количество перешедших по переходу абонентов будет равно 0, значит, и вес перехода также станет равным 0, что всегда меньше заданного критического веса, поэтому переход откроется.

При задании исходного шаблона перемещений необходимо указать три узла, через которые должен «пройти» абонент. Первый узел становится начальным, второй — серединным, третий — конечным. Узлы могут совпадать. Чтобы обеспечить меньшую повторяемость перемещений при использовании небольшого количества шаблонов эти три узла варьируются в определенном интервале: любой или несколько узлов могут быть заменены теми, на которые у них имеются переходы (независимо от того, разрешены они или запрещены).

Кроме того, должны быть заданы максимальное время прибытия на узел и минимальное время убытия с узла. Прибывать на точку раньше допускается, позже — нет. Убывать с точки позже также допускается, раньше — нет. Если по каким-то причинам прибыть на точку возможно только позже указанного времени, то до этого времени абонент двигается по направлению к заданной точке, по прошествии этого времени — в сторону следующей заданной точки, пропустив ту, на которую он «не успел». Аналогично выбору узлов, сроки прибытия и убытия варьируются в заданном интервале, что уменьшает повторяемость перемещений. Если абонент попал на узел вовремя, он остается на нем (не совершает переходов) до указанного минимального времени убытия.

На первом шаге алгоритма определяется требуемое направление движения путем построения вектора, соединяющего узел p_i с целевым узлом $p_ц$, (один из трех заданных узлов). По полученному вектору определяется требуемое направление движения. После определения требуемого направления движения выбираются три предпочтительных для перемещения узла в порядке возрастания вероятности перехода, при этом значение приоритета первого увеличивается на 1, второго — на 2, третьего — на 3 (чем ближе узел к вектору, соединяющему i-ый узел с целевым, тем больше вероятность перемещения в него при прочих равных условиях). После выбора трех предпочтительных для перемещения узлов сравниваются их веса. Переходы сортируются в порядке уменьшения веса.

После этого выбирается переход с наибольшим приоритетом, и осуществляется переход по нему. Если переход невозможен, то выбирается переход со средним приоритетом, если и он невозможен — то выбирается третий переход (с наименьшим приоритетом). В случае возникновения ситуации, в которой переход невозможен ни по одному из указанных переходов, абонент остается на месте (переход не осуществляется).

При выборе очередного (l-го) перехода учитываются номер i узла p_i, на котором сейчас находится абонент, наличие фишек на переходах, соеди-

няющих p_i с соседними узлами и вес этих переходов. Перед выбором шага значения приоритета для каждого из возможных переходов обнуляются.

Далее для каждого из абонентов выполняются действия по указанному алгоритму.

Информация о местоположении абонентов за весь период времени, используемая в дальнейшем при синтезе биллинговой информации, хранится в виде трехмерной матрицы, в ячейках которой может быть от 0 до n_h (по количеству абонентов) нолей или единиц. Единица означает, что абонент там присутствует, ноль — что абонента там нет. Два измерения из трех являются координатами квадрата карты (узла сети Петри) по «широте» и «долготе», третье — время. В каждой плоскости матрицы хранится информация о положении абонентов в определенный момент времени. В каждой ячейке присутствует информация об абонентах, находившихся там в выбранный момент времени.

Для хранения весов переходов используется двумерная квадратная матрица размерности *2*k,* где k — размерность матрицы, описывающей карту. Матрица хранения весов делится, начиная с верхнего левого угла, на квадратные подматрицы размерности 2. В каждом из 4 элементов такой подматрицы хранится информация о весе перехода с соответствующей стороны. В случае, если с описываемой элементом матрицы стороны нет перехода (элемент внешний), туда записывается значение 0. Тогда, при сбросе всех весов переходов после шага, это значение будет сохраняться.

2.5. *Выводы по главе 2*

Глава 2 описывает разработанный научно-методический инструментарий имитационного моделирования при синтезе интерактивной сетевой среды для компьютерных полигонов, впервые представленный 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.

В ней раскрываются основные элементы комплексного метода синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности метода на примере модели сетевой среды функционирования в задаче тестирования ССЗИ. Модель сетевой среды функционирования основывается на свойствах ССЗИ, подлежащих тестированию. Тестовые массивы состоят из массивов фоновых данных и массивов атакующего воздействия. Подробно описаны алгоритмы синтеза массивов фоновых данных для тестирования СОА, ТКО и ИАСБ. Алгоритмы имеют схожую структуру и состоят из следующих шагов:

— определение значений характеристик сетевой среды ССЗИ, запись результатов в виде набора матриц;

— синтез области данных генерируемых массивов;

— синтез потоков пакетов;

— оценка адекватности синтезируемых массивов.

Синтез массивов данных осуществляется на основе ранее сохраненных статистических характеристик реального трафика, для чего используется матричная модель хранения характеристик внешней среды. Предложенный алгоритм определения значений характеристик сетевого трафика и их сохранения в виде матричной модели позволяет в дальнейшем формировать структуру трафика на основе алгебраических выражений для полученных состав-

ляющих сетевого трафика. В рамках расчета векторов характеристик сетевого трафика на основе матричных операторов предложены способы расчета и формирования графов потоков передачи между источниками и получателями, средних значений длин пакетов и интервалов времени между пакетами.

При синтезе тестовых массивов данных учитываются как статистические распределения, так и наполнение области данных, для формирования которого применяются алгоритмы марковских цепей.

Предложен метод синтеза массивов фоновых данных, предназначенных для тестирования ССЗИ, который является совокупностью элементов процесса синтеза массивов фоновых данных, включая синтез фонового сетевого трафика IP-сетей. Разработанная модель сетевой среды функционирования ССЗИ позволяет создавать на ее основе алгоритмы и программный комплекс, решающий задачу синтеза массивов фонового сетевого трафика в соответствии со статистическими характеристиками потоков информации в компьютерных сетях.

Представлен ряд методов и алгоритмов синтеза массивов фоновых данных для тестирования СОА, ТКО и ИАСБ, основанных на преобразовании матриц характеристик трафика. С целью анализа реалистичности тестовых массивов условно-реальных данных предложен метод оценки реалистичности синтезируемых массивов сетевого трафика для тестирования СОА и ТКО, в основе которого лежит анализ свойства самоподобия телетрафика с применением показателя Херста, который выступает показателем «пульсации», сравнение значений показателя Херста для исходного и сгенерированного трафиков.

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. Синтез атакующих (ситуационных) массивов данных осуществляется на основе алгоритмов сетей Петри, где ситуационные задачи (атаки) представляют собой формируемую по определенным пра-

вилам последовательность элементарных событий, распределенных по времени. Для синтеза атакующего воздействия, предназначенного для анализа корректности реализованных алгоритмов в задаче тестирования СОА, предложен аппарат стохастических сетей Петри, в рамках которого дано понятие элементарного атакующего воздействия и комплексной атаки как совокупности элементарных событий. Для тестирования СОА используется модифицированная стохастическая сеть Петри, представляющая обобщенную стохастическую сеть Петри с задержками, сдерживающими дугами и взвешенными переходами. Показана применимость предложенного аппарата для моделирования комплексных компьютерных атак.

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, алгоритмов сетей Петри для синтеза динамической составляющей атакующего воздействия, позволяет формировать сценарии действий нарушителя и генерировать граф атакующего воздействия, используемый в процессе анализа защищенности ИТС и создания ситуационных задач.

Предложены подходы к синтезу тестирующего массива данных атакующего воздействия и способ автоматизации тестирования с применением аппарата генетических алгоритмов. С целью определения границ устойчивости ТКО к атакующему воздействию типа «отказ в обслуживании» предложен метод автоматизации тестирования, основанный на применении эволюционно-генетического подхода. Выполнена формализация параметров генетических алгоритмов в терминах задачи тестирования ТКО. В качестве входных параметров особи используется совокупность параметров модели сетевой среды функционирования ССЗИ, описывающей топологию моделируемой сети и структуру циркулирующего в ней сетевого трафика.

Впервые предложенная пространственно-временная статистико-событийная модель взаимодействия пользователей ИТС позволяет создать на ее основе программный комплекс, решающий задачу синтеза массивов бил-

линговой информации, в котором для построения модели соединений на основе модели перемещений использован алгоритм сетей Петри.

Рассмотрен метод синтеза фонового массива биллинговой информации в задаче тестирования ИАСБ, включающий модель хранения статистических данных для синтеза массива биллинговой информации, процедуру синтеза базы абонентов и алгоритм формирования соединений абонентов сетей операторов сотовой связи. Алгоритм использует абонентскую базу, информацию о базовых станциях, статистические распределения видов событий по времени и продолжительности и шаблоны перемещений абонентов.

Разработан имитационно-статистический метод синтеза массивов условно-реальных данных, основанный на структурно-параметрической модели взаимодействия пользователей с применением аппарата сетей Петри с целью формирования динамики развития коммуникационного взаимодействия абонентов ИТС. Метод состоит в последовательном формировании статических (структурной основы) и динамических компонентов с использованием композиции существующих моделей построения сложных сетей на основе статистических распределений структурных параметров сервисов мобильной связи и социальных сетей, где сервисы социальных сетей рассматриваются в виде социальных графов. Разработанный метод синтеза и анализа атакующего воздействия и ситуационных задач построен на применении стохастических сетей Петри, использует модель формирования атакующего воздействия, основанную на теоретико-графовом подходе, и алгоритм построения оптимального неповторяющегося маршрута абонентов при синтезе массивов данных биллинговой информации.

Аппарат сетей Петри также применяется для построения оптимального неповторяющегося маршрута абонентов при синтезе массивов данных биллинговой информации и для формирования соединений биллинга на основе шаблонов, каждый из которых описывает типовое поведение абонентов с точки зрения совершаемых действий в сети оператора связи.

Также на основе сетей Петри предложен способ формирования графов атак для последующего применения в технологии Honeynet при построении имитаторов уязвимых систем при тестировании САЗ.

Разработанный комплексный метод синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности, основанный на выделении структурных элементов сетевого трафика реальных сетей с учетом функционального предназначения тестируемого ССЗИ, учитывающий вариативность ИТС и динамику развития ситуационных задач, предусматривающий воздействие на тестируемый образец комбинации двух видов трафика: фонового и атакующего, 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.

Таким образом, в главе приведено решение следующих частных задач исследования:

— 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;

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

— разработка моделей и алгоритмов синтеза массивов фоновых данных для тестирования СОА, ТКО и ИАСБ с обоснованием методов анализа реалистичности синтезируемых тестовых массивов.

3. КОМПЛЕКС МОДЕЛЕЙ, МЕТОДИК, АЛГОРИТМОВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УЧЕБНО-ЭКСПЕРИМЕНТАЛЬНЫХ СТЕНДОВ ДЛЯ ТЕСТИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ АТАК И ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

3.1. *Экспериментальный стенд и методика тестирования систем обнаружения атак*

3.1.1. Методика тестирования сетевых систем обнаружения атак

Методика проведения сравнительного тестирования сетевых СОА основана на анализе вероятности обнаружения сетевых атак в зависимости от интенсивности сетевого трафика и доли атакующего воздействия.

В связи с тем, что СОА является подмножеством систем обнаружения в целом, целесообразно для оценивания СОА применять классические критерии качества. При этом учитывать ошибки первого и второго рода: вероятности правильного обнаружения атак и вероятности ложных тревог.

Сравнение СОА в соответствии с наличием или отсутствием у них дополнительных функций, не имеющих отношение к вероятностям правильного обнаружения атак и вероятностям ложных тревог, является второстепенным и нецелесообразным.

Для оценивания сетевых СОА в рамках предложенной методики применяются следующие критерии: качество идентификации компьютерных атак, качество обработки сетевого трафика, оптимальная рабочая характеристика СОА. Указанные критерии учитывают вероятности правильного обнаружения атак и вероятности ложных тревог.

Методика проведения испытаний образцов сетевых СОА, разработанная для применения с использованием стенда тестирования СОА, состоит из пяти этапов.

Этап 1. Анализ качества идентификации компьютерных атак. Цель тестирования по критерию «Качество идентификации компьютерных атак» — выявление широты охвата атак и возможности СОА по обнаружению скры-

тых и модифицированных атак. В результате тестирования оценивается общее количество атак, выполненных в процессе тестирования, и количество обнаруженных правильно идентифицированных атак.

Путем последовательной генерации трафика сетевых атак фиксируется, каким образом СОА выявляет и идентифицирует каждую атаку из базы данных сетевых атак. В журнале СОА анализируются содержание и количество предупреждений, фиксируемое в процессе проведения атаки.

В результате фиксируется количество и тип (согласно предложенной классификации) корректно выявленных атак, а также дается перечень атак, которые не были выявлены системой, либо их идентификация была неверной.

Дополнительно на данном этапе в файлах журнала СОА экспертным путем выделяются сигнатуры предупреждений, выдаваемых СОА при прохождении каждой из атак. Указанные сигнатуры в виде текстовых строк должны быть уникальными для множества всех предупреждений, выдаваемых СОА при прохождении всех тестовых атак. Полученные сигнатуры применяются на этапе 4.

Этап 2. Анализ корректности обработки фонового сетевого трафика. Тестирование по критерию «Качество обработки сетевого трафика» состоит в получении порогового значения интенсивности сетевого трафика, анализируемого СОА без потери пакетов. Указанный критерий показывает возможность применения СОА в сетях различной производительности. При анализе СОА рассматриваются два случая: обработка фонового трафика, не содержащего атак, и обработка трафика, состоящего из непрерывного атакующего воздействия. В результате фиксируется интенсивность сетевого трафика, при которой СОА анализирует 100 % пакетов для первого случая и обнаруживает 100 % атак для второго.

Генерируется фоновый сетевой трафик с минимальной интенсивностью (до 1 Мбит/сек). Анализируется количество предупреждений, выдаваемых СОА. По каждому предупреждению выявляется причина его появления. В случае необоснованного отнесения фрагмента фонового трафика к атаке данное предупреждение фиксируется как ложное срабатывание. Для прове-

дения дальнейших испытаний из фонового трафика удаляются фрагменты, вызывающие все ложные срабатывания СОА.

Путем исключения фрагментов фонового трафика обеспечивается отсутствие предупреждений, выдаваемых СОА, при его генерации с малой интенсивностью (до 1 Мбит/сек).

Этап 3. Получение порогового значения интенсивности сетевого трафика, анализируемого СОА без потери пакетов в режиме фонового трафика. Применяется генерируемый фоновый трафик различной интенсивности. Фиксируется (на основании информации, выдаваемой СОА) максимальная интенсивность фонового трафика, при которой СОА анализирует 100% сетевых пакетов. Дополнительно фиксируется интенсивность фонового трафика, при которой СОА анализирует 90, 80 и 50 % пакетов. На основании полученных данных строится график зависимости производительности СОА от интенсивности фонового трафика в режиме отсутствия сетевых атак.

Все предупреждения, выдаваемые СОА на данном этапе, фиксируются как ложные срабатывания.

На полученном графике дополнительно строится кривая зависимости числа ложных срабатываний от интенсивности фонового трафика.

Этап 4. Получение порогового значения интенсивности сетевого трафика, анализируемого СОА без потери пакетов в режиме интенсивного атакующего воздействия. Формируется сценарий атакующего воздействия в виде последовательности атак. Сценарий применяется циклически. Генерируется атакующее воздействие различной интенсивности без применения фонового трафика. Фиксируется (на основании информации, выдаваемой СОА) максимальная интенсивность атакующего воздействия, при которой СОА идентифицирует 100 % сетевых атак. Дополнительно фиксируется интенсивность атакующего воздействия, при которой СОА идентифицирует 90, 80 и 50 % сетевых атак.

Количество выявленных атак фиксируется с помощью программы-анализатора журнала СОА.

В случае невозможности модификации программы-анализатора для автоматизированного анализа файла-журнала СОА применяется упрощенная методика проведения данного этапа. Упрощение заключается в том, что атакующее воздействие генерируется не в соответствии со сценарием, а выбирается одна атака и циклически генерируется трафик, ее содержащий. Количество выявленных атак в этом случае фиксируется по размеру получаемого файла предупреждений, который должен быть кратен размеру файла предупреждений для одного экземпляра атаки.

Предупреждения, выдаваемые СОА, не имеющие отношения к выполненным атакам, фиксируются как ложные срабатывания.

На основании полученных данных строится график зависимости производительности СОА от интенсивности атакующего воздействия.

Этап 5. Получение рабочей характеристики СОА. При тестировании по критерию «Оптимальная рабочая характеристика СОА» в тестовый трафик на максимальной для исследуемой СОА интенсивности вводятся пакеты атакующего воздействия. Строится график зависимости доли идентифицированных атак от доли атакующего воздействия в суммарном сетевом трафике. Выявляется доля атакующего воздействия, при которой СОА обнаруживает 100% атак.

Аналогично этапу 4 циклически применяется сценарий атакующего воздействия. В качестве исходной задается интенсивность суммарного сетевого трафика на уровне, при котором СОА анализирует 100 % сетевых пакетов. Генерируется атакующее воздействие различной интенсивности в соответствии со сценарием. Для каждого значения интенсивности атакующего воздействия подбирается интенсивность фонового трафика с таким расчетом, чтобы интенсивность суммарного трафика была постоянной. Для каждой пары [интенсивность атакующего воздействия, интенсивность фонового трафика] фиксируется количество выявленных сетевых атак.

Дополнительно проводятся аналогичные измерения для повышенной интенсивности суммарного трафика (в два раза выше интенсивности, при которой СОА анализирует 100 % сетевых пакетов) и для пониженной интен-

сивности суммарного трафика (в два раза ниже интенсивности, при которой СОА анализирует 100 % сетевых пакетов).

Количество выявленных атак фиксируется с помощью программы-анализатора журнала СОА.

В случае невозможности модификации программы-анализатора также применяется упрощение методики. Фиксируются ложные срабатывания.

На основании полученных данных строятся графики зависимости производительности СОА от доли атакующего воздействия в сетевом трафике при различной интенсивности суммарного трафика (три графика).

Для каждого измерения на всех этапах эксперимент повторяется не менее семи раз. В качестве результирующего берется среднее арифметическое значение полученных величин.

3.1.2. Структура экспериментального стенда сравнительного тестирования сетевых систем обнаружения атак

Тестирование СОА проводится на специальном стенде, который имитирует атакующее воздействие и фоновый сетевой трафик. Предлагается подход к организации атакующего воздействия, основанный на формировании базы данных тестовых атак в виде массивов предварительно записанных сетевых пакетов. Указанные пакеты должны содержать трафик, передаваемый по сети в процессе осуществления компьютерных атак различного типа.

Организация атакующего воздействия включает два этапа: подготовку массива сетевых пакетов и имитацию атакующего воздействия.

Подготовка массивов сетевых пакетов выполняется следующим образом. Сначала готовятся программные модули, реализующие атаки. Эти модули могут быть либо получены в готовом виде из сети Интернет, либо откомпилированы на основе исходных кодов, также получаемых из Интернет. Для каждого модуля, согласно его описанию, готовится ОС и серверное ПО требуемой версии, уязвимой к данной атаке. При этом уязвимая ОС устанавливается не на отдельный компьютер, а формируется ее образ, подключаемый в виде виртуальной машины. В качестве виртуальных машин используется,

например, ПО VMware Workstation. Таким же способом формируется образ ОС, в которой функционирует атакующий модуль.

Далее в подготовленной виртуальной среде осуществляется атакующее воздействие, а сетевой трафик записывается с помощью анализатора. За один сеанс захвата фиксируется одна реализация атаки. Затем из трафика удаляются все лишние Ethernet-кадры, а оставшиеся делятся на три группы: сгенерированные атакующим («запросные»), сгенерированные атакуемым («ответные») и прочие, являющиеся служебным трафиком, не содержащие сигнатуры атакующего воздействия, но относящиеся к обмену между атакующим и атакуемым. Разделение ведется автоматически по следующему алгоритму. Первый Ethernet-кадр, содержащий в качестве нагрузки IP-пакет, считается сгенерированным атакующим и адресованным жертве. IP-адреса источника и приемника этого пакета запоминаются и в дальнейшем используются для выделения кадров, отправляемых атакующим и жертвой (группы «запросные» и «ответные»). Все остальные кадры формируют группу «прочие».

Ранее записанные массивы сетевого трафика компьютерных атак в процессе тестирования воспроизводятся с помощью стенда тестирования через различные сетевые адаптеры: пакеты, сгенерированные источником атаки, а также пакеты фонового сетевого трафика воспроизводятся через один сетевой адаптер, пакеты узла, на который направлено атакующее воздействие, генерируются вторым адаптером. Генерация осуществляется в строгом порядке протоколов сетевого взаимодействия, что контролируется модулем управления тестированием. С целью обеспечения вариативности эксперимента обеспечена возможность корректировки диапазонов IP-адресов в генерируемых пакетах, что позволяет осуществлять имитацию IP-сетей произвольного масштаба в рамках одного генератора сетевых пакетов. Для тестируемой СОА, подключаемой к SPAN-порту сетевого оборудования и производящей анализ трафика, такой сетевой трафик является естественным, а сетевой обмен полностью реалистичным.

Предлагаемое решение имеет следующие преимущества:

— уменьшение числа узлов, используемых на стенде. Роль атакующих уз-

лов и узлов-жертв выполняет один компьютер с двумя сетевыми интерфейсами и специально разработанным ПО;

— отсутствие ограничения по количеству выполняемых атак. Подготовка массивов сетевых пакетов ведется заранее. Уязвимые версии ОС и ПО, необходимые для этого, могут быть предварительно подготовлены и сохранены в виде образов виртуальных машин. Следовательно, количество реализуемых в ходе тестирования атак зависит лишь от числа программных модулей, имеющихся у эксперта;

— упрощенный порядок установки и использования ОС узлов-жертв. Благодаря применению технологии виртуальных машин на одной рабочей станции может храниться значительное количество образов операционных систем. Полученные образы легко переносятся с компьютера на компьютер без необходимости переустановки драйверов оборудования. После реализации атакующего воздействия можно в течение нескольких минут восстановить исходное состояние образа ОС из резервной копии;

— упрощение процесса автоматизации атакующего воздействия. Так как все сетевые пакеты, относящиеся к реализации атаки, генерируются одним и тем же ПО, существенно упрощается процесс синхронизации пакетов в рамках одной атаки, а также выстраивания атак в очередь. Упрощается процесс имитации одновременного многоузлового воздействия с применением различных атак;

— возможность циклического повторения атак. Данная возможность является одной из самых важных. Как уже говорилось, на стенде отсутствуют сами узлы-жертвы, следовательно, имитация атак не оказывает реального разрушительного воздействия на сетевые узлы. Таким образом, нет необходимости в перезагрузке или обновлении конфигурации узлов-жертв перед очередным выполнением сетевой атаки;

— возможность идентификации атакующего воздействия. Так как ПО, установленное на стенде, самостоятельно генерирует все пакеты, передаваемые по сети в ходе реализации атаки, то упрощается процесс регистрации событий, связанных с атаками. Например, могут фиксироваться: временные

метки начала и окончания атаки, идентификатор атаки, адреса атакующего и жертвы. Кроме того, заранее подготовленный сетевой трафик гарантирует, что все внешние признаки успешного проведения атаки присутствуют, и система обнаружения должна зафиксировать предупреждение.

Экспериментальный стенд (рисунок 3.1), предназначенный для проведения сравнительного тестирования сетевых СОА, а также сетевых компонентов универсальных СОА, состоит из трех персональных компьютеров (не включая ПЭВМ, на которой развертывается тестируемый образец СОА) и двух коммутаторов. «Генератор фонового сетевого трафика» — ПЭВМ, на которой установлено разработанное программное обеспечение для генерации фонового трафика в канал связи ТКО, генерируется трафик, сформированный в модуле «Синтез фонового сетевого трафика». «Модуль управления тестированием» — ПЭВМ, на которой установлено программное обеспечение, осуществляющее генерацию атакующего воздействия, централизованное управление системой тестирования и визуализацию результатов. Данное ПО включает в себя следующие компоненты: «Генератор трафика атакующего воздействия» — программный модуль, имитирующий сетевой узел атакующего (или несколько сетевых узлов), который генерирует в сеть, связанную ТКО, сетевые пакеты сформированные модулем «Синтез трафика атакующего воздействия»; «Генератор трафика атакуемой ИТС» — программный модуль, имитирующий атакуемую систему (один или несколько сетевых узлов). «Имитатор атакуемой ИТС» — ПЭВМ, оснащенная высокопроизводительным сетевым адаптером, на MAC-адрес которого направляются сетевые пакеты фонового трафика. Кроме того, данная ПЭВМ используется в составе стенда при записи трафика атакующего воздействия. Для имитации атакуемых сетевых узлов используется технология виртуальных машин, разворачиваемых на атакуемой станции с пассивной (не имеющей выделенного IP-адреса) основной операционной системой. При необходимости имитации дополнительных узлов-жертв осуществляется развертывание нескольких контрольных образцов серверов или рабочих станций.

В состав программного обеспечения стенда, позволяющего тестировать сетевые СОА в соответствии с предложенной методикой на основе использования сценариев атакующего воздействия и применения сетевого трафика с различными характеристиками, также входят единая база данных ЭТВ (хранение сетевых атак, сценариев атакующего воздействия, протоколов испытаний и служебной информации), программа «Анализатор журнала тестирования СОА» (автоматизированный анализ журналов СОА и подсчет количества обнаруженных в процессе тестирования атак).

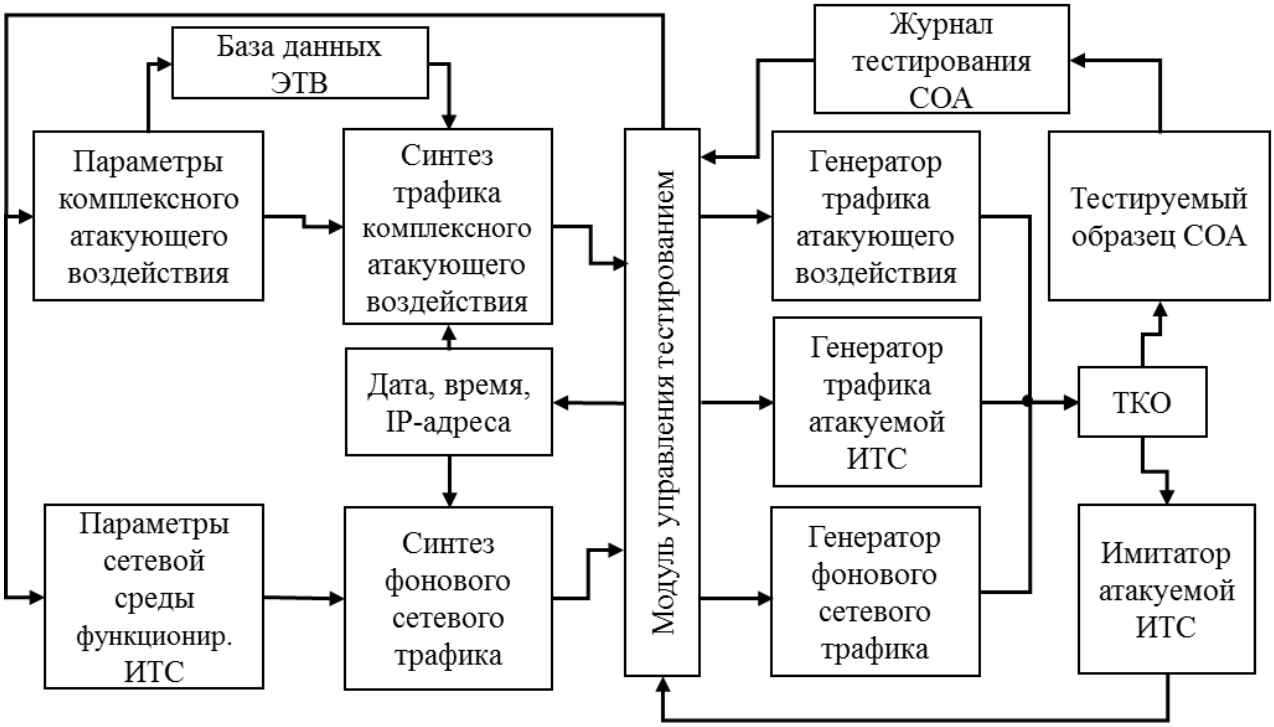

Рисунок 3.1. Схема экспериментального стенда тестирования СОА

Сформирована база данных ЭТВ (сетевых атак) в виде массивов сетевого трафика. База данных ЭТВ основана на предложенной классификации сетевых атак, учитывающей параметры сетевых потоков, протекающих между атакующим узлом и жертвой. Для каждой из атак, используемых для тестирования СОА, подготовлен образ уязвимой системы, результативность атакующего воздействия проверена, процесс проведения атаки зафиксирован с помощью анализатора сетевого трафика.

В целях пополнения базы ЭТВ и поддержания ее актуальности подготовлена база уязвимых систем в виде образов виртуальных машин. Такой

подход позволяет в короткие сроки настроить произвольную систему в уязвимой конфигурации для проверки работоспособности новой атаки и пополнения базы данных тестовых атак.

Программное обеспечение модуля управления тестированием с использованием базы данных ЭТВ позволяет формировать сценарии атакующего воздействия любой сложности без необходимости присутствия реальных узлов-жертв в момент тестирования.

Таким образом, предложенный подход к организации экспериментального стенда, предназначенного для проведения сравнительного тестирования СОА, основан на воспроизведении заранее записанных сетевых пакетов и обладает рядом преимуществ по сравнению с известным, заключающимся в реализации атак с использованием подготовленных программных модулей.

3.1.3. Программная реализация синтеза фонового сетевого трафика

Синтез фонового сетевого трафика обеспечивает генератор сетевого трафика массивами сетевых пакетов, предназначенными для направления в сетевые интерфейсы. Синтез осуществляется на основании исходных данных, формируемых при постановке сценария ситуационной задачи. Трафик генерируется трех основных видов — трафик IP-сетей, трафик протоколов http и ftp, трафик почтовых протоколов и трафик взаимодействия в социальных сетях. Синтез фонового СТ (рисунок 3.2) осуществляется тремя взаимосвязанными элементами (модулями): «Сервер», «Клиент» и модуль генерации трафика на основе матричной модели.

Модуль «Сервер» предназначен для создания виртуального Web-сервера, формирующего наполнение области данных сетевых пакетов содержимым типового Web-сервера. В «Базе данных» хранятся результаты работы, промежуточные данные и входные данные (словарь и матрицу переходов, сформированные на основе существующих текстов [227]).

Словарь и матрица переходов используются для генерации текста на основе цепей Маркова. Задачу создания Web-страницы из текста, файлов изображения и/или мультимедиа решает модуль создания Web-страниц. Для

совокупности Web-страниц формируются гиперссылки. Количество Web-страниц и их объем определяются на этапе работы модуля управления исходя из количества и характеристик потоков к Web-серверу.

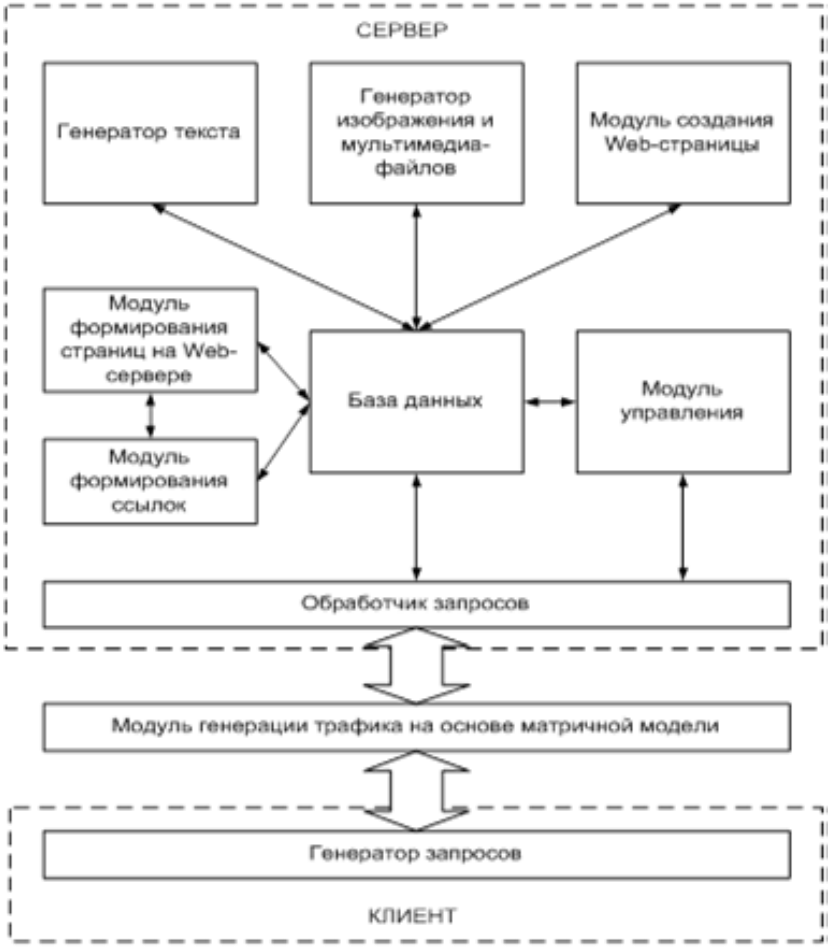

Рисунок 3.2. Схема программной реализации синтеза сетевых пакетов

Модуль управления обеспечивает взаимосвязь между всеми остальными модулями. Входными данными для этого модуля является матрица характеристик СТ, на основе которой происходит формирование структуры и наполнения Web-серверов. Объем страниц определяется в соответствии с выбранными значениями интервалов времени между пакетами и моделью нагрузки, предложенной в [231].

Работу Web-сервера выполняет «обработчик запросов», представляющий собой виртуальный Web-сервер, работающий согласно модели, описанной в [229].

Модуль «Клиент» выполняет отправку сетевых пакетов на виртуальный Web-сервер в соответствии с параметрами, описанными в [232-234]. Ис-

ходными данными являются матрица характеристик СТ и данные от модуля «Сервер» — сформированные страницы и их ранг. В соответствии с матрицей вероятностей перехода на эти страницы и матрицей характеристик СТ в момент времени начала первого потока отправляется первый сетевой пакет. Далее пакеты отправляются в соответствии с алгоритмом синтеза потоков пакетов согласно матричной модели.

3.1.4. Выявление комплексных компьютерных атак средствами многоагентной СОА AGATA

Как указывалось выше, отличительной особенностью современных компьютерных атак является их комплексный характер, который проявляется в реализации атаки через различные информационные технологии в протяженный период времени от различных источников. Далеко не все современные СОА способны к выявлению подобных атак.

С целью выявления комплексного атакующего воздействия, объединяющего как сетевые атаки, так и атаки на уровне узла, на основе модели нечетких иерархических систем разработана и внедрена в состав полигона система обнаружения атак AGATA (AGATA — AGgregated Anomaly Tracking Agent based framework — агрегированный комплекс средств отслеживания аномалий, основанный на агентах), в основе которой лежит многоагентная модель выявления комплексного атакующего воздействия (подробно описано в [270, 271, 280, 281]. Многоагентность системы обусловлена тем, что элементарные атакующие воздействия, являющиеся компонентами комплексных компьютерных атак, могут воздействовать на различные элементы ИТС. При обнаружении комплексных компьютерных атак необходимо выявлять связь между элементарными атакующими воздействиями. Многоагентная СОА построена на агентах (сенсорах) различного типа (сетевые сенсоры, узловые сенсоры, сенсоры систем контроля уровня доступа и т.п.). Анализ информации, поступающей от сенсоров, осуществляется системой принятия решений, анализирующей превышение значений различных признаков заданных пороговых значений, определяемых политикой безопасности.

В качестве источника для получения признаков обнаружения компьютерных атак может применяться политика безопасности, которая состоит из частных политик, определяющих аномальное и нормальное поведением для различных системных и сетевых параметров, и содержащих оценку критичности отклонения от сценариев нормального поведения.

С целью формализации положений политики безопасности для получения признаков обнаружения компьютерных атак используется структура данных (онтология), состоящая из совокупности лингвистических переменных и нечетких правил [280, 281].

СОА AGATA представляет собой универсальное средство обнаружения комплексных компьютерных атак на основе признаков, получаемых путем формализации положений политики безопасности с использованием аппарата иерархических нечетких систем. Возможность выявления комплексных компьютерных атак заложена в многоагентной архитектуре СОА AGATA, позволяющей для обнаружения в режиме отложенной обработки использовать информацию об инцидентах ИБ, поступающую от сенсоров различного типа.

СОА AGATA является многоагентной системой, представлена совокупностью следующих компонентов (рисунок 3.3):

- сенсорами (агентами, датчиками);
- подсистемой сбора и обработки данных о событиях ИБ;
- каталогом онтологий;
- анализатором данных, поступающих с сенсоров.

Сенсорами являются программные агенты, устанавливаемые на АРМ и серверы, связанные сетью передачи данных. Система AGATA поддерживает одновременную работу с несколькими онтологиями разработанной модели многоагентной СОА, совокупность которых называется каталогом онтологий.

Анализатор является центральным компонентом системы, осуществляет анализ и визуализацию данных о событиях ИБ, поступающих от сенсоров.

Основной функцией сенсоров является сбор значений различных параметров ИТС и ее компонентов и передача их анализатору для дальнейшей об-

работки. Выделяются два типа сенсоров — локальные и удаленные. Локальные сенсоры, через интерфейсы ОС получают значения системных параметров и характеристик сетевого узла, на котором они запущены. Удаленные сенсоры производят сбор информации с использованием протоколов сетевого управления, средств удаленного мониторинга, сетевых сенсоров СОА Snort, средств сканирования и контроля эффективности системы защиты и др.

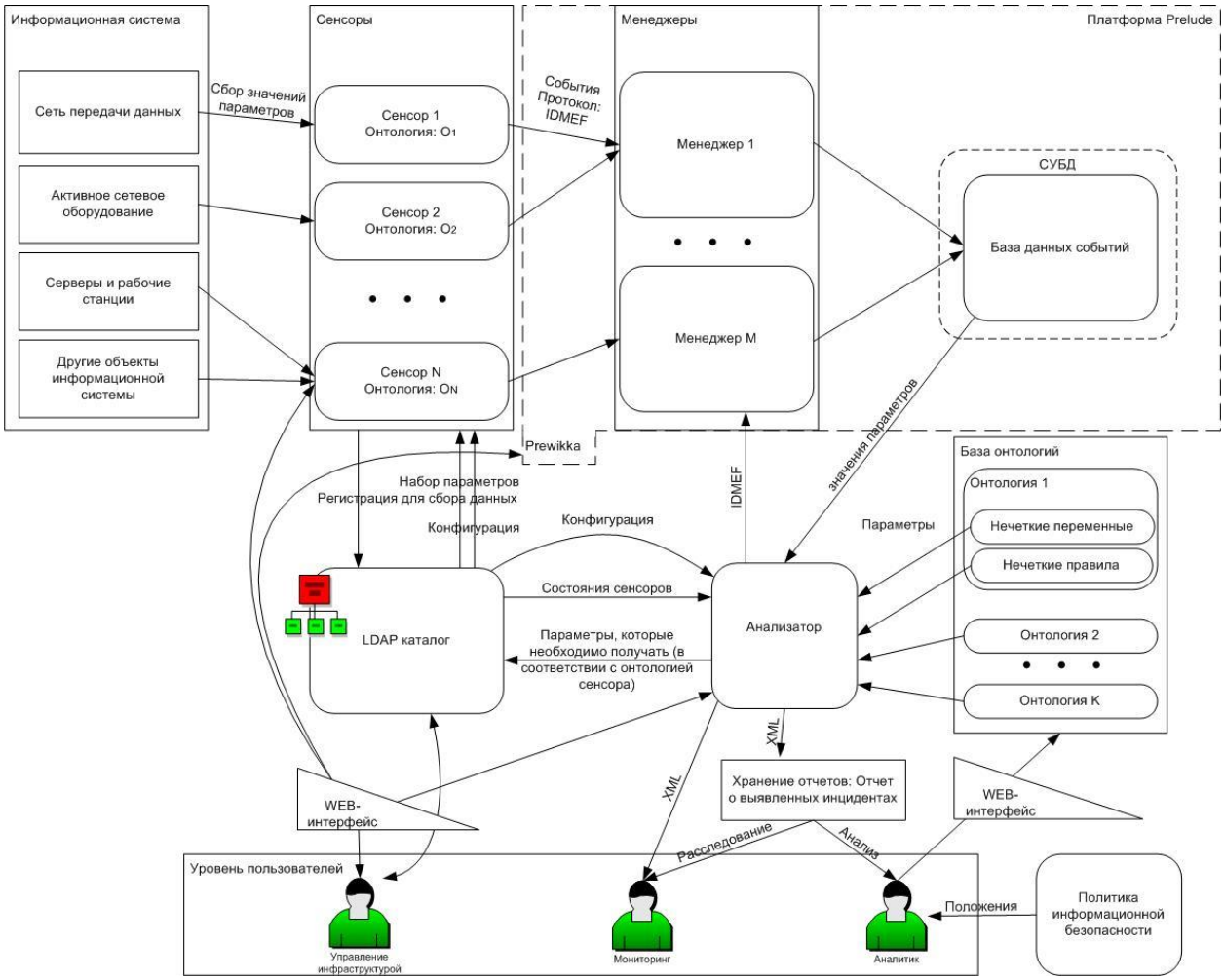

Рисунок 3.3. Структурная схема взаимодействия компонентов СОА AGATA

Каждый сенсор ассоциирован с некоторой онтологией обнаружения компьютерных атак, структура которой представлена наименованием и текстовым описанием онтологии, а также набором лингвистических переменных и нечетких правил. Для формирования онтологии используется политика безопасности, являющаяся основой для выявления аномального поведения,

отличающегося от нормального поведения, укладывающегося в рамки политики безопасности.

Объект, представляющий лингвистическую переменную, содержит следующие поля — наименование, текстовое описание, флаг значимости («интересности»), процедура извлечения, область определения функций принадлежности термов, совокупность термов. Объект «терм» также представляет структуру данных и содержит собственное наименование, функцию принадлежности и информацию о методе, которым должна вычисляться его функция принадлежности. Каждое нечеткое правило представляется парой: предпосылка и заключение, которые в свою очередь из наименования лингвистической переменной и ее значения.

Анализатор использует активные элементы каталога онтологий, указывая сенсорам, какие параметры должны быть извлечены и переданы, используя процедуры извлечения, соответствующие входным лингвистическим переменным. При обработке набора параметров анализатор использует нечеткие правила, входящие в состав онтологии, для подсчета значений значимых переменных. При ненулевых значениях значимых переменных происходит сигнализация о возможности атаки.

В функции анализатора входит также предоставление пользователю отчета об обнаруженных возможных комплексных атаках — как в интерактивном режиме, так и в виде, предназначенном для последующего анализа, например в формате IDMEF. В отчете представлена информация о времени начала атаки, наименование онтологии, в рамках которой производилось обнаружение, и сработавшие значимые переменные — с их значениями в виде графика результирующей функции принадлежности и в виде значения, полученного после дефаззификации центроидным методом.

Выявление комплексных компьютерных атак основывается на принципах ассоциативной и временной корреляции событий, поступающих в базу данных событий ИБ.

3.1.5. Процедура и результаты тестирования СОА

3.1.5.1. Результаты апробации методики для тестирования СОА Snort

Для апробации методики была использована СОА Snort версии 2.6 в режиме применения всех правил и включения всех препроцессоров.

Результаты этапа 1. Применены 6 атакующих воздействий (таблица 3.1).

Таблица 3.1. Анализ качества идентификации компьютерных атак

Атака	Идентификация атаки в журнале СОА	Точность идентификации
1. SYN-Portscan	SNMP trap tcp	Идентификация некорректна, выявлено сканирование только TCP-портов 161 и 162
2. MS04-011	MS04-011	✓
3. MS03-026	MS03-026	✓
4. MS02-045	MS02-045	✓
5. MS06-040	MS04-007	Атака выявлена, однако присвоен идентификатор иной атаки
6. FreeBSD 6.0 NFS DoS	Отсутствует	Атака выявлена, однако идентификация отсутствует

Результаты этапа 2. Установлено, что СОА Snort выявляет в качестве атаки анонимные обращения к FTP-серверу, включенные в фоновый трафик. К категории ложных срабатываний указанные обращения не относятся, однако сетевыми атаками также не являются. По результатам этапа из фонового трафика были удалены пакеты, содержащие анонимные обращения к FTP-серверу. При анализе СОА Snort полученного фонового трафика при его генерации интенсивностью 1 Мбит/сек предупреждения не выявляются.

Результаты этапа 3. Анализ 100 % пакетов в присутствующей на стенде конфигурации ПЭВМ достигается при интенсивности фонового трафика 12 Мбит/сек. При интенсивности 90 Мбит/сек анализируется 88,1 % пакетов (таблица 3.2).

Результаты этапа 4. Тестирование осуществлено повторением сценария, всего 15 000 атак. Выявление 100 %атак в присутствующей на стенде конфигурации ПЭВМ достигается при интенсивности атакующего воздей-

ствия 6 Мбит/сек. Ложных срабатываний не зафиксировано (рисунок 3.4, таблица 3.2).

Таблица 3.2. Получение порогового значения интенсивности трафика, анализируемого СОА без потери пакетов в режимах фонового трафика и интенсивного атакующего воздействия

Интенсивность фонового трафика, Мбит/сек	Анализируется пакетов в режиме фонового трафика, %	Анализируется пакетов в режиме интенсивного атакующего воздействия, %	Выявлено атак, %
6	100	100	100
12	100	64	63,8
25	98,2	27,6	27,6
50	94,4	11,7	11,7
90	88,1	5,1	5,1

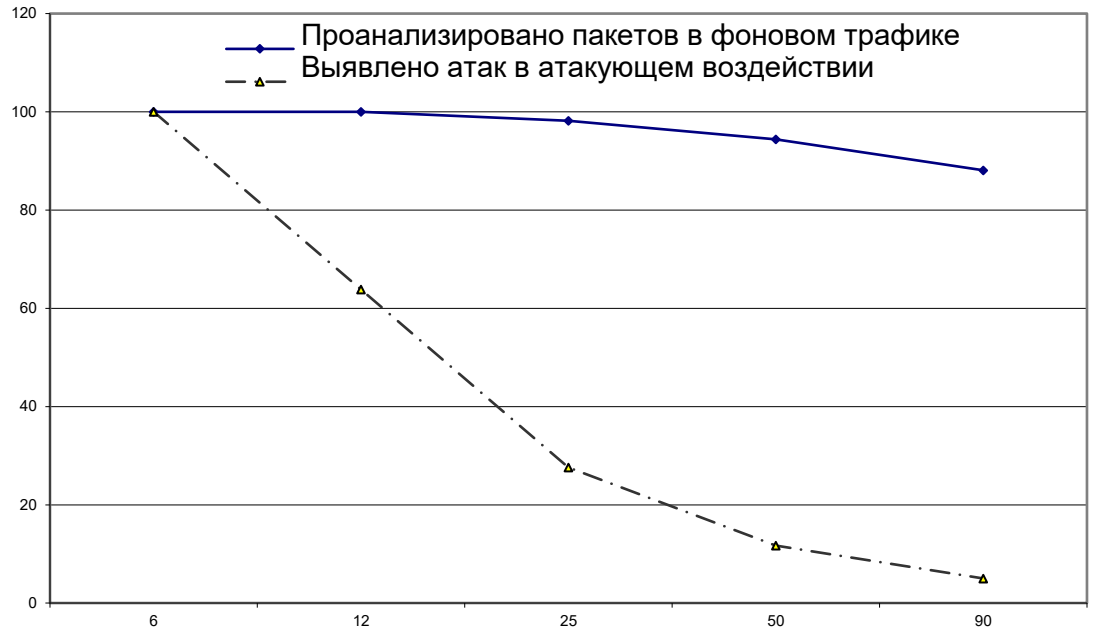

Рисунок 3.4. График зависимости % обнаружения атак от интенсивности трафика

Результаты этапа 5. Тестирование осуществлено циклическим повторением сценария, всего 300 атак трех типов. Варьировались интенсивности фонового трафика и атакующего воздействия с целью получения суммарной интенсивности 12 Мбит/сек, полученной по результатам этапа 3 (рисунок 3.5, таблица 3.3).

Таблица 3.3. Получение рабочей характеристики СОА

Интенсивность, Мбит/сек			Анализируется пакетов, %	Выявлено атак, %
фоновый трафик	атаки	% атак		
11	1	8	98,0	100
9	3	25	97,2	100
7	5	42	99,9	100
5	7	58	92,0	100
3	9	75	96,7	96,7
1	11	92	82,3	80,6

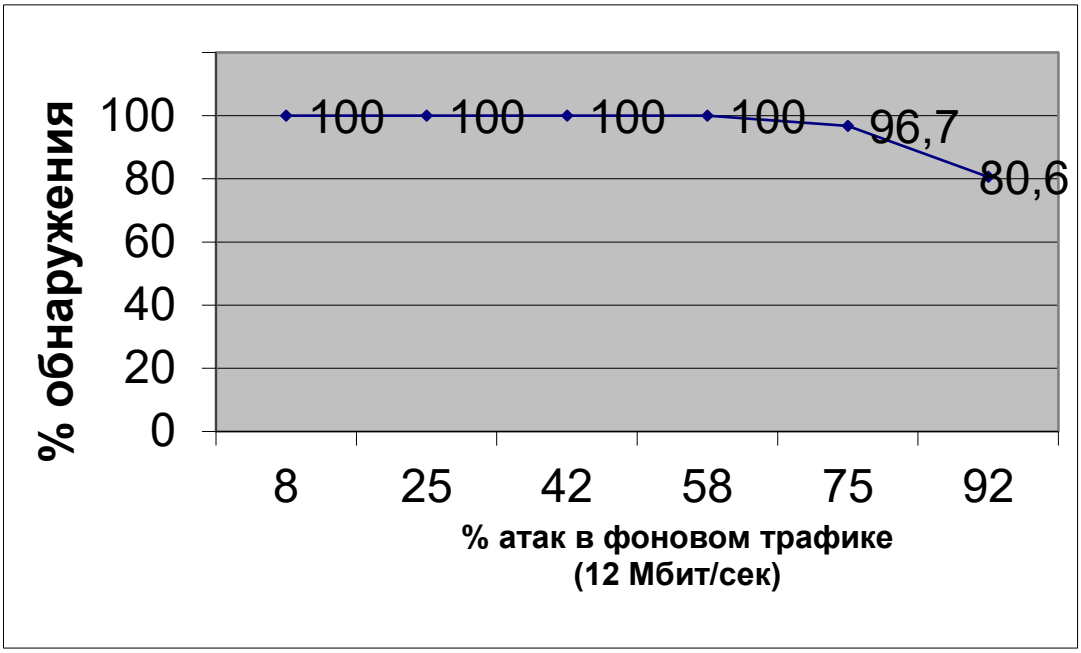

Рисунок 3.5. График рабочей характеристики СОА

Таким образом, предложенная методика апробирована для тестирования сетевой СОА Snort в стандартной конфигурации. Результаты, в частности, показали, что анализ 100 % пакетов в присутствующей на стенде конфигурации ПЭВМ достигается СОА Snort при интенсивности фонового трафика 12 Мбит/сек, при интенсивности 90 Мбит/сек анализируется 88,1 % пакетов. Выявление 100 % атак без применения фонового трафика достигается при интенсивности атакующего воздействия 6 Мбит/сек. СОА Snort осуществляет выявление 100 % атак при интенсивности трафика 12 Мбит/сек и доле атакующего воздействия до 58 %.

3.1.5.2. Тестирование многоагентных систем контроля политики безопасности

Предложенная выше методика может быть использована для тестирования сетевых СОА, функционирование которых основано на анализе сетевого трафика и выявлении атак, производимых по сети. Вместе с тем в настоящее время активно развиваются системы, называемые *локальными (host-based)*, использующие для обнаружения атак информацию, получаемую от элементов персонального компьютера, на который они установлены. Такие системы ориентированы на отслеживание попыток регистрации на локальной ЭВМ, на отслеживание активности пользователей, наделенных повышенными полномочиями в системе, на проверку целостности отдельных файлов или ключей реестра и т.п. Современные реализации указанных систем, предназначенные для выявления нарушений политики безопасности организации, относятся к классу систем контроля политики безопасности (далее — СКПБ).

Особенностью СКПБ является их многоагентность, что подразумевает их распределенную структуру, различную физическую структуру сенсоров и, соответственно, разноплановость информации, поступающей от них.

В качестве системы для отработки предлагаемого подхода к тестированию была использована разработанная СОА AGATA [271], реализующая многоагентную идеологию, состоящая из сенсоров различного типа, базы данных событий и модуля принятия решений. Кроме того, в качестве образца рассмотрен программный продукт компании Cisco Systems — система предотвращения атак на уровне узла CSA.

Атакующее воздействие на СКБП может являться последовательностью действий пользователя, включающую в себя: запуск программ, доступ к файлам (чтение, удаление, создание, модификация), модификацию учетных записей, загрузку центрального процессора и оперативной памяти, блокирование систем ввода-вывода, редактирование реестра. Особенностью тестирования СКПБ является необходимость имитации фонового и атакующего воздействия, производимого пользователями ИТС и ИС. В качестве фонового воздействия должна моделироваться многопользовательская работа сотруд-

ников организации, в качестве атакующего должно имитироваться производимое локальным пользователем воздействие, нарушающее определенное положение политики безопасности и фиксируемое системой как атака. Для организации такого воздействия требуется разработка тестовой среды, в которой, согласно определенным сценариям, должна имитироваться работа многих пользователей.

В качестве тестовой среды используется система виртуальных машин, на каждой из которых в требуемой операционной системе развертываются один или несколько сенсоров многоагентной СКПБ. В основной операционной системе стендового компьютера выполняется сценарий, имитирующий действия пользователя по регистрации в системе, запуску определенных программ, по манипуляциям с файлами. Результатом работы сценария является генерируемый клавиатурный ввод, который с помощью разработанной оболочки передается внутрь виртуальной машины, имитируя действия локального пользователя. При этом на стендовом компьютере может быть запущено одновременно несколько виртуальных машин, что позволяет имитировать одновременную работу нескольких сотрудников.

Для формирования сценариев активности пользователей разработано программное средство, эмулирующее действия легального пользователя в системе. Данное средство, используя вероятностный автомат, выполняет действия, типичные для нормальной (легитимной) работы пользователя в системе. Последовательность действий пользователя определяется вероятностной функцией перехода между состояниями автомата. Для каждого состояния параметры могут определяться с учетом особенностей работы пользователя в операционной среде.

Предложено два способа имитации действий пользователей в системе: с применением языка AutoIt и на основе использования интерфейсов системы виртуальных машин VirtualBox. AutoIt — свободно распространяемый язык, предназначенный для создания сценариев автоматизации (макросов). Сценарии конвертируются в исполняемый файл, который помещается в среду виртуальной машины, где и происходит его запуск на исполнение. Преимуще-

ства языка — в возможности создания гибкой модульной системы, что позволяет синтезировать каждое отдельное действие пользователя либо реализовывать несколько действий в едином сеансе работы пользователя.

Разработаны сценарии атакующего воздействия, реализующие атаки: отказ в обслуживании путем загрузки ресурсов центрального процессора и оперативной памяти; открытие файлов на чтение и модификацию, доступ к которым запрещен требованиями политики безопасности; модификация списка пользователей и рабочих групп ОС, создания учетных записей и включения их в группы администраторов; изменения окружения пользователя, включая модификацию параметров рабочего стола; модификации реестра путем добавления параметров автозапуска программ и удаления отдельных разделов и ключей.

Недостатком указанного подхода является то, что откомпилированный сценарий должен быть внедрен в тестируемую систему в качестве исполняемого модуля и в ней выполнен, что само по себе нарушает политику безопасности. Решением, преодолевающим этот недостаток, является использование интерфейсов системы виртуальных машин VirtualBox. Здесь сценарии создаются в виде последовательности нажатых пользователем клавиш при выполнении определенных действий. И с использованием программного интерфейса IKeyboard в виртуальную машину передаются скан-коды клавиш, нажатие которых имитируется. При данном подходе не требуется внедрения и запуска кода в тестируемой системе, что делает процесс тестирования более объективным. Разработана программа, позволяющая передавать сценарии действий пользователя в атакующую систему в виде последовательности нажатий клавиш.

Дополнительной особенностью тестирования СКПБ является невозможность тестирования с помощью общеизвестного перечня атак. СКПБ настраиваются на выявление атак в соответствии с различными требованиями, сформулированными в политике безопасности той или иной организации. Поэтому возможность определения той или иной атаки зависит от внедренной в СКПБ совокупности правил обнаружения, построенных на основа-

нии политики безопасности, т.е. зависит от качества политики безопасности. Таким образом, тестирование СКПБ должно учитывать качество выполнения системой функций по обнаружению атак в соответствии с такой политикой безопасности, на основании которой может быть получена эталонная система правил обнаружения атак.

При этом могут быть определены границы возможностей СКПБ по количеству сенсоров и интенсивности поступающих от них событий, информация от которых обрабатывается модулем принятия решений без потери событий безопасности. Для этого могут быть определены параметры функции *f:* $E \rightarrow t$, где, E — количество событий, обработанных системой, t — отрезок времени, которая система тратит на обработку заданного количества событий. Таким образом, определяется параметр EPS, представляющий собой количество связанных с безопасностью событий, которые СКПБ может получить, нормализовать, проанализировать, произвести их корреляцию и выдать результаты за приемлемый отрезок времени. В соответствии с данным показателем определяется количество сенсоров, передающих события с заданной частотой, способных нормально работать в системе.

В результате пробного тестирования прототипа СОА [271] получены результаты, позволяющие сделать вывод о работоспособности предлагаемого подхода к тестированию, с одной стороны, и о требуемой функциональности, которой обладает СОА AGATA, с другой.

3.1.6. Учебно-экспериментальные стенды для тестирования СОА и проведения учений по информационной безопасности

3.1.6.1. Стенд для тестирования СОА

В процессе тестирования исследуются свободно распространяемые программные СОА Snort и Suricata [301], аппаратно-программные комплексы типа Cisco IDS Sensor, Cisco MARS [304]. Структура учебно-экспериментального стенда для тестирования СОА Snort, Suricata и Cisco IDS Sensor в целом полностью повторяет стенд, используемый для тестирования СОА (рисунок 3.1).

Стенд представлен совокупностью информационных технологий на основе web-сервера (имитирует объект атаки), системы обнаружения сетевых компьютерных атак Cisco IDS Sensor и системы обнаружения комплексных атак на базе устройства Cisco MARS. Имитация атакующих воздействий и фонового сетевого трафика осуществляется с применением разработанных генераторов.

Для развертывания данной сети используется виртуальный стенд, состоящий из четырех ВМ и двух виртуальных сетей VMware (рисунок 3.6). Технологическая подсеть подключена к виртуальной сети VMnet1, управляющая – к сети VMnet2.

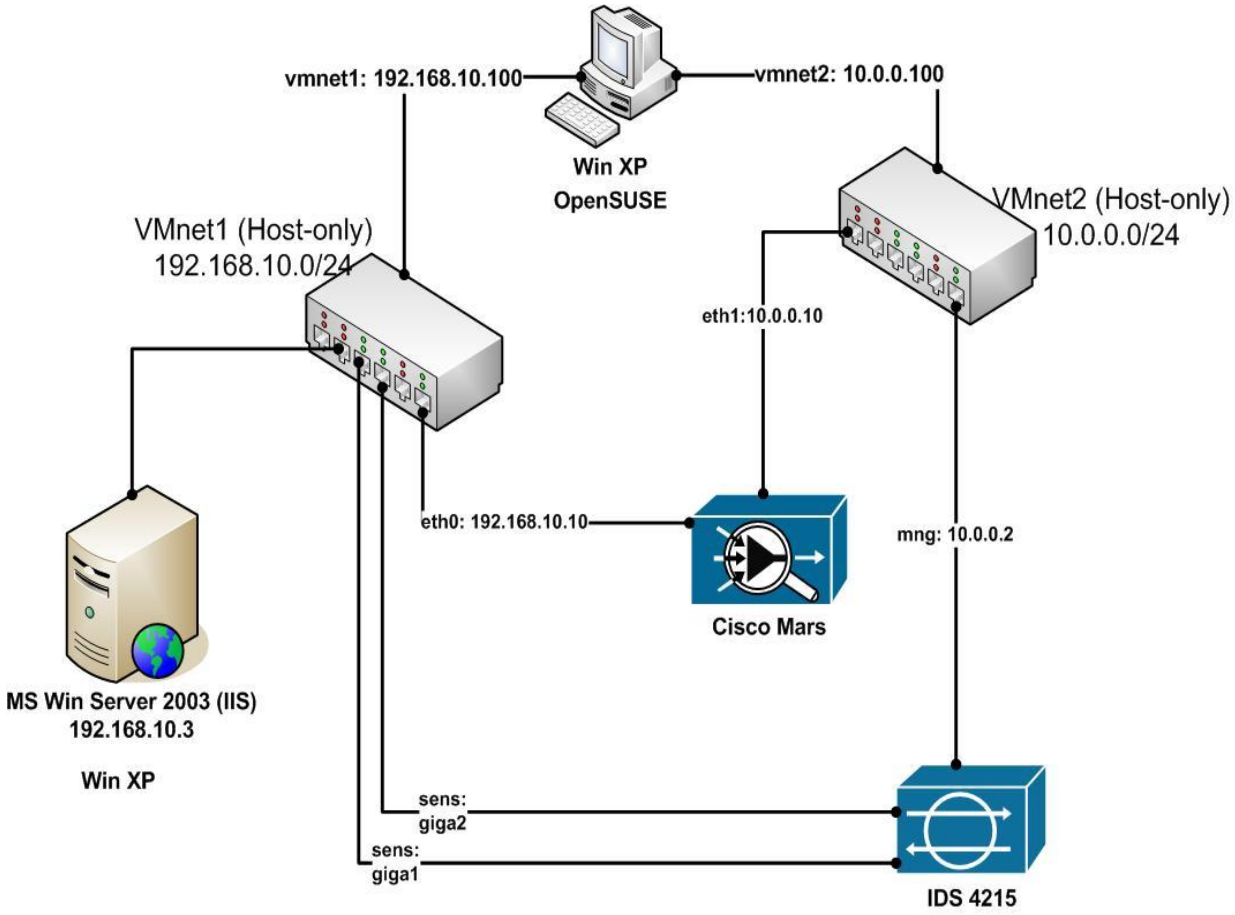

Рисунок 3.6. Структура имитируемой сети при изучении Cisco MARS

Задания для тестирования указанных СОА приведены в учебном пособии «Системы обнаружения компьютерных атак» [302], разработанном с участием автора, и представляют ряд действий по имитации и обнаружению комплексного атакующего воздействия.

3.1.6.2. Стенд для проведения учений по информационной безопасности в формате CTF

В рамках итоговых занятий, завершающих изучение дисциплины «Программно-аппаратные средства обеспечения информационной безопасности», проводятся учения по информационной безопасности в формате CTF (Capture The Flag — командная игра, главной целью которой является захват «флага» у соперника). В процессе учений учебная группа делится на две команды: атакующие и защищающиеся. Задача защищающихся — конфигурирование СОА с целью обнаружения атакующего воздействия, производимого группой атакующих на экспериментальный стенд, и расследование инцидента, связанного с реализацией атаки. Задача атакующих — проведение этапа инструментальной проверки процедуры аудита защищенности методом теста на проникновение.

«Флагами» являются метки, имеющие определенный формат и сигнатуру. «Флаги» для атакующих расположены в тех разделах инфраструктуры стенда, которые обязательны для проверки в рамках методики аудита защищенности. Обнаружение всех «флагов» показывает полноту проведенной процедуры аудита. Для защищающихся в дополнение к атакам, производимым атакуемыми, осуществляется запуск серии атак с применением генератора атакующего воздействия. В этом случае «флагами» является перечень атак, которые были имитированы генератором. Обнаружение всех «флагов» свидетельствует о правильной настройке правил обнаружения в СОА.

На стенде имитируется фиксация в журналах и файловой системе защищаемой сети следов компьютерного инцидента, вызванного проведенным атакующим воздействием. Здесь «флаги» — это заранее созданные метки в журналах безопасности и в массивах сетевого трафика и биллинговой информации. Выявление всех «флагов» говорит о полноте расследования инцидента. Результаты работы каждой из команд фиксируются автоматически путем направления соответствующего идентификатора «флага» в систему учета результатов.

3.2. *Экспериментальный стенд и методика тестирования телекоммуникационного оборудования*

3.2.1. Методика тестирования защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании»

Методика тестирования защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании» содержит следующие этапы:

1. Определение предельно допустимых значений параметров доступности информации $\widetilde{\omega} = \langle \widetilde{\omega}_j \rangle_{j=1}^{\dim \Omega}$ для сетевой среды функционирования ТКО.

2. Тестирование образца ТКО с использованием генетического алгоритма, в результате которого формируется база данных точек $\rho = \{\rho_i \mid \rho_i \in \Psi \times \Omega\}$, отражающих соответствие параметров сетевого трафика, обрабатываемого ТКО, обеспечиваемой им доступности информации:

2.1. Подключение ТКО к экспериментальному стенду, предназначенному для синтеза и воспроизведения тестового СТ.

2.2. Установка настроек ТКО, идентичных используемым в ИТС.

2.3. Исполнение генетического алгоритма.

3. Анализ результатов работы генетического алгоритма:

3.1. Внесение в настройки стенда данных о предельно допустимых значениях доступности информации $\widetilde{\omega}$.

3.2. Выделение точек $\rho^* = \{\rho_i \mid \forall i \; \exists j \colon \omega_{i,j} \geq \widetilde{\omega}_j\}$, которые соответствуют параметрам показываемой ТКО доступности информации, находящимся вне заданных предельно допустимых значений.

3.3. Кластерный анализ множества точек ρ^* методом сдвига среднего, в результате которого формируются кластеры $K = \{K_m \mid K_m \subseteq \rho^*\}$.

3.4. Определение для каждого из кластеров K_m границ критических областей C_m, отражающих параметры сетевых компьютерных атак типа «отказ в обслуживании», к которым ТКО уязвимо.

3.2.2. Анализ результатов работы генетического алгоритма

После завершения работы генетического алгоритма выполняется анализ результатов его работы, который может быть проиллюстрирован упрощенным примером (рисунок 3.7), где значимые параметры сетевого трафика компьютерных атак представлены в трехмерном пространстве Ψ, а пространство параметров доступности информации Ω является одномерным. В результате работы комплекса формируется область, являющаяся совокупностью точек пространства, в которых ТКО не обеспечивает заявленные производителем параметры производительности, $\rho = \{\rho_i \mid \rho_i \in \Psi \times \Omega\}$, где $\rho_i = \langle \psi_i, \omega_i \rangle$, $\psi_i \in \Psi$, $\omega_i \in \Omega$, (рисунок 3.7а).

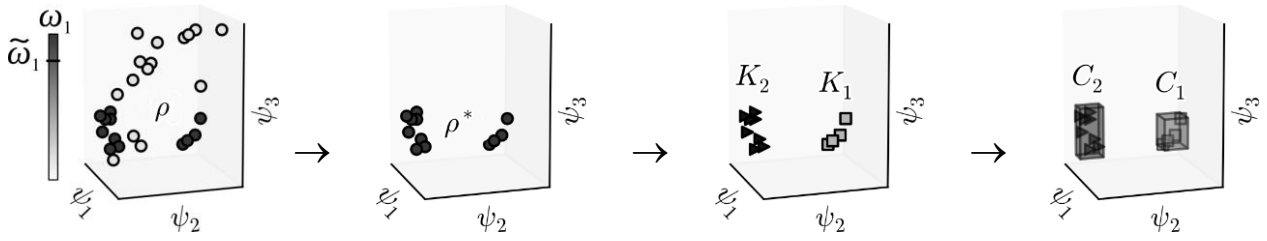

Рисунок 3.7. Пример выполнения процедуры анализа результатов работы генетического алгоритма

В данной совокупности производится выделение точек $\rho^* = \{\rho_i \mid \forall i \; \exists j : \omega_{i,j} \geq \widetilde{\omega}_j\}$, где значения параметров доступности информации превышают заданные требованиями к ИТС пороговые значения $\widetilde{\omega} = \langle \widetilde{\omega}_j \rangle_{j=1}^{\dim \Omega}$ (рисунок 3.7б). Кластерный анализ ρ^*, выполняемый с использованием алгоритма сдвига среднего (Mean Shift) [63-64], позволяет обобщить и очертить границы значений параметров сетевого трафика сетевых компьютерных атак типа «отказ в обслуживании» путем выделения множества кластеров (рисунок 3.7в) $\{K_m \mid K_m \subseteq \rho^*\}$, каждый из которых соответствует критической области C_m (рис. 3.8г), ограниченной минимальными $\langle \check{\psi}_{m,1}, \dots, \check{\psi}_{m,\dim \Psi} \rangle$ и максимальными $\langle \hat{\psi}_{m,1}, \dots, \hat{\psi}_{m,\dim \Psi} \rangle$ значениями координат точек K_m и представляющей собой многомерный прямоугольный параллелепипед размерностью $\dim \Psi$.

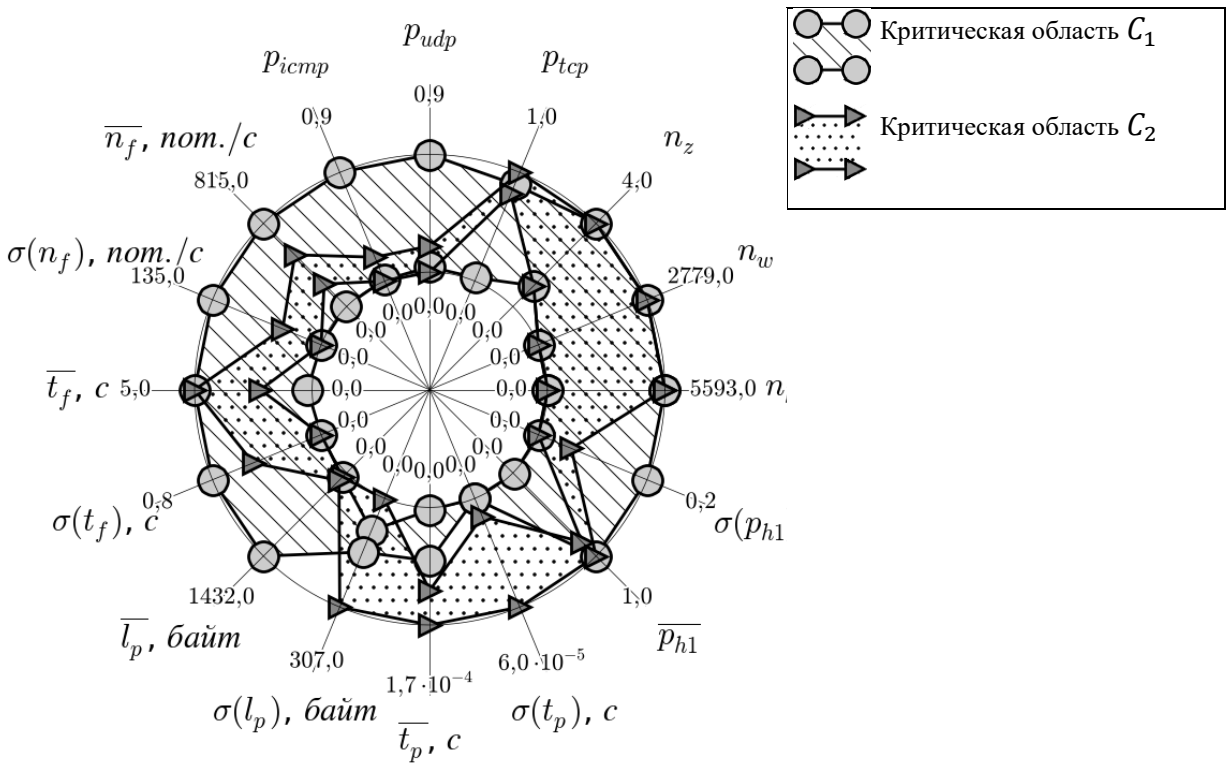

Рисунок 3.8. Пример визуализации критических областей, соответствующих параметрам сетевых компьютерных атак типа «отказ в обслуживании», к которым уязвимо ТКО, с помощью лепестковой диаграммы

Критическая область C_m— область пространства параметров сетевого трафика, циркулирующего в сетевой среде функционирования ТКО, в которой обеспечиваемая ТКО доступность информации оказывается худшей в сравнении с предельно допустимым значением, заданным для рассматриваемой ИТС. Визуализация параметров сетевого трафика выявленных сетевых компьютерных атак в многомерном пространстве Ψ производится с использованием лепестковой диаграммы (рисунок 3.8), где выявленные критические области C_1 и C_2 описываются геометрическими областями, заключенными между обозначенными на осях координат максимальными и минимальными значениями параметров сетевого трафика соответствующих им компьютерных атак типа «отказ в обслуживании» [259].

Практическая значимость решения состоит в возможности нахождения ранее неизвестных уязвимостей, приводящих к нарушению производительности ТКО при определенных сочетаниях параметров входных данных, не являющихся пороговыми.

3.2.3. Экспериментальный стенд тестирования защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании»

Экспериментальный стенд для оценки защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании» содержит следующие компоненты (рисунок 3.9):

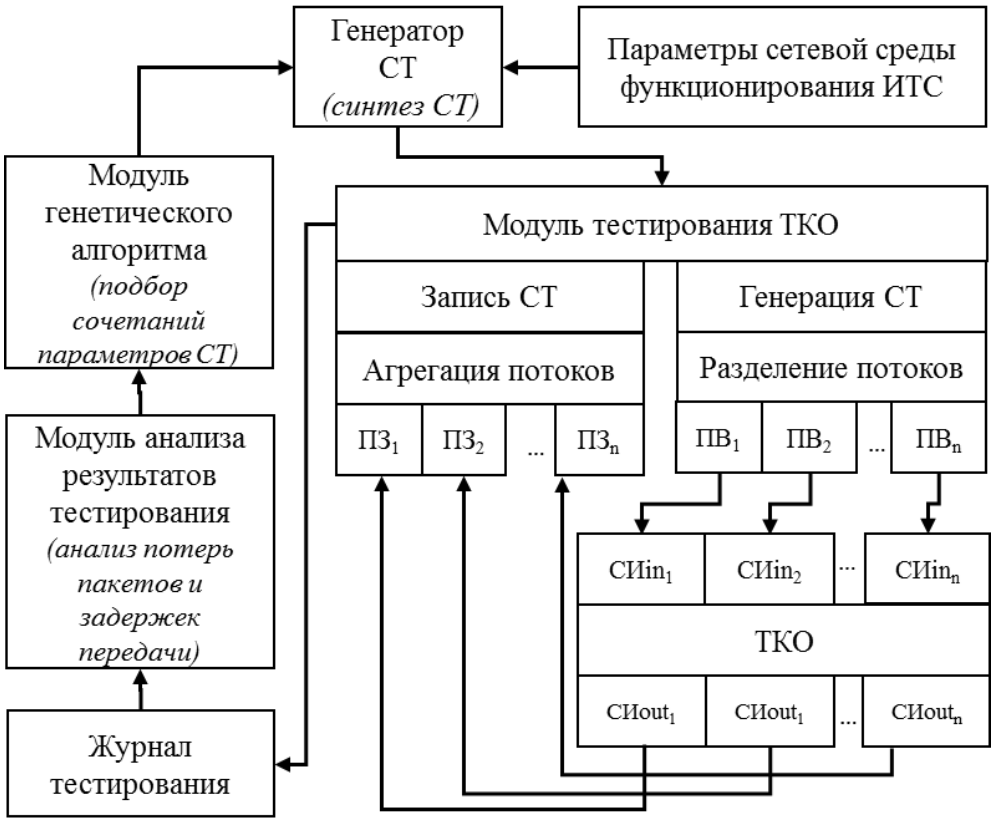

Рисунок 3.9. Структура экспериментального стенда для оценки защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании»

— модуль тестирования, выполняющий воспроизведение тестового сетевого трафика и одновременную запись сетевого трафика, принятого после обработки тестируемым образцом ТКО;

— генератор сетевого трафика, синтезирующий тестовый сетевой трафик с параметрами, заданными моделью сетевой среды функционирования ТКО;

— 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 процессе работы модуля тестирования, сформированные генератором массивы тестового сетевого трафика $\{T_i\}_{i=1}^{n_z}$ передаются для воспроизведения через сетевые интерфейсы программами воспроизведения. Одновременно на всех сетевых интерфейсах модуля тестирования программами записи производится перехват пакетов, как отправляемых, так и принимаемых с сетевых интерфейсов в соответствующие файлы $\{D_i\}_{i=1}^{n_z}$. С целью количественной оценки параметров доступности информации определяется соответствие между отправленными и принятыми пакетами. Для этого с помощью программы распределения производится копирование пакетов, содержащихся в $\{D_i\}_{i=1}^{n_z}$, в множества $\{S_i\}_{i=1}^{n_z}$ и $\{R_i\}_{i=1}^{n_z}$ файлов, где в S_i и R_i помещаются пакеты, отправленные ТКО с -го сетевого интерфейса и перехваченные в моменты их передачи в направлениях от модуля тестирования к ТКО и обратно. Программа сопоставления производит анализ сформированных файлов для определения соответствия отправленных пакетов принятым, моментов времени их отправки и приема и вычисления вектора параметров доступности информации $\omega \in \Omega$. Кроме того, программа сопоставления производит вычисление значений вектора $\psi \in \Psi$ статистических параметров перехваченного сетевого трафика. Данные векторы ω и ψ передаются для дальнейшей обработки модулю генетического алгоритма.

Генератор создает образцы тестового сетевого трафика на основе параметрической модели сетевой среды функционирования ТКО. Данная модель позволяет имитировать условия внешней среды, в которой функционирует тестируемый образец ТКО — совокупность структуры компьютерной сети, в которую образец включен, и статистических характеристик обрабатываемого им сетевого трафика (как штатного, так и содержащего атакующее воздействие).

Применение экспериментального стенда включает следующие этапы:

1. Настройка тестируемого образца ТКО (установка IP-адресов сетевых интерфейсов, таблиц маршрутизации) и экспериментального стенда (границы допустимых параметров тестирования, IP- и MAC-адреса).

2. Тестирование образца ТКО.

3. Анализ результатов тестирования образца ТКО, выявление параметров обнаруженных сетевых компьютерных атак типа «отказ в обслуживании», к которым ТКО уязвимо в заданной сетевой среде.

При создании генератора сетевого трафика для увеличения объемов генерируемого трафика и минимизации возможных задержек на пути пакетов в составе стенда нагрузочного тестирования ТКО использован [285] генератор трафика, работающий в виде модуля ядра ОС Linux. Генератор позволяет варьировать параметрами трафика: диапазоном MAC-адресов и IP-адресов (исходящих и назначения), максимальным и минимальным размерами UDP-пакетов при случайной генерации заполнения пакетов, номерами UDP-портов, исходящими и назначения, задержками между пакетами. Тестирование модуля показало его способность генерации до 1 млн UDP-пакетов в секунду, что составляет около 2 Гб/с.

3.2.4. Особенности применения генетического алгоритма при тестировании серверов IP-телефонии

В рамках задачи тестирования сервера IP-телефонии под особью генетического алгоритма будем понимать конкретные параметры генерируемого трафика. Каждая особь состоит из 4-х генов (характеристик трафика, см. п. 1.2.4.3): количество запросов REGISTER на регистрацию абонента; количество запросов INVITE на совершение звонка; количество пакетов RTP с «голосом»; количество запросов OPTIONS на получение информации о сервере.

Диапазон изменений и шаг характеристик трафика определены с помощью нагрузочного тестирования. Пределы допустимых значений параметров генов: в качестве минимального значения выбирается среднее, в качестве максимального – пороговое (таблица. 3.4). К внешним наблюдаемым призна-

кам можно отнести: время ответа сервера на каждый из пакетов, потерю пакетов, джиттер, неравномерность обработки и т.д.

Таблица 3.4. Допустимые параметры генов

Тип запроса	Минимальное значение	Максимальное значение	Шаг	Максимальное значение, полученное в результате работы ГА
INVITE	40	1000	20	500
REGISTER	100	1060	20	200
OPTIONS	38	1100	20	500
RTP	92	2230	50	1000

Степень приспособленности каждой особи зависит от значения времени обработки каждого из пакетов. Таким образом, требуется получить оценку фенотипа и отразить ее на оси положительных (время не может быть отрицательно) чисел. Применительно к задаче поиска глобальных максимумов, чем больше особь приспособлена к внешней среде, тем выше значение ее функции приспособленности. Следовательно, цель эволюции заключается в повышении функции приспособленности, т.е. в получении максимальных значений SIP-трафика, при которых сервер успевает отвечать за 150 мс на 90% полученных пакетов. Численность популяции в эксперименте 30 особей, а число поколений равно 100.

В процессе работы генетического алгоритма, когда на сервер направлялись пакеты с увеличением количества пакетов по всем видам запросов, выявлены пороговые значения, которые существенно ниже пороговых значений, ранее выявленных нагрузочным тестированием.

Результатом тестирования с применением генетического алгоритма явилось выявление уязвимости системы IP-телефонии к атаке на отказ в обслуживании при относительно небольших количественных параметрах трафика: сервер обрабатывает запросы с задержкой более 150 мс при одновременном выполнении более 250 звонков (т.к. каждый звонок сопровождается двумя пакетами INVITE) и направлении RTP пакетов с интенсивностью более 3-х раз в секунду.

3.2.5. Экспериментальные результаты применения метода синтеза сетевого трафика и генетического алгоритма при тестировании ТКО

С использованием предложенного экспериментального стенда проведен ряд экспериментов по синтезу сетевого трафика и выявлению критических уязвимостей ТКО к сетевым компьютерным атакам типа «отказ в обслуживании», результаты которых опубликованы в [259, 269 и 268].

Для проведения экспериментов были использованы массивы сетевого трафика, представленные в открытом доступе в сети Интернет, содержавшие пакеты протоколов IP-телефонии (SIP и RTP), HTTP, FTP, NetBIOS и DNS, а также ряда реализаций сетевых атак типа «отказ в обслуживании» таких как ARP Poisoning, UDP Flood, ICMP Flood и TCP SYN Flood. В рамках эксперимента проводился анализ по ряду величин, в том числе по значениям величин интенсивности передачи данных и межпакетного временного интервала.

Экспериментальные результаты при проведении сравнения статистических характеристик образцов сетевого трафика и тестового сетевого трафика показали, что максимальное значение относительного отклонения параметров синтезированного сетевого трафика от параметров имеющихся образцов сетевого трафика компьютерных сетей не превысило 0,02.

Результаты тестирования образцов ТКО приведены в виде лепестковых диаграмм: управляемый коммутатор FastEthernet, применяемый, в том числе в сетях АСУ ТП (ТКО1, рисунок 3.10), управляемый коммутатор Ethernet третьего уровня (ТКО2, рисунок 3.11), маршрутизатор (ТКО3, рисунок 3.12) и маршрутизатор, реализующий функции коммутатора Ethernet третьего уровня (ТКО4, рисунок 3.13), предназначенные для применения в сетях масштаба предприятия.

В качестве критерия тестирования были приняты следующие требования к результатам обработки ТКО информации: относительная доля потерь пакетов $q<0{,}001$, джиттер $\sigma(\delta t_p) <50$ мс, средняя задержка передачи пакетов $\bar{t}_d < 100$ мс. Использован трафик различной интенсивности I_d, как в диапазонах максимальных значений интенсивности, так и при низких значениях.

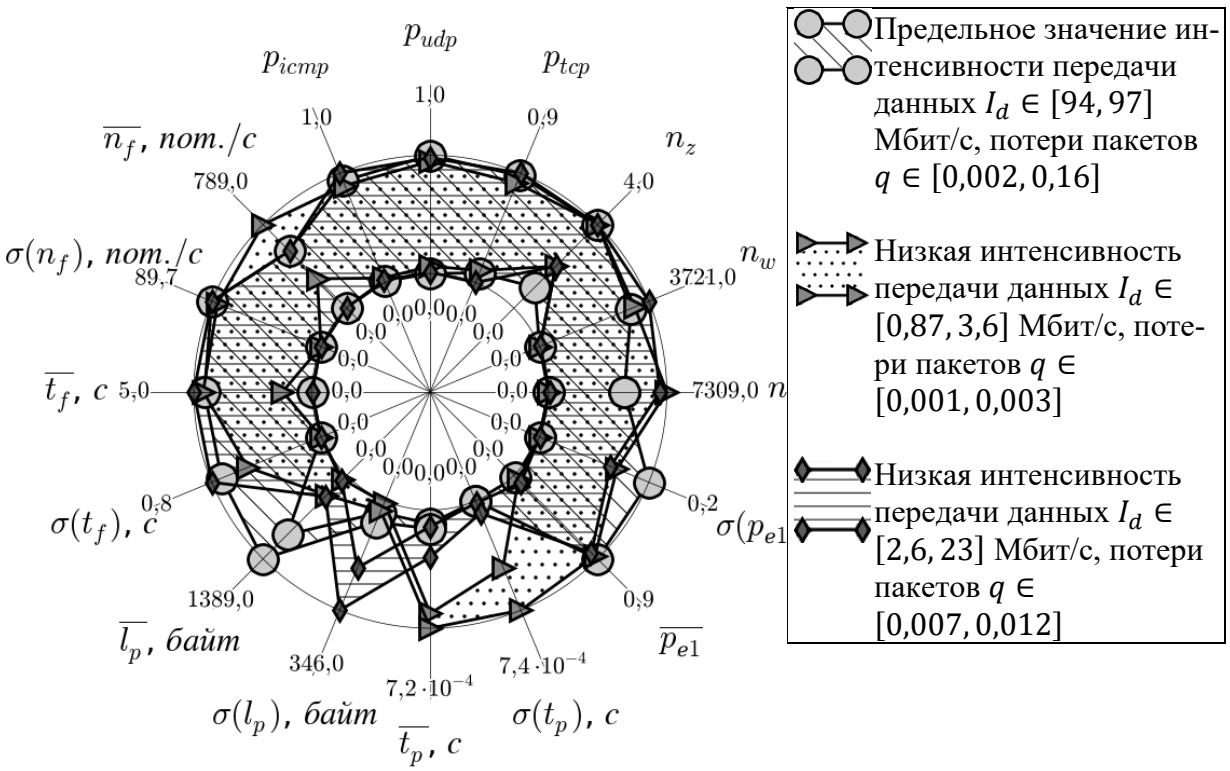

Рисунок 3.10. Критические области, выявленные при тестировании ТКО1

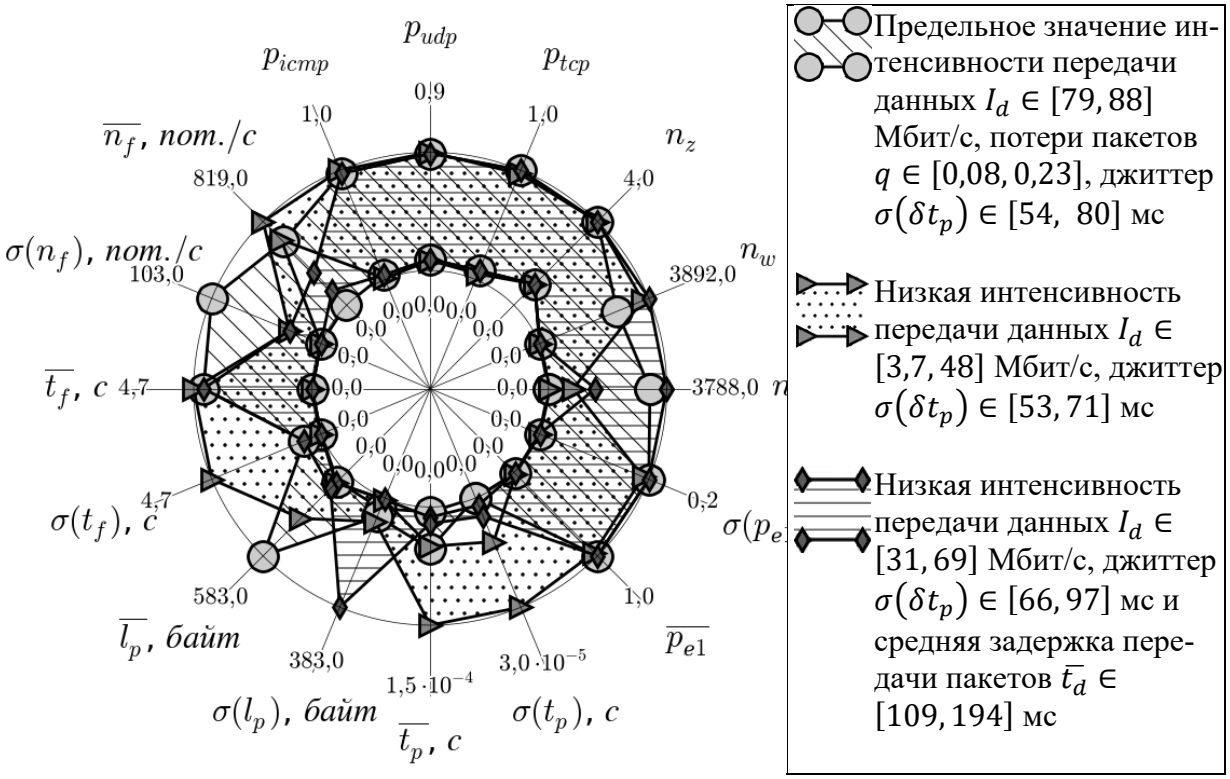

Рисунок 3.11. Критические области, выявленные при тестировании ТКО2

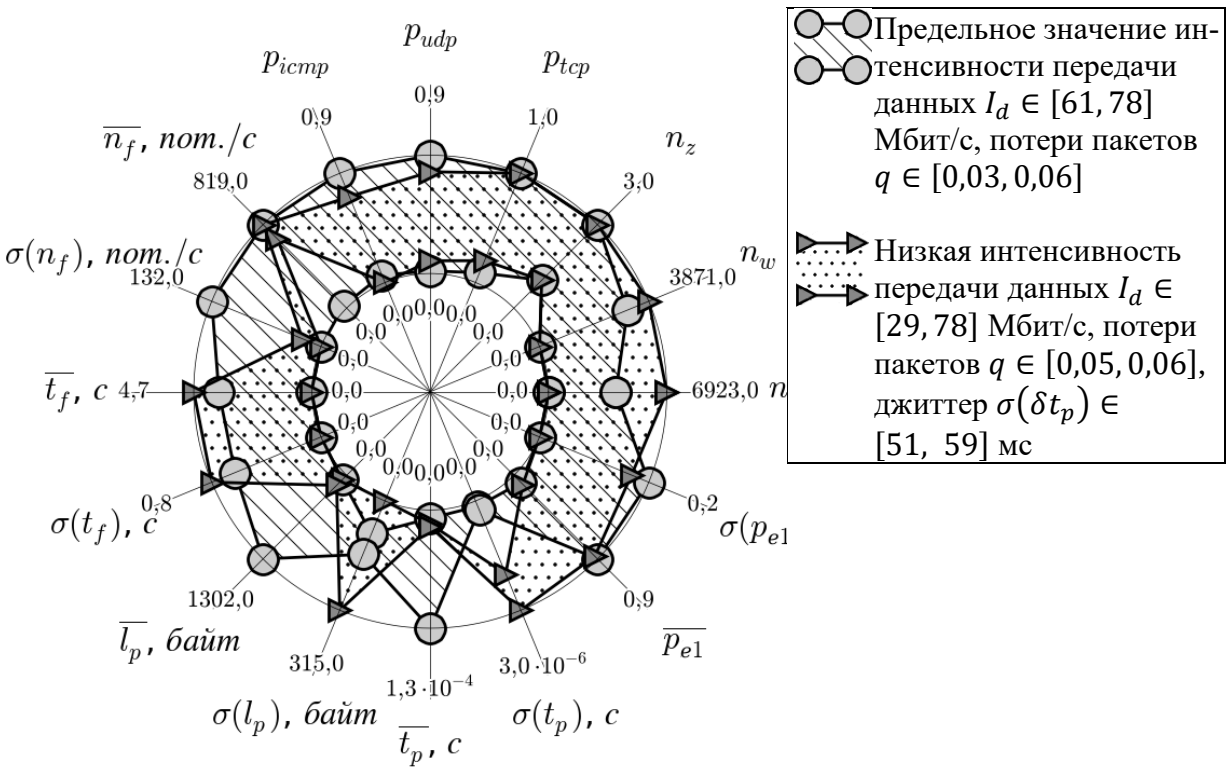

Рисунок 3.12. Критические области, выявленные при тестировании ТКО3

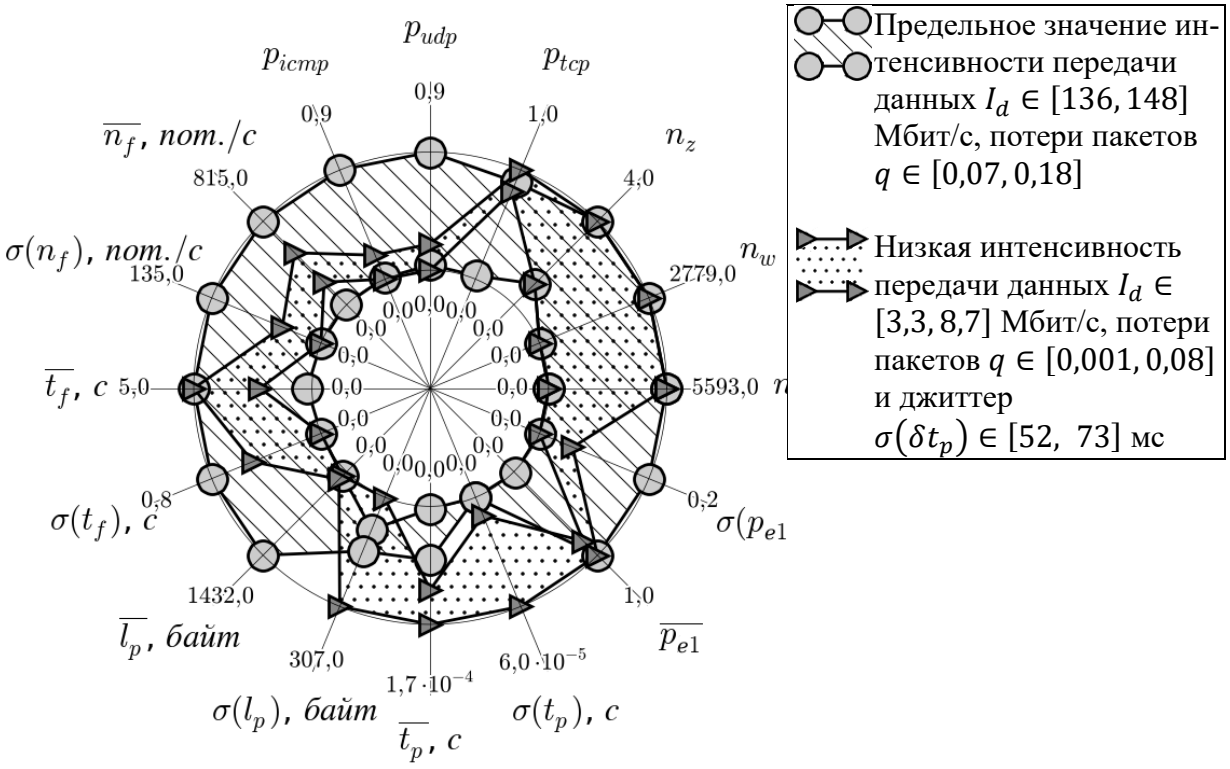

Рисунок 3.13. Критические области, выявленные при тестировании ТКО4

Результаты тестирования представленных образцов показали, что при достижении предельных значений интенсивности передачи данных, но значительно ниже заявленных в документации на устройства, выявляются параметры сетевого трафика, которые вызывают существенные потери производительности образцов ТКО и позволяют реализовать компьютерные атаки типа «отказ в обслуживании».

Вместе с тем, для каждого из образцов выявлена минимально одна критическая зона, в которой при определенных сочетаниях параметров сетевого трафика относительно низкой интенсивности проявляются высокие значения потерь пакетов, что свидетельствует о наличии уязвимости к указанному выше классу атак.

Для сравнения проведено тестирование указанных образцов ТКО с помощью специализированных средств нагрузочного тестирования IxChariot и D-ITG, реализующих методику тестирования RFC 2544 (таблица 3.5). Специализированными средствами были выявлены критические области уязвимости к сетевым компьютерным атакам типа «отказ в обслуживании», обусловленные достижением образцами ТКО предельного значения интенсивности передачи данных. С помощью разработанного стенда дополнительно выявлены уязвимости при низкой интенсивности трафика.

Таблица 3.5. Результаты тестирования образцов ТКО

Средство тестирования	Количество выявленных/невыявленных критических областей			
	ТКО1	ТКО2	ТКО3	ТКО4
Разработанный экспериментальный стенд	3/0	3/0	2/0	2/0
IxChariot и D-ITG	1/2	1/2	1/1	1/1

Таким образом, экспериментальные исследования подтвердили способность разработанного генетического алгоритма тестирования ТКО с высокой степенью надежности выявлять сочетания параметров сетевого трафика, при которых ТКО уязвимо к атакам типа «отказ в обслуживании».

3.3. *Выводы по главе 3*

В главе 3 представлен комплекс моделей, методик, алгоритмов, программного обеспечения и учебно-экспериментальных стендов для тестирования СОА и ТКО.

Описаны предложенные экспериментальный стенд и методика тестирования СОА. Методика проведения сравнительного тестирования сетевых СОА основана на анализе вероятности обнаружения сетевых атак в зависимости от интенсивности сетевого трафика и доли атакующего воздействия.

Для оценивания сетевых СОА в рамках предложенной методики применяются критерии, учитывающие вероятности правильного обнаружения атак и вероятности ложных тревог: качество идентификации компьютерных атак, качество обработки сетевого трафика, оптимальная рабочая характеристика СОА. Тестирование СОА проводится на специальном стенде, который имитирует атакующее воздействие и фоновый сетевой трафик, основан на воспроизведении заранее записанных сетевых пакетов. Синтез фонового сетевого трафика осуществляется на основании исходных данных, формируемых при постановке сценария ситуационной задачи, и реализуется генератором сетевого трафика.

Представлен комплекс моделей, методик, алгоритмов, программного обеспечения и учебно-экспериментальных стендов для тестирования ТКО. С целью определения границ устойчивости ТКО к атакующему воздействию типа «отказ в обслуживании» предложен метод автоматизации тестирования, основанный на применении эволюционно-генетического подхода. Практическая значимость решения состоит в возможности нахождения ранее неизвестных уязвимостей, приводящих к нарушению производительности оборудования при определенных сочетаниях параметров входных данных, не являющихся пороговыми. Предложенный подход нашел положительное применение для тестирования ТКО — маршрутизаторов, межсетевых экранов и серверов IP-телефонии.

Адекватность представленных алгоритмов (построенных на базе изложенного в главе 2 комплексного метода синтеза интерактивной сетевой сре-

ды для компьютерных полигонов в сфере информационной безопасности) и их программной реализации подтверждена положительными результатами их внедрения в 2015 и 2021 годах в режиме опытной эксплуатации в обществе с ограниченной ответственностью «Уральский центр систем безопасности» с целью тестирования образцов ТКО и расследования инцидентов информационной безопасности, что подтверждено актами о внедрении.

Таким образом, комплекс моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных, основанный на методике моделирования интерактивной сетевой среды для тестирования СОА, позволяет осуществлять автоматизированное тестирование СОА. Комплекс моделей, алгоритмов, методик и программного обеспечения для тестирования устойчивости ССЗИ к сетевым атакам типа «отказ в обслуживании», основанный на применении эволюционно-генетического подхода, позволяет в автоматизированном режиме выявлять ранее неизвестные уязвимости ССЗИ к сетевым атакам, приводящим к нарушению производительности ССЗИ при определенных сочетаниях параметров входных данных, не являющихся пороговыми. Решена частная научная задача по разработке алгоритма, обеспечивающего автоматизацию процесса выявления пороговых параметров устойчивости ССЗИ на примере ТКО к компьютерным атакам типа «отказ в обслуживании».

4. КОМПЛЕКС МОДЕЛЕЙ, МЕТОДИК, АЛГОРИТМОВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УЧЕБНО-ЭКСПЕРИМЕНТАЛЬНЫХ СТЕНДОВ КОМПЬЮТЕРНОГО ПОЛИГОНА ПО РАССЛЕДОВАНИЮ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. *Модель компьютерного полигона по расследованию инцидентов информационной безопасности*

4.1.1. Понятие и схема расследования инцидента информационной безопасности

В соответствии с [15], инцидент информационной безопасности определяется как «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность». Во многих случаях инциденты ИБ происходят в результате и в рамках компьютерных атак, определяемых согласно [23], как «целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств».

Таким образом, процесс расследования инцидентов ИБ включает, прежде всего, анализ событий («определенной совокупности обстоятельств») ИБ, являющихся, в соответствии с [24], составляющими частями инцидента ИБ. Расследование проводится с помощью ИАСБ путем загрузки и анализа данных, зафиксированных техническими средствами.

Расследование инцидентов ИБ связано с анализом множества разноформатных массивов данных, присущих компьютерной системе и содержащих информацию о воздействиях на файлы: временные отметки файлов, журналы событий операционной системы, журналы аудита, журналы средств защиты информации, записи о последних открытых файлах и т.д.

Причиной возникновения инцидента является событие ИБ, которое согласно [14], определяется как «идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нару-

шение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности». В соответствии с [15] инцидент определяется как совокупность событий ИБ, каждое из которых является воздействием на файловый объект.

Процесс расследования инцидентов ИБ с точки зрения анализа событий, зафиксированных техническими средствами, в общем случае может быть разбит на четыре основных этапа (рисунок 4.1).

1. Выявление IP-адреса, типа и временной метки атакующего воздействия. журналы СОА.

2. Определение Интернет-провайдера, которому принадлежит данный IP-адрес. Анализируется база данных о принадлежности IP-адресов.

3. Анализ журналов авторизации пользователей и выявление совокупности IMSI, MSISDN в заданном интервале времени. Анализируются журналы системы авторизации (TACACS и RADIUS).

4. Анализ сведений о взаимодействии и перемещении пользователей в сетях оператора сотовой связи и в социальных сетях.

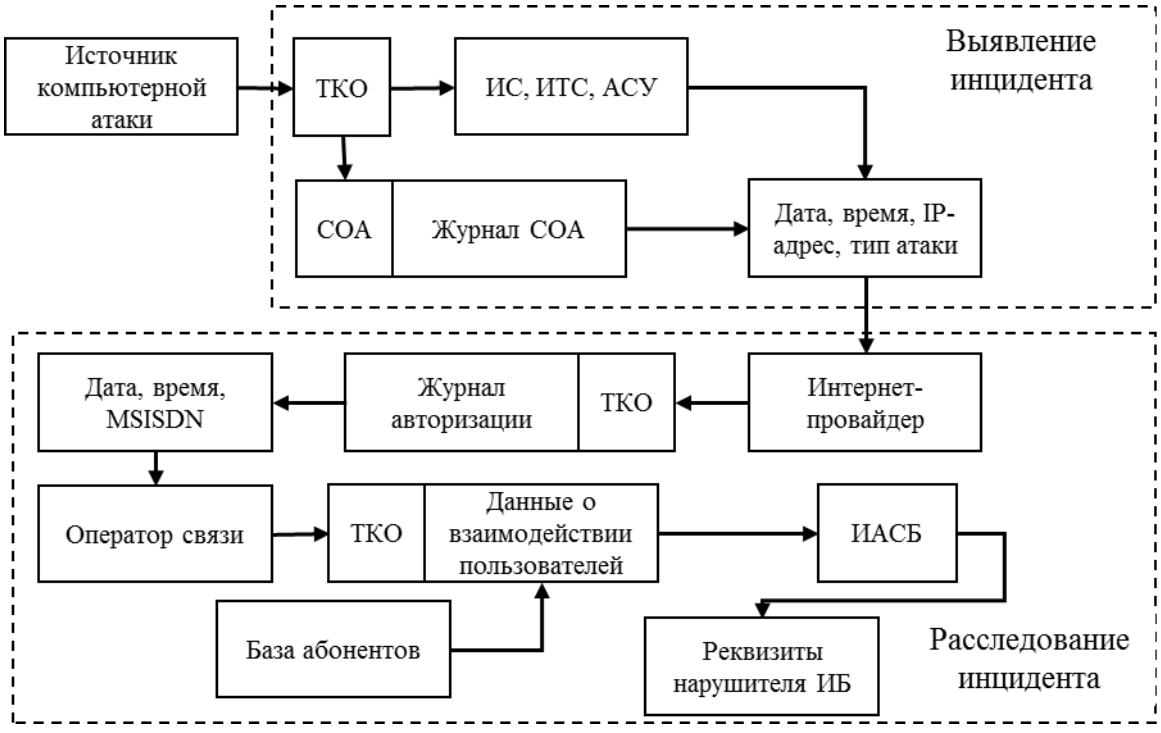

Рисунок 4.1. Схема расследования инцидента информационной безопасности

4.1.2. Функциональная модель автоматизированной обучающей системы компьютерного полигона по расследованию инцидентов информационной безопасности

Одним из важнейших этапов построения автоматизированной обучающей системы (АОС как разновидности автоматизированной информационной системы — АИС) является ее синтез, который предполагает, в том числе разработку модели системы (состава и функционального назначения модулей) в соответствии со стандартом IDEF0, где описание системы организовано в виде совокупности иерархически упорядоченных и взаимосвязанных диаграмм.

В результате анализа складывается функциональная модель проведения учений по расследованию инцидентов информационной безопасности в виде иерархии диаграмм потоков данных с разработанными для всех информационных процессов нижнего уровня детальными спецификациями. На основе функциональной модели далее определяются архитектура АОС, ее задачи по отдельным модулям, а также интерфейсы АИС и распределение функционала между преподавателями, техническими специалистами и обучающимися.

Структура АОС построена на базе предложенной функциональной модели процесса проведения учений по расследованию инцидентов информационной безопасности. В представленной модели процесс проведения учений разделен на четыре направления: синтез комплексной ситуационной задачи, выявление атакующего воздействия, сбор и анализ технических данных, выявление субъекта атакующего воздействия.

IDEF0-схемы основных блоков разработанного комплекса программных средств АОС киберполигона по расследованию инцидентов информационной безопасности демонстрируют взаимосвязь процессов при организации и проведении учений по компьютерной безопасности (рисунок 4.2 - рисунок 4.9). В рамках модели проведена декомпозиция единого процесса проведения учений на отдельные процессы и подпроцессы, что позволило учесть важнейшие составляющие моделируемых процессов при разработке функциональной структуры АОС. Для каждого процесса выделены входные и выход-

ные данные. Входными данными для процессов являются условия ситуационных задач, требуемые для формирования компетенции и материально-технические (стенды и ПО) ресурсы.

В качестве выходных данных выступают результаты выполнения этапов расследования инцидентов, позволяющие сформировать и оценить степень сформированности компетенций.

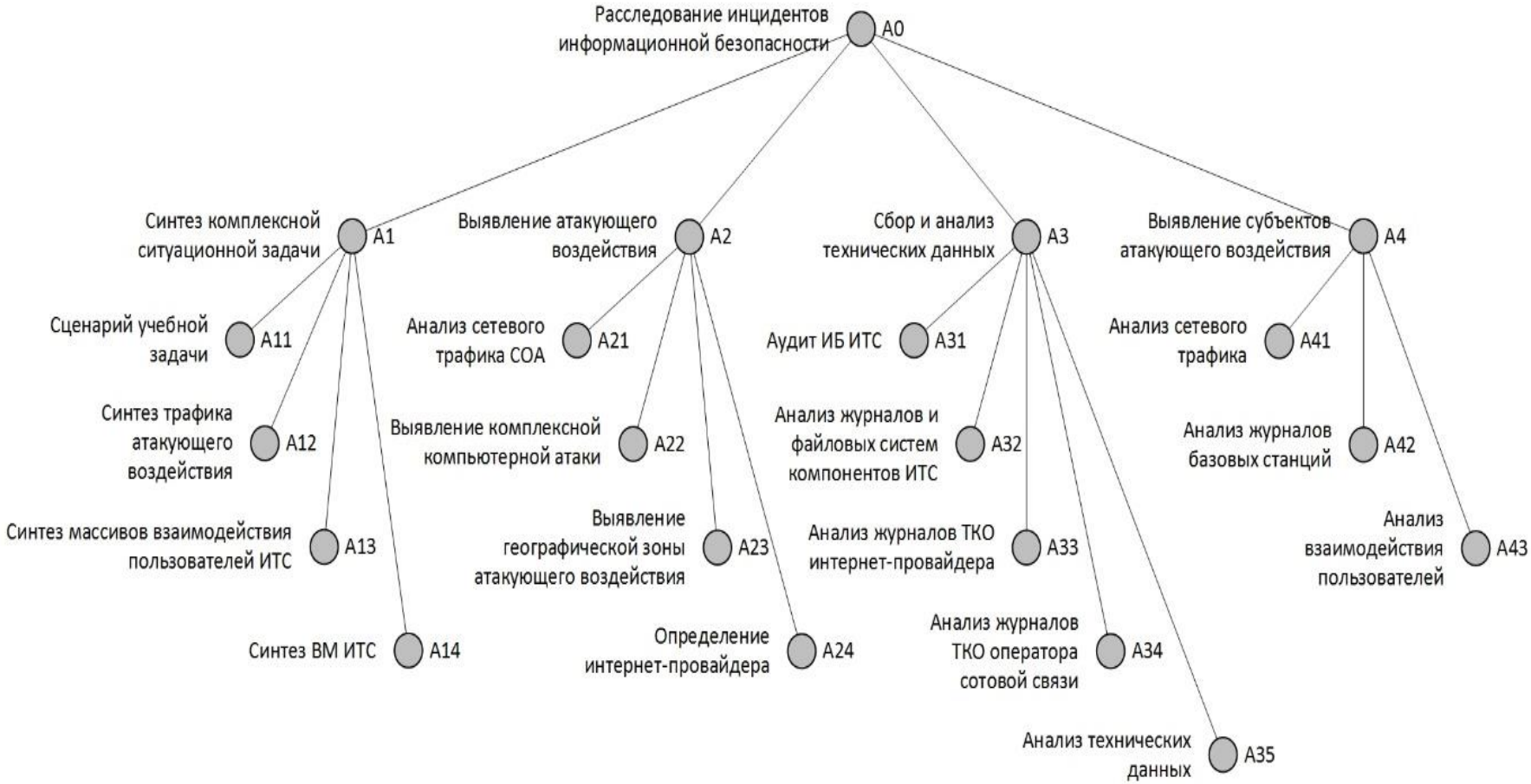

Рисунок 4.2. Схема дерева узлов АОС киберполигона по расследованию инцидентов информационной безопасности

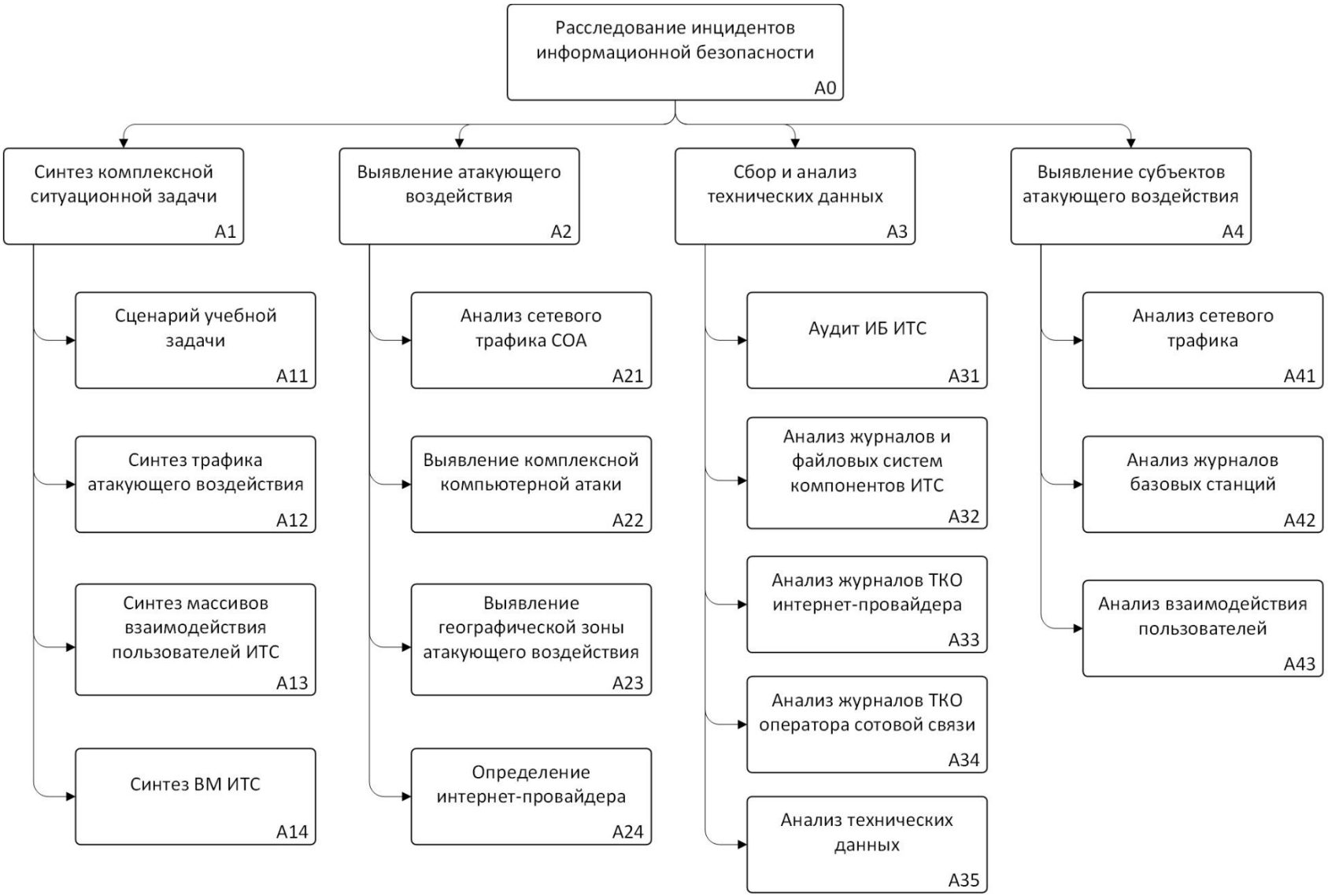

Рисунок 4.3. Концептуальная схема АОС киберполигона по расследованию инцидентов информационной безопасности

Рисунок 4.4. Схема А-0 АОС киберполигона по расследованию инцидентов информационной безопасности

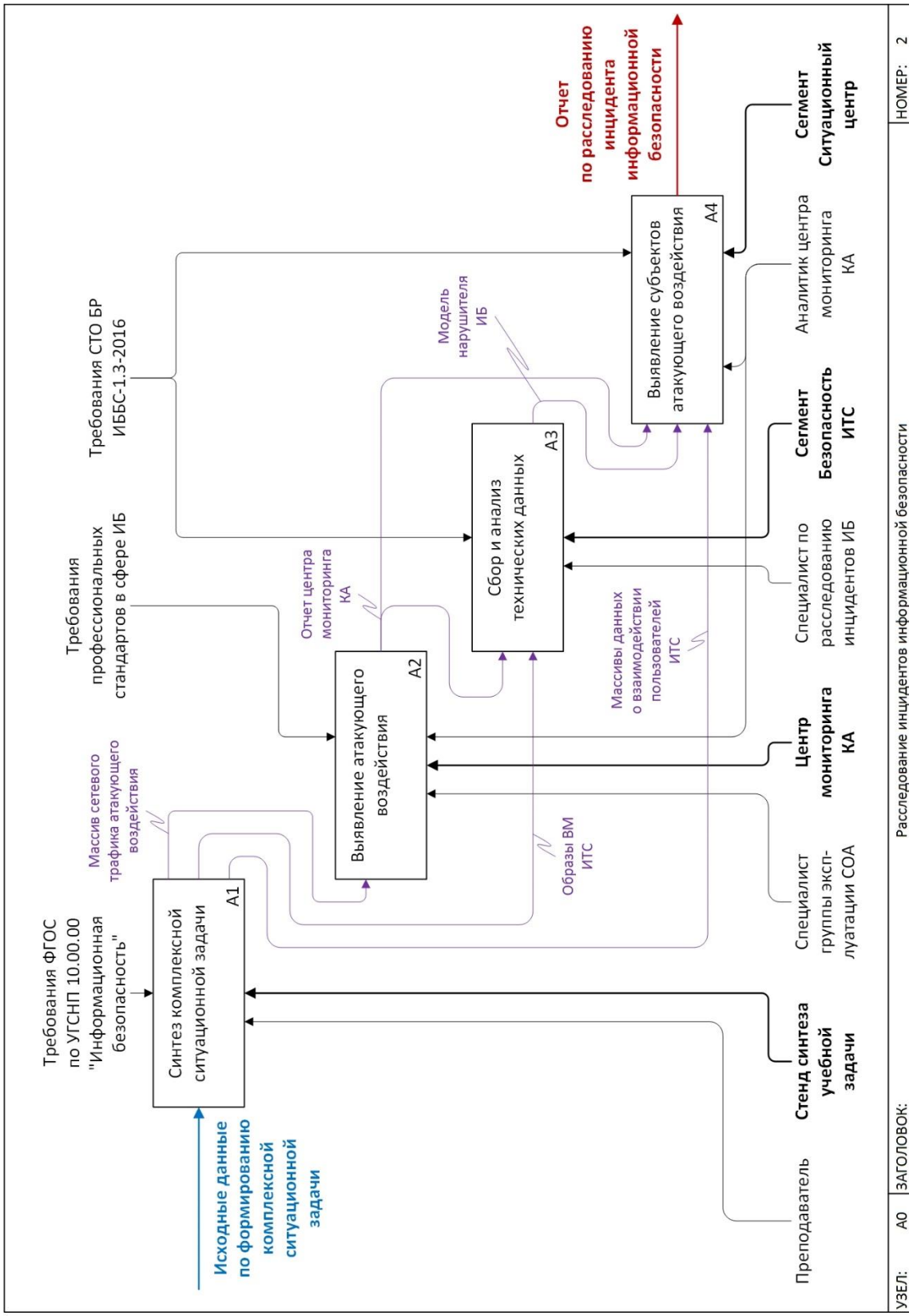

Рисунок 4.5. Схема A0 основных процессов

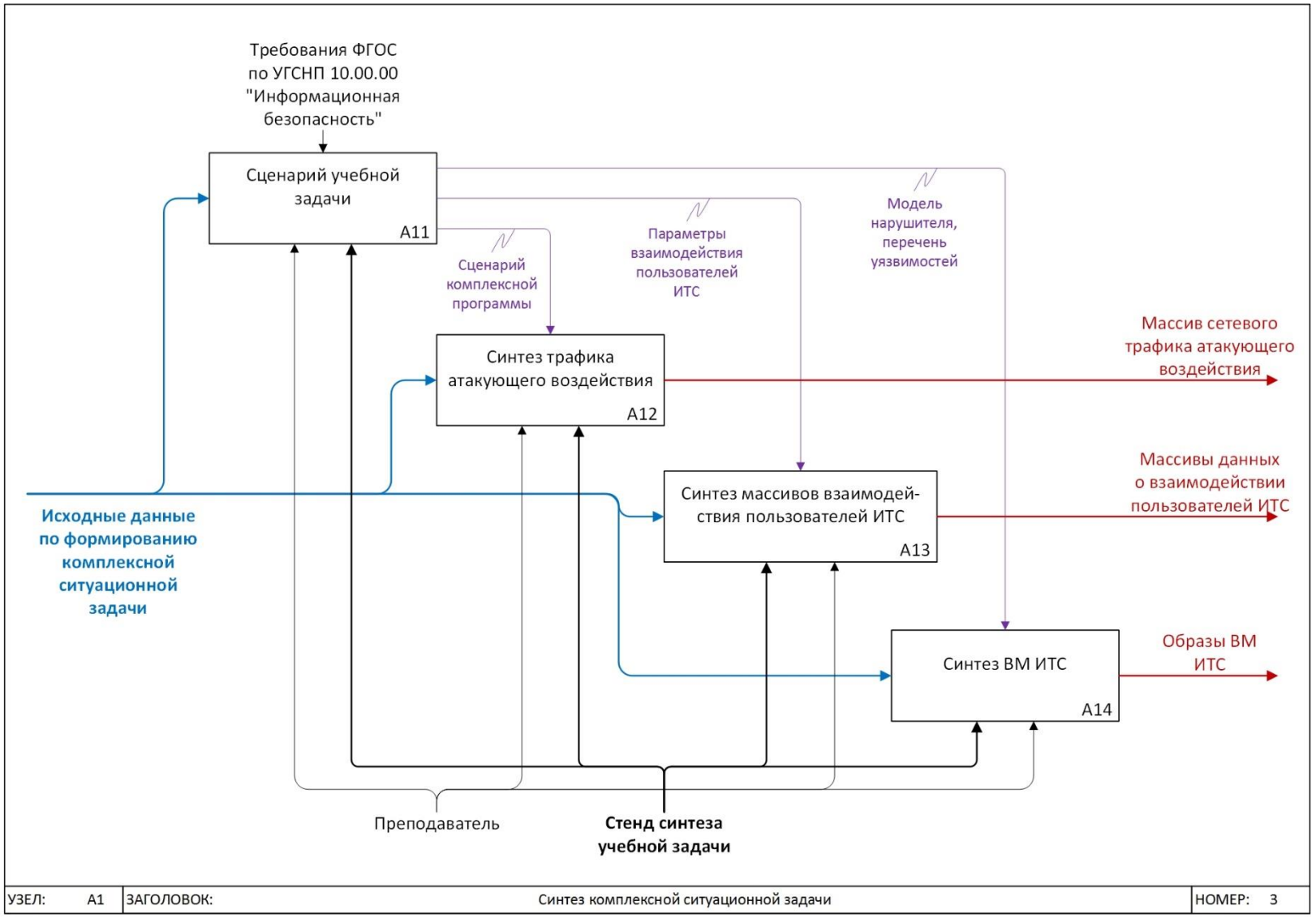

Рисунок 4.6. Схема процесса синтеза комплексной ситуационной задачи

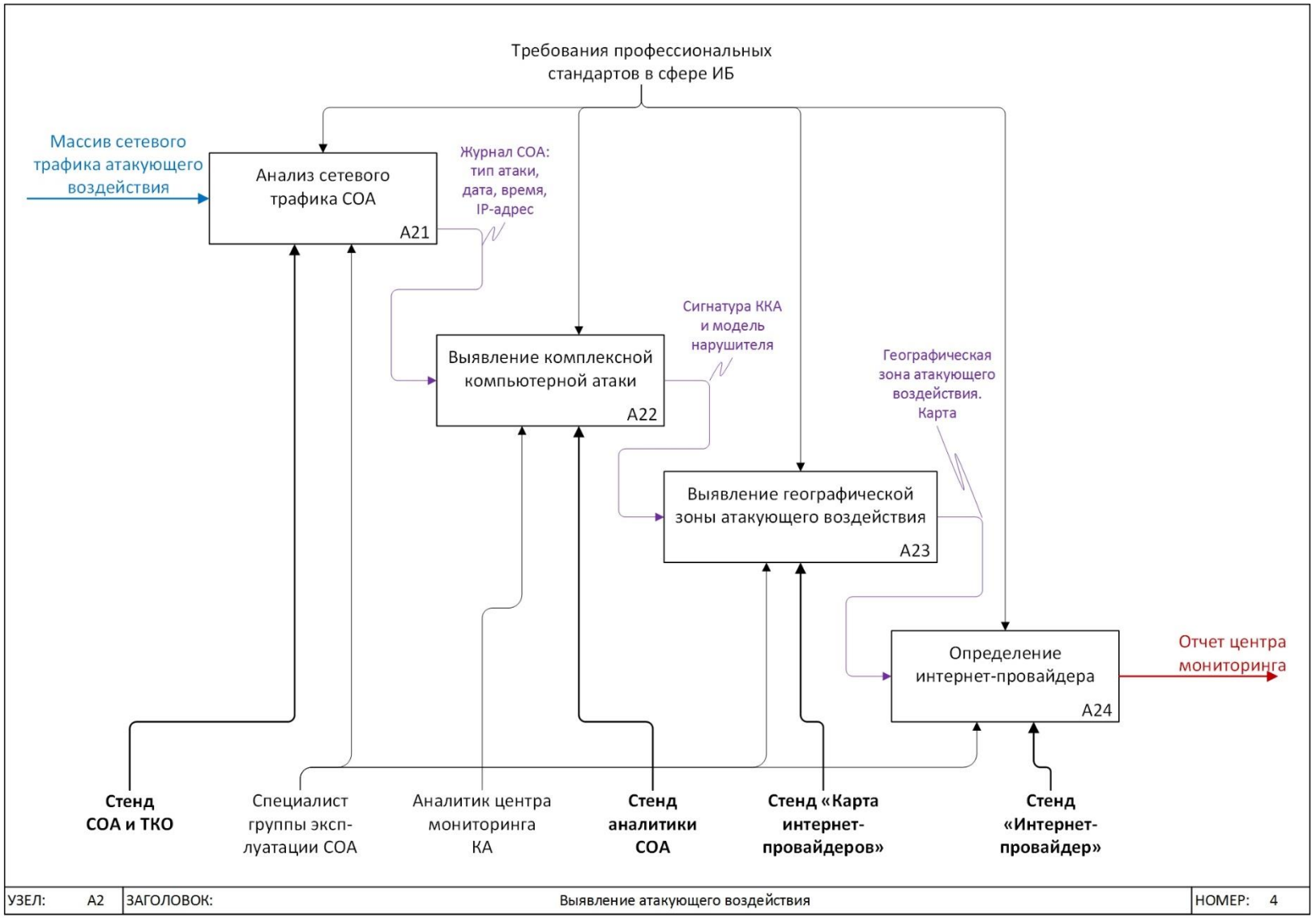

Рисунок 4.7. Схема процесса выявления атакующего воздействия

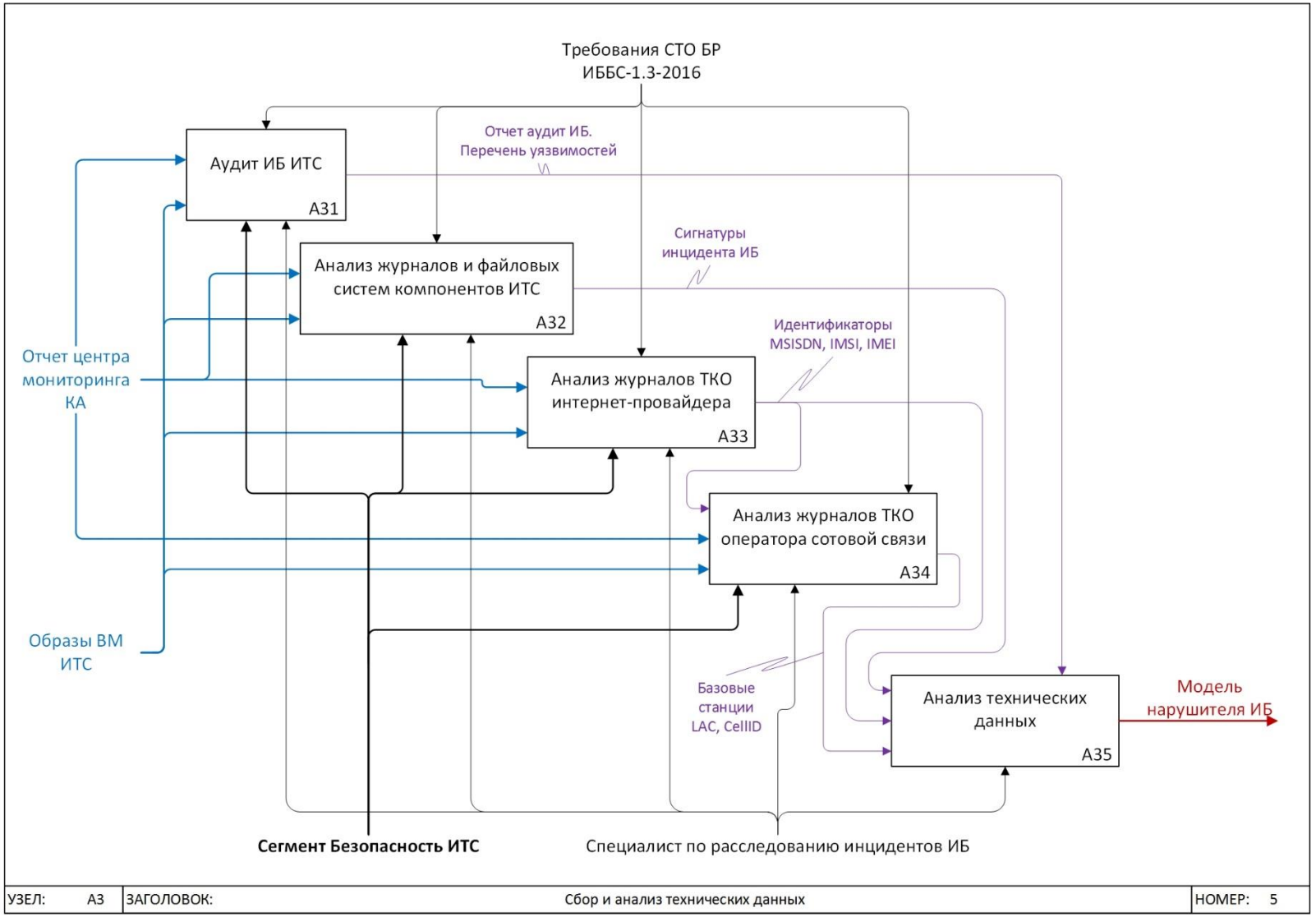

Рисунок 4.8. Схема процесса сбора и анализа технических данных

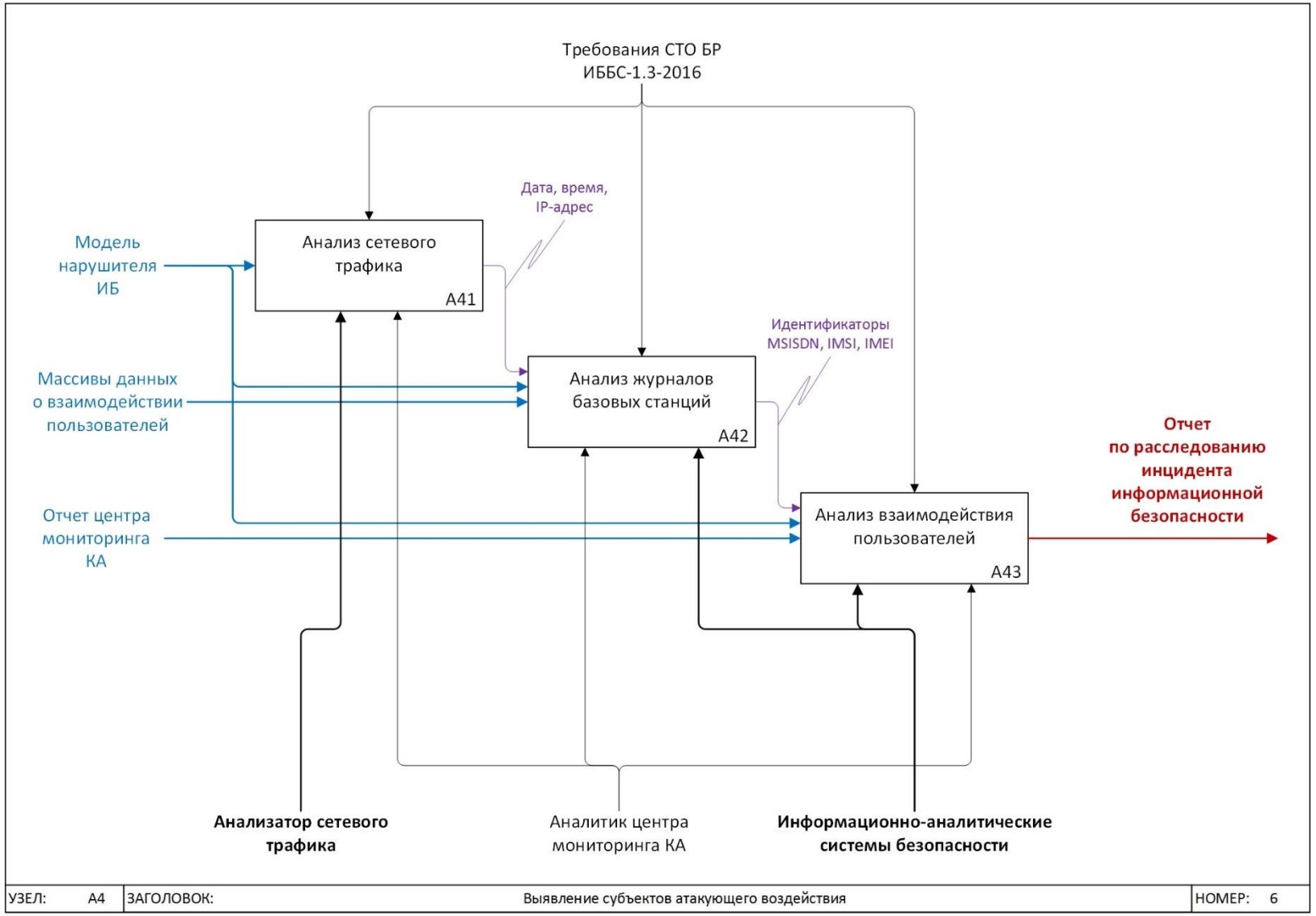

Рисунок 4.9. Схема процесса выявления субъекта атакующего воздействия

4.1.3. Функциональная и организационная структура АОС

Информационные ресурсы АОС представляют собой децентрализованное хранилище, состоящее из ряда баз данных (далее — БД), предназначенных для хранения статистических характеристик сетевых сред функционирования ССЗИ, массивов сетевого трафика компьютерных атак, типовых сценариев атакующего воздействия и вспомогательных баз данных, образы операционных систем и приложений и средства общего и специального программного обеспечения: система управления учебными курсами Moodle, система виртуализации VMWare; генераторы атакующего воздействия, фонового сетевого трафика, массивов информации о взаимодействии пользователей ИТС.

Организационная структура, обеспечивающая функционирование АОС, включает в себя пользователей, состоящих из двух категорий — преподавателей и студентов, и администраторов АОС, основной задачей которых является поддержание ее работоспособности. Пользователями АОС являются преподаватели, ведущие соответствующие занятия и проводящие учения, и студенты, проходящие обучение по направлению «Информационная безопасность». Обеспечение штатного функционирования АОС возлагается на администраторов, которые отвечают за резервирование данных и поддержание работоспособности технического и программного обеспечения.

В основе разработки АОС лежат следующие принципы:

— использование стандартного программного обеспечения, преимущественно российского производства;

— использование общепризнанных и широко распространенных стандартов структурирования информации;

— высокая степень масштабируемости программных средств;

— использование платформенно-независимого программного обеспечения для хранения, обработки и представления информации.

В соответствии с вышеперечисленными принципами разработки АОС создана в среде операционной системы Astra Linux с применением технологии виртуализации.

4.1.4. Модели синтеза условно-реальных данных для ситуационной задачи по расследованию инцидента информационной безопасности

Компьютерный полигон по расследованию инцидентов информационной безопасности — это совокупность программно-аппаратных средств, которые предназначены для анализа событий, зафиксированных различными техническими средствами. Следовательно, необходим комплексный подход к формированию модели инцидента ИБ с учетом действий нарушителей ИБ во временном, пространственном, а также информационном аспектах.

Таким образом, ситуационная задача для расследования инцидента ИБ должна формироваться совокупностью моделей сетевых сред:

1. Модель сетевой среды синтеза компьютерной атаки;
2. Модель сетевой среды синтеза биллинговой информации;
3. Модель сетевой среды синтеза взаимодействия пользователей в социальных сетях.

Синтез сетевой среды компьютерной атаки представляет собой совокупность этапов:

1. Синтез фонового сетевого трафика;
2. Синтез сценария комплексной компьютерной атаки;
3. Визуализация IP-адреса, его привязка к провайдеру и географическому месторасположению.

Синтезируемый массив сетевого трафика описывается множеством записей $T=\{t_i\}_{i=1}^{n_t}= T_s \cup T_b$, где *Ts* – трафик компьютерной атаки, *Tb* – фоновый трафик, *ti* – элемент массива (строка), описывающий поток данных в сети, *nt* — общее количество строк, строка *ti* имеет вид $t_i \in T = \{id, Time, IP\_A, IP\_B, data\}$,где *id* — идентификатор учетной записи пользователя (номер IMSI), *Time* — временная метка, *IP_A* — IP-адрес отправителя, *IP_B* — IP-адрес получателя, *data* – сведения об атакующем воздействии.

Потенциально вредоносную активность в трафике должна фиксировать СОА, которая будет опираться на массив правил $R=\{r_i\}_{i=1}^{n_r}$, где r_i – правило для проверки сигнатур трафика, протоколов и аномалий, n_r — общее

количество правил.

Структура правила r_i имеет следующий вид:

$$r_i \in R = \{Action, Protocol, Source\_address, Source\_port, Direction, Destination\_address, Destination\_port, Rule\_option\},$$

где *Action* — действие правила, которое может генерировать предупреждение, передавать информацию в журнал, протоколировать пакет без предупреждений, игнорировать пакеты, генерировать предупреждение, после чего включать динамическое правило;

Protocol — протокол передачи данных, например, TCP, UDP, ICMP, IP;

Source_address — IP-адрес источника потока данных или диапазон IP-адресов;

Source_port — номер порта или диапазон портов источника;

Direction – оператор направления трафика, который явно указывает источника и получателя;

Destination_address — IP-адрес получателя данных;

Destination_port — номер порта или диапазон портов получателя;

Rule_option — опции правила.

После выполнения сценария компьютерной атаки в журнале СОА фиксируется протокол событий. Расследование инцидента ИБ начинается с исследования журнала СОА, результатом являются IP-адрес источника и время атаки.

Следующий этап — определение принадлежности IP-адреса к Интернет-провайдеру и получение установочных данных лица, на которого оформлен договор об оказании услуг связи (при их наличии). Производится анализ журналов серверов авторизации RADIUS.

Структура записи u_i о пользователе в базе данных оператора связи U имеет следующий вид:

$$u_i \in U = \{id, Contact, Address, Username, Password\},$$

где *id* — уникальный номер пользователя в базе данных оператора связи;

Contact — фамилия, имя, отчество, дата рождения и прочие паспортные данные пользователя;

Address — адрес фактического места жительства;

Username, Password — данные пользователя для авторизации в сети провайдера.

После получения полной информации от оператора расследование инцидента ИБ, осуществляется путем анализа массивов биллинга сотовой связи, где нарушитель мог оставить свои следы при подключении к базовым станциям, а также путем анализа изображений с видеокамер наружного наблюдения, в объектив которых мог попасть нарушитель.

Синтез учебных массивов условно-реальных данных биллинговой информации осуществляется с использованием разработанного ПО «Программное обеспечение синтеза массивов данных для стенда тестирования информационно-аналитических систем безопасности» [273], в котором применена пространственно-временная статистико-событийная модель синтеза биллинговой информации (рисунок 4.10).

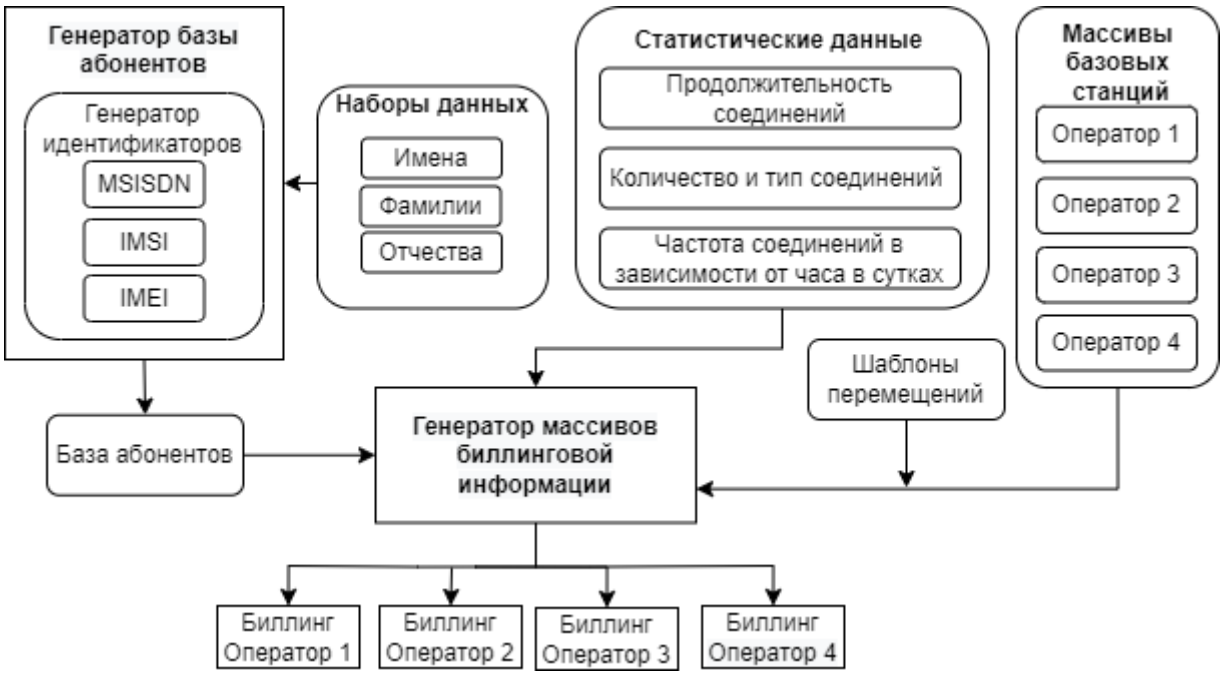

Рисунок 4.10. Схема синтеза массивов биллинговой информации

При синтезе фонового массива биллинговой информации используются абонентская база, созданная ранее, файл с LAC и CellID базовых станций выбранной местности, статистические распределения видов событий

по времени и продолжительности, распределение количества звонков по дням недели, заранее сгенерированный массив ситуационного биллинга, шаблоны перемещений для создания динамики подключения абонентов к базовым станциям при перемещении в рамках имитируемого населенного пункта (рисунок 4.11).

По результатам выявления идентификационных данных нарушителя в массиве биллинговой информации осуществляется анализ сведений о взаимодействии пользователей в социальных сетях.

Рисунок 4.11. Схема синтеза массивов биллинговой информации

Модель сетевой среды синтеза взаимодействия пользователей в социальных сетях основана на создании популяции виртуальных пользователей, являющихся группой участников социального Интернет-сообщества, зарегистрированных на одном Интернет-ресурсе и взаимодействующих путем передачи через стационарные и мобильные терминалы двух типов коммуникационных событий: открытые публикации с возможностью их оценки другими пользователями и приватные (диалоговые) сообщения (рисунок 4.12).

Рисунок 4.12. Схема синтеза массивов данных о взаимодействии пользователей в социальных сетях

Один типовой пользователь социальной сети обладает уникальным идентификатором Интернет-сообщества (UID), статическим IP-адресом при работе через стационарные терминалы или IP-адресом оператора сотовой связи при передаче данных через мобильные терминалы, логином Интернет-соединения. Структура синтезируемых массивов условно-реальных позволяет корректно отображать в ИАСБ взаимодействие пользователей в соответствующем ИТ-сервисе.

Таким образом, представленный комплекс моделей сетевых сред позволяет в рамках компьютерного полигона по расследованию инцидентов ИБ формировать ситуационную задачу для расследования учебных инцидентов ИБ и тестирования аналитических методик ИАСБ.

4.1.5. Алгоритм анализа взаимодействия пользователей сетей операторов сотовой связи на основе теоретико-графового подхода

С целью тестирования аналитических методик и выявления взаимодействия пользователей в ИТС, в том числе в сетях операторов сотовой связи применен алгоритм, основанный на ранее разработанном теоретико-графовом подходе к задачам количественного анализа защиты информации в компьютерных системах [254].

Алгоритм предназначен для анализа биллинговой информации и выявления сеансов работы выбранного объекта (пользователя) при «глубине» взаимодействия более двух. Где под «глубиной» взаимодействия понимается опосредованная связь абонента с абонентами, связанными прямыми соединениями с теми абонентами, с которыми у анализируемого абонента было непосредственное соединение. Если «глубина» взаимодействия равная одному формируется путем простого анализа биллинга на вхождение строк (записей), то для выявления связей «глубиной» более двух требуется применение аналитических алгоритмов, один из которых возможен на основе указанного выше теоретико-графового подхода.

Задача решается путем построения ориентированного социального графа (см. п. 2.4.1), характеризующего взаимодействие пользователей, $G = (U, E)$, где U — множество вершин графа; E — множество ребер графа; $|U|=N$ — количество вершин в графе, $|E|=L$ — число связей (ребер). Социальный граф G задается матрицей смежности A размера $N \times N$, где N — число участников сети, e_{ij} — элемент матрицы, показывающий наличие или отсутствие взаимосвязи между участниками u_i и u_j. Анализируемый абонент — пользователь $u_x(G) \in U$: $u_x(G) = \{O(G, u_x(G)), Atr(u_x(G))\}$.

Значимые атрибуты учетной записи u_x пользователя в сети сотовой связи (граф G_M): $IMSI(u_x(G_M))$ — номер SIM-карты, $IMEI(u_x(G_M))$ — IMEI (номер аппарата), $MSISDN(u_x(G_M))$ — MSISDN (номер телефона), $surname(u_x(G_M))$, $name(u_x(G_M))$, $secname(u_x(G_M))$ — фамилия, имя и отчество пользователя. Атрибуты строятся на основании запросов к базе данных, со-

держащих биллинговую информацию, и базе данных принадлежности номеров IMSI физическим лицам.

Ребро графа e_{ij} является направленным и взвешенным. Направление ребра характеризует направление информационного взаимодействия между пользователями u_i и u_j. Вес ребра — кортеж, определяющий количество взаимодействий (звонков – входящих или исходящих, сообщений) по каждому фиксируемому типу информационного взаимодействия (звонок, SMS-сообщение и т.п.).

Структурные атрибуты, представляющие систему взаимоотношений между пользователями ИТС, описываются как окрестность[1] $O(G, u_x(G))$ вершины социального графа. Тогда решение задачи состоит в формировании окрестности $O(G, u_x(G))$ вершины $u_x(G)$.

Алгоритм формирования окрестности $O(G, u_x(G))$ состоит из следующих этапов:

1. Выделяется атрибут $MSISDN(u_x(G_M))$ анализируемого абонента $u_x(G)$.

2. Осуществляется выборка из базы биллинговой информации по атрибуту $IMSI(u_x(G_M))$, соответствующему искомому $MSISDN(u_x(G_M))$, всех записей в отдельную базу данных непосредственных соединений абонента $u_x(G)$.

3. Формируется матрица смежности M_x для окрестности $O(G, u_x(G))$, в строках и столбцах матрицы формируются вершины (имеющие смысл абонентов сети, с которыми у анализируемого абонента было установлено непосредственное взаимодействие). В строках формируются абоненты — источники соединения, в столбцах — абоненты — получатели соединения. В ячейках матрицы формируются значения ребер e_{ij}. Матрица смежности не симметрична, формируется построчно, ребро формируется при наличии соединения от источника к получателю, в значении ребра накапливается количество соединений соответствующего типа.

[1] ***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.

4. Выделяется очередной абонент, соединение с которым зафиксировано в матрице смежности, — $u_i(G)$. По его атрибуту $MSISDN(u_i(G_M))$ осуществляется выборка из базы биллинговой информации записей в базу данных непосредственных соединений абонента $u_i(G)$.

5. В единую матрицу смежности M_x дополняются вершины графа $O(G, u_i(G))$ и формируются ребра e_{ij} с учетом направления, типа и количества соединений.

6. Алгоритм проходит все вершины окрестности $O(G, u_x(G))$, этапы 4 и 5 повторяются по всем вершинам окрестности $O(G, u_x(G))$.

7. Алгоритм продолжает работу для вершин $u_i(G)$, повторяются этапы 4 – 6. Алгоритм завершает работу при достижении задаваемой глубины

8. Применяются матричные операции, подробно описанные в [254], позволяющие сформировать цепочки опосредованного взаимодействия абонента $u_x(G)$.

9. Осуществляется визуализация сформированного графа, описываемого матрицей смежности M_x.

Визуализация основана на применении различных раскладок ориентированных графов. При визуализации ребра графа формируются вес (толщина линии на изображении) и направление, вершины снабжаются дополнительной информацией из атрибутов учетных записей u_i. Визуализация реализуется с помощью библиотек программы GraphVisualizer [298].

Таким образом, предложенный алгоритм выявления взаимодействия пользователей сетей операторов сотовой связи на основе ранее опубликованного теоретико-графового подхода к задачам количественного анализа защиты информации в компьютерных системах позволяет осуществлять эффективную программную реализацию в целях тестирования аналитических методик и анализа массивов биллинговой информации.

4.2. *Учебно-научный компьютерный полигон*

4.2.1. Образовательные задачи, требующие моделирования сетевой среды, и их решение в рамках учебно-научного компьютерного полигона

Ситуационные задачи (тестовые массивы) обеспечивают комплексность формирования профессиональных компетенций специалистов по УГСНП «Информационная безопасность» с поэтапным решением задач:

- обнаружение комплексной КА и выявление источников атаки,
- выявление уязвимостей, способствовавших реализации КА,
- проведение мероприятий по реагированию на КИ,
- сбор информации с технических средств для расследования КИ,
- назначение и проведение компьютерных экспертиз и исследований,
- выявление субъектов КА (инициаторов и исполнителей) на основе анализа взаимодействия пользователей в сетях связи.

Современные ССЗИ — сложные многокомпонентные решения, предназначенные для использования в сетях со сложной конфигурацией. Для полноценной работы ССЗИ кроме сетевой инфраструктуры требуется и информационное наполнение учебных стендов, в том числе имитация работы многочисленных пользователей системы, а также нарушителей информационной безопасности.

Для проведения исследований в составе полигона разработаны учебно-экспериментальные стенды, оснащенные как программными, так и программно-аппаратными комплексами ССЗИ. Стенды оснащены генераторами фоновых массивов данных (сетевого трафика) и генераторами ситуационных (тестовых) задач. Основной особенностью разработанных стендов является их мобильность, основанная на применении технологии виртуальных машин (далее — ВМ).

В рамках дисциплин «Программно-аппаратные средства обеспечения информационной безопасности» и «Основы проектирования защищенных телекоммуникационных систем» проводятся занятия по таким темам как:

- изучение ТКО (маршрутизаторов и межсетевых экранов);

— изучение СОА;

— построение инфраструктуры сети провайдера Интернет;

— моделирование угроз безопасности в АСУ ТП;

— применение ИАСБ для анализа биллинговой информации при расследовании инцидентов ИБ;

— учения по информационной безопасности в формате CTF.

Каждый вид занятий требует имитации работы в ИТС, также, как и при тестировании рассматриваются две конфигурации — фоновые массивы и атакующие (ситуационные) массивы. Фоновые массивы содержат так называемый «нормальный» сетевой трафик (биллинг), который должен соответствовать массивам реальных сетей. Атакующие (ситуационные) массивы содержат задачу для решения обучающимися.

Для методического обеспечения образовательного процесса по тематике ССЗИ разработан и используется в составе полигона по расследованию инцидентов ИБ ряд учебных пособий: «Системы обнаружения компьютерных атак» [302], Аудит информационной безопасности компьютерных систем [303], «Защита информации в компьютерных сетях. Практический курс» [301], «Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс» [304] и электронных учебно-методических комплексов (УМК): «Методы и средства защиты компьютерной информации» [305], «Защита информации в компьютерных сетях» [306], «Специализированные программно-аппаратные средства защиты информации» [307].

Таким образом, разработанные учебно-экспериментальные стенды и соответствующее методическое обеспечение, развернутые в составе компьютерного полигона по расследованию инцидентов ИБ, позволяют проводить лабораторные работы и практические занятия и имитировать при этом ИТС различного масштаба.

4.2.2. Структура учебно-научного компьютерного полигона по расследованию инцидентов информационной безопасности

Учебно-научный компьютерный полигон (киберполигон) по расследованию инцидентов информационной безопасности (рисунок 5.6) является совокупностью сегментов, объединенных в единую информационную систему, представленных соответствующими стендами, каналами связи и вычислительными ресурсами.

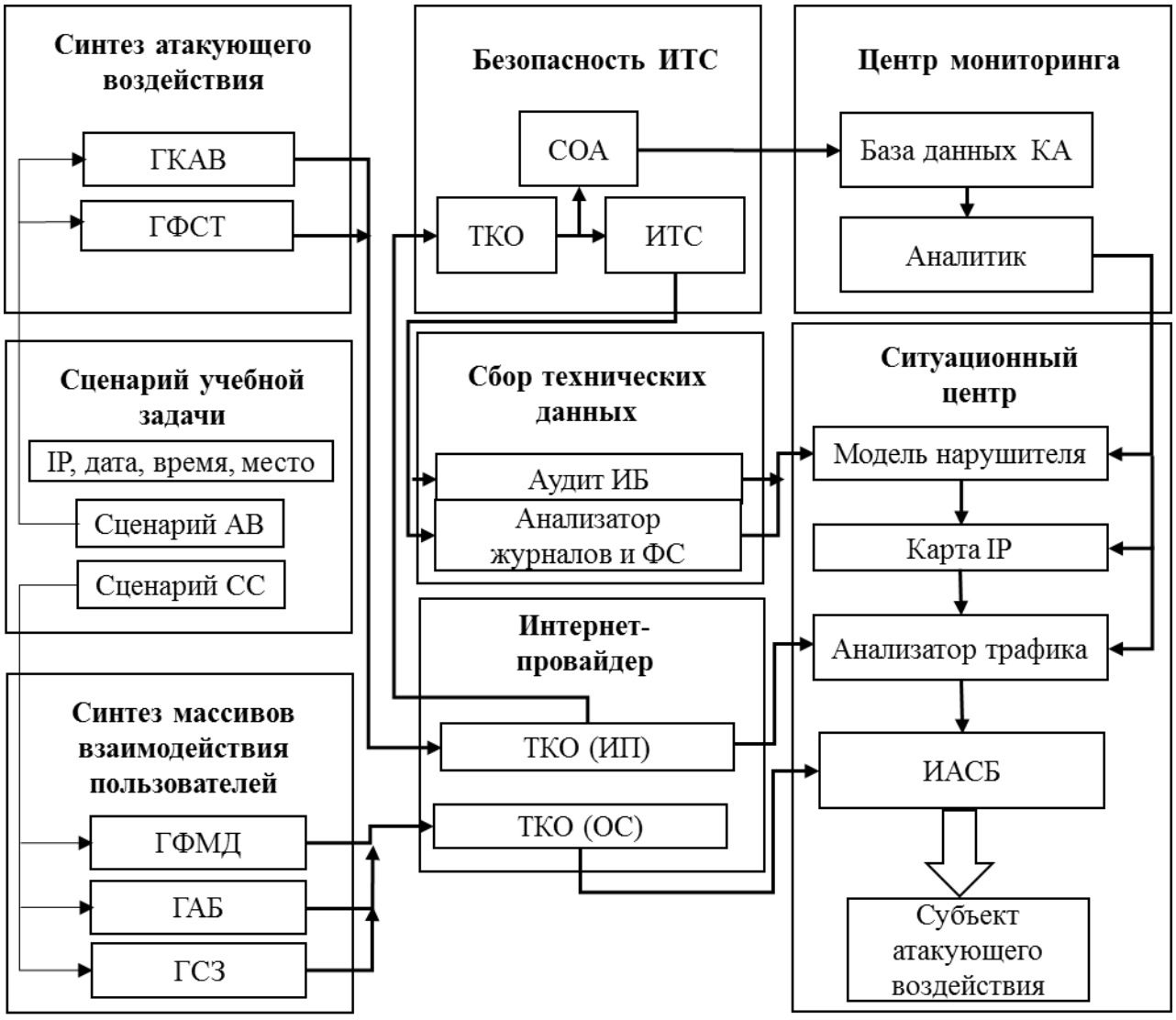

Рисунок 4.13. Схема информационного взаимодействия сегментов киберполигона по расследованию инцидентов ИБ

Полигон состоит из следующих сегментов, объединенных в единую информационную систему, включающую в свой состав автоматизированную обучающую систему: «Синтез атакующего воздействия», «Безопасность ИТС», «Центр мониторинга», «Ситуационный центр», «Сбор технических данных», «Интернет-провайдер (оператор связи)», «Синтез массивов взаимодействия пользователей» и «Сценарий учебной задачи».

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). Дополнительно сегмент служит для формирования сетевой среды при проведении занятий в виде киберучений в формате «захват флага». Из рассматриваемого сегмента в сетевую инфраструктуру полигона поступает совокупность массивов сгенерированного 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, содержит ряд стендов, имитирующих ИТС и ИС различного назначения. Основными элементами сегмента «Безопасность ИТС» являются сенсор системы обнаружения атак (СОА) и телекоммуникационное оборудование (ТКО), устанавливаемые в ИТС.

На базе сегмента «Безопасность ИТС» выполняются практические задания по проведению аудита информационной безопасности (блок «Аудит ИБ»). При анализе защищенности ИТС и ИС производится подключение средств анализа защищенности (САЗ) к элементам ИТС с целью выявления потенциальных возможностей внешнего и внутреннего нарушителей и построения модели нарушителя и графов атак. Уязвимые системы имитируются на стенде тестирования САЗ.

Результатом работы узлов сегмента «Безопасность ИТС», помимо выявленных уязвимостей узлов ИТС в рамках аудита ИБ, являются записи

об атакующем воздействии, которые генерируются сенсорами СОА и поступают для дальнейшего анализа в сегмент «Центр мониторинга».

Сегмент «Сбор технических данных» представляет совокупность образов дисков операционных систем 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 (КА), 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.

Результаты работы сегмента передаются в «Ситуационный центр», сюда поступают аналитические данные по обнаруженным атакам, территориальная принадлежность IP-адресов атакующего воздействия и атакуемых ИТС и ИС.

Сегмент «Ситуационный центр» предназначен для визуализации хода проведения мероприятий по расследованию инцидентов информационной безопасности в рамках взаимодействия руководителей, аналитиков и технических специалистов. На вход в сегмент поступает информация:

– из сегмента «Безопасность ИТС» — результаты проведения мероприятий по оценке защищенности ИТС и ИС;

– из сегмента «Центр мониторинга» — результаты анализа комплексного атакующего воздействия, выявленные IP-адреса атакующих и атакованных ИТС, территориальная и юридическая принадлежность IP-адресов к провайдерам сети Интернет.

– из сегмента «Интернет-провайдер» — результаты анализа сетевого трафика по IP-адресам, а также результаты анализа информации о взаимодействии пользователей в сетях операторов сотовой связи и социальных сетей.

Сегмент «Ситуационный центр» предназначен для выявления субъектов (источников) атакующего воздействия, включает информационно-аналитические системы безопасности (ИАСБ) — комплексы анализа информации о взаимодействии пользователей в сетях операторов сотовой связи и социальных сетей.

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 телекоммуникационном оборудовании, и сведения о них. Результаты анализа трафика контролируемых IP-адресов объектов ИТС и анализа информации о взаимодействии субъектов атакующего воздействия передаются в «Ситуационный центр».

Сегмент «Синтез массивов взаимодействия пользователей» предназначен для генерации массивов данных о взаимодействии пользователей в ИТС, в том числе о взаимодействии в сетях операторов сотовой связи и в социальных сетях. Сегмент состоит из генератора фоновых массивов 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 «Синтез массивов взаимодействия пользователей» в виде файлов, предназначенных для загрузки в ИАСБ, поступают сгенерированные массивы биллинговой информации и массивы баз 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 информационной безопасности. Сценарий учебной задачи определяет совокупность условий для генерации массивов данных, объединенных единым замыслом.

В блоке синтеза сценария учебной задачи формируется общая сценарная схема учений по информационной безопасности, в основе которой лежит единый сценарный план, предполагающий единые цели атакующих, единый диапазон IP-адресов, единый временной интервал и единую территориальную зону, учитываемые как при синтезе IP-трафика (сценарий АВ), так и при формировании массивов биллинговой информации о взаимодействии в сетях операторов связи и в социальных сетях (сценарий СС).

Для размещения сегментов предложенного киберполигона используется лабораторный фонд 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), условно состоящий из двух модулей: «Полигон обнаружения компьютерных атак» и «Центр расследования инцидентов».

Модуль «Полигон обнаружения компьютерных атак», развернутый на лабораторной базе УНЦ ИБ, включает сегменты «Синтез атакующего воздействия», «Безопасность ИТС» и «Центр мониторинга».

В состав типового объекта ИТС, имитируемого сегментом «Безопасность ИТС», входят блоки корпоративной сети предприятия, включая элементы автоматизированной системы управления технологическими процессами (АСУ ТП), отделенные от сети Интернет телекоммуникационным оборудованием с установленными сенсорами систем обнаружения атак, системами управления информацией и событиями безопасности (SIEM) и системами предотвращения утечки данных (DLP), управляемыми центром обеспечения безопасности (SOC). Также типовым решением для объекта ИТС является наличие демилитаризованной зоны (ДМЗ), содержащей серверные приложения и центр обработки данных (ЦОД), доступные удаленным пользователям через VPN-соединение. В сегменте также развернуто телекоммуникационное оборудование и сенсор СОА (рисунок 4.14).

Особенностью сегмента «Безопасность ИТС» является его вариативность, которая обеспечивается применением технологии виртуальных машин,

позволяющей использовать различные операционные системы и приложения, с одной стороны, и решением студентами отдельной задачи по созданию собственного объекта ИТС, обладающего необходимым комплексом защитных компонентов. В рамках курса «Программно-аппаратные средства обеспечения информационной безопасности» реализуется проект по модулю «Оборудование и эксплуатация функциональных защищенных систем», где основной задачей, решаемой студентами в подгруппах, является создание сетевой инфраструктуры объекта ИТС на основе различных сетевых информационных технологий, операционных систем, серверных приложений и средств защиты информации, в том числе различных СОА. При этом изучаются вопросы внедрения сенсоров СОА в состав ИТС, их развертывания и эксплуатации. Результатом проекта по модулю является развертывание студентами в составе сегмента «Безопасность ИТС» различных по применяемым средствам вариантов ИТС, обычно каждый вариант включает до десяти образов виртуальных машин. Одним из обязательных элементов системы защиты является СОА, которая выбирается студентами из доступного перечня, включающего как свободно распространяемые системы, такие как Snort и Suricata, так и поставляемые разработчиками, такие как DATAPK от компании СайберЛимфа, ViPNet IDS от компании ИнфоТеКС и иные.

Дополнительно в составе сегмента развернуты стенды «Безопасность АСУ ТП» и «Информационная система в защищенном исполнении». В качестве одного из сенсоров СОА развернуты сенсоры разработанной СОА AGATA.

Физически сегмент «Безопасность ИТС» представляет собой ряд серверов, объединенных в серверные стойки и ТКО и сенсорами СОА, а также АРМ администраторов имитируемых ИТС и ИС (рисунок 4.15).

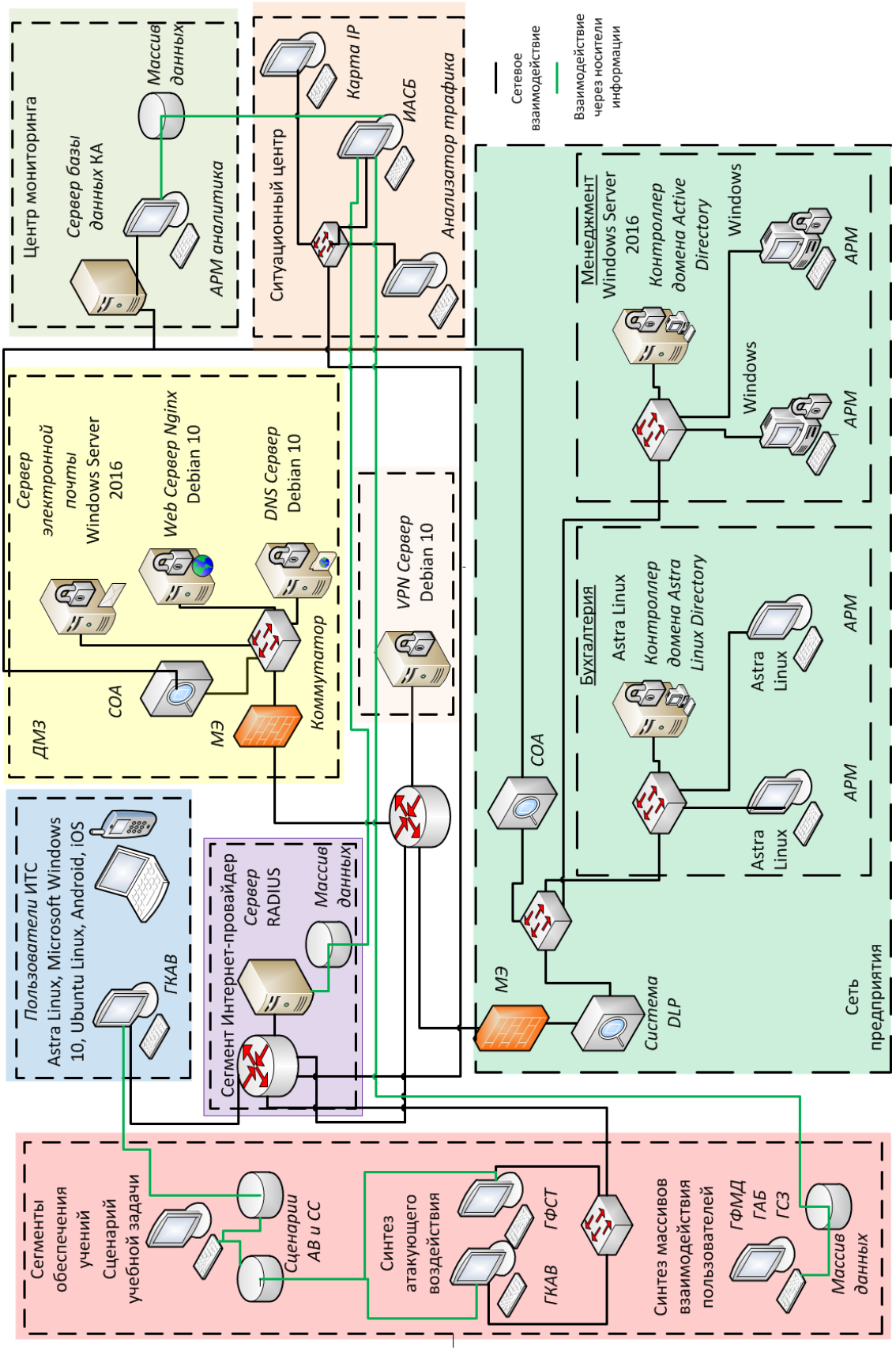

Рисунок 4.14. Основные компоненты киберполигона

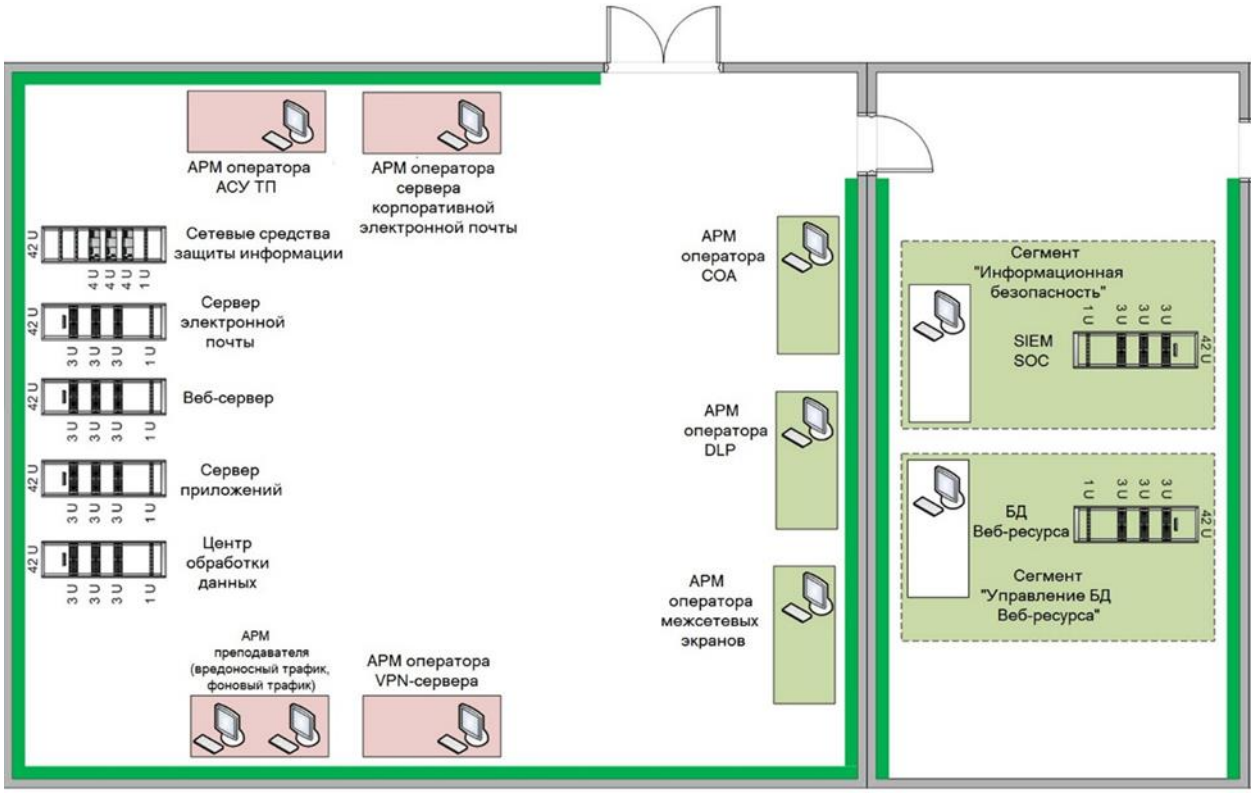

Рисунок 4.15. Расположение объектов сегмента «Безопасность ИТС» модуля «Полигон обнаружения компьютерных атак»

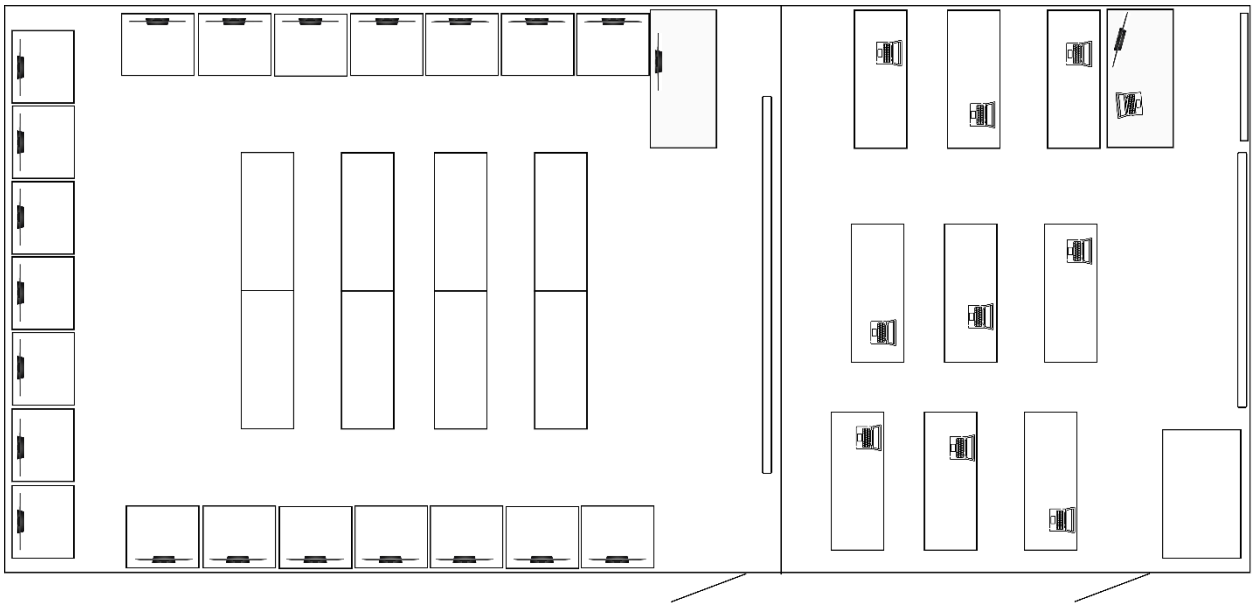

Рисунок 4.16. Расположение объектов компьютерного полигона на базе компьютерного класса (слева) и лаборатории (справа)

Сегмент «Синтез атакующего воздействия» построен на основе разработанных программных средств, реализующих функционал генераторов ком-

плексного атакующего воздействия и фонового сетевого трафика. «Программный комплекс нагрузочного тестирования систем обнаружения компьютерных атак с применением генетического алгоритма» [274] и «Программный комплекс синтеза массивов данных для стенда тестирования телекоммуникационного оборудования» [275] 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. Формирование оптимального набора характеристик для синтеза трафика обеспечивается применением генетического алгоритма. Комплексы позволяют генерировать вариативный сетевой трафик с интеграцией имитируемого атакующего воздействия в соответствии со сценарием учебной задачи.

Сегмент «Центр мониторинга» построен на базе технологии виртуализации и позволяет подключать различные аналитические системы, предназначенные для создания аналитических методик при обнаружении комплексных компьютерных атак. Выявление компьютерных атак осуществляется по базе данных компьютерных атак (БД КА), формируемой по результатам работы СОА. В рамках дисциплины «Основы проектирования защищенных телекоммуникационных систем» студентами решается задача по разработке собственной аналитической системы, позволяющей на основе событий безопасности, фиксируемых СОА, и совокупности статистических данных строить аналитические отчеты. В качестве базы применяются свободно распространяемые решения, такие как проект Security Onion и система визуализации журналов СОА Kibana.

Работа аналитика по разбору инцидентов ИБ и КА 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.

Результатами работы аналитической системы является совокупность IP-адресов источников атакующего воздействия с привязкой по территориальному признаку и принадлежности к провайдеру сети Интернет.

Результаты работы сегмента передаются в «Ситуационный центр»: аналитика по обнаруженным атакам, территориальная принадлежность IP-адресов атакующего воздействия и атакуемых ИТС и ИС.

Модуль «Центр расследования инцидентов» объединяет четыре описанных выше сегмента: «Ситуационный центр», «Интернет-провайдер (оператор связи)», «Синтез массивов взаимодействия пользователей» и «Сценарий учебной задачи».

Сегмент «Сценарий учебной задачи» позволяет преподавателю с помощью ряда интерфейсов сформировать сценарии комплексных учебных задач, задавая сценарий атакующего воздействия (территориальную принадлежность источников атаки, IP-адреса атакующих, сценарий атаки с временной детализацией), сценарии взаимодействия в сетях сотовой связи (временные параметры, совокупность базовых станций, идентификаторы сетей сотовой связи, виды и последовательность соединений) и в социальных сетях (идентификаторы социальных сетей, временные метки и типы взаимодействия). В блоке синтеза сценария учебной задачи формируется общая сценарная схема учений по информационной безопасности, в основе которой единый сценарный план, предполагающий единый диапазон IP-адресов, единый временной интервал и единую территориальную зону, учитываемые как при синтезе IP-трафика (сценарий АВ), так и при формировании массивов биллинговой информации при взаимодействии в сетях операторов связи и в социальных сетях (сценарий СС). Также в рамках ситуационной задачи разрабатываются единые цели атакующих, их реквизиты в сетях операторов сотовой связи и социальных сетях.

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 даль-

нейшего синтеза сетевого трафика, массивов биллинговой информации и журналов телекоммуникационного оборудования.

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» [273] реализует 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.

«Программное обеспечение синтеза массивов данных для стенда тестирования информационно-аналитических систем безопасности» [273] 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 Эрдёша-Реньи для задания начального распределения ребер социального графа, модель Барабаши-Альберт для формирования статической структуры сервиса социальных сетей.

Сегмент «Интернет-провайдер» имитирует результаты работы телекоммуникационного оборудования провайдеров услуг сети Интернет и операторов сетей сотовой связи в части формирования для дальнейшего анализа информации о подключении и взаимодействии абонентов. Включает, в том числе серверы аутентификации, авторизации и аудита (RADIUS-серверы), а также средства анализа сетевого трафика типа WireShark.

Сегмент «Ситуационный центр» является основным и завершающим цепочку расследования инцидента информационной безопасности. В основе

сегмента лежат ИАСБ типа IBM i2 и Lampyre и построители графов связей типа Gephi, в которые стекается информация из остальных сегментов. Путем анализа поступающей информации из «Центра мониторинга» формируются сведения о территориальной принадлежности атакующих, 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. В состав программного обеспечения сегмента включена программа анализа взаимодействия пользователей в сетях операторов сотовой связи, реализующая алгоритм, основанный на ранее разработанном теоретико-графовом подходе к задачам количественного анализа защиты информации в компьютерных системах.

Сегмент «Ситуационный центр» предназначен для визуализации хода проведения мероприятий по расследованию компьютерных инцидентов в рамках взаимодействия руководителей, аналитиков и технических специалистов, обеспечивающих расследование инцидента ИБ. На вход в сегмент поступает информация:

— из сегмента «Сбор технических данных» — результаты проведения аудита безопасности ИТС и ИС и анализа файловых систем компьютеров, подвергшихся атакующему воздействию;

— из сегмента «Центр мониторинга» — результаты анализа атакующего воздействия, выявленные IP-адреса атакующих и атакованных ИТС и ИС, территориальная и юридическая принадлежность IP-адресов к провайдерам сети Интернет для анализа и отображения на карте IP-адресов;

— из сегмента «Интернет-провайдер» — результаты анализа сетевого трафика по IP-адресам, выявленным в атакующем воздействии, а также результаты анализа информации о взаимодействии абонентов в сетях операторов сотовой связи и социальных сетей в соответствии с временной и территориальной зонами атакующего воздействия.

4.2.3. Единая ситуационная задача по проведению расследования инцидентов информационной безопасности

Единая ситуационная задача охватывает процедуры выявления уязвимостей ИТС, обнаружения компьютерных атак, а также реагирования и проведения расследования инцидентов ИБ.

Использование предложенного учебно-научного киберполигона по расследованию инцидентов информационной безопасности позволяет решить несколько задач, направленных на развитие у обучаемых практических навыков:

– тестирования наличия уязвимостей в ИТС и ИС в целом;

– выявления комплексного атакующего воздействия на ИТС и ИС;

– сбора и анализа технических данных при реагировании на инциденты ИБ;

– проведения поиска в сети Интернет, локализации источников и субъектов компьютерных атак.

Представленная задача позволяет формировать, в том числе следующие компетенции в рамках ФГОС ВО по УГСНП 10.00.00 «Информационная безопасность»:

– ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования;

– ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

– ОПК-1.1. Способен проводить анализ защищенности и осуществлять поиск уязвимостей компьютерной системы;

– ОПК-1.2. Способен оценивать корректность программных реализаций алгоритмов защиты информации;

– ОПК-1.3. Способен проводить тестирование и использовать средства верификации механизмов защиты информации;

– ОПК-4.2. Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения);

– ОПК-6.1. Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;

– ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

– ОПК-7.2. Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.

4.3. *Учебно-экспериментальные стенды на базе генераторов трафика и атакующего воздействия*

4.3.1. Учебный стенд «Информационная система в защищенном исполнении»

Заданием по разделу «Построение информационных систем в защищенном исполнении» является создание и реализация на стенде защищенной информационной системы, выполнение настройки основных механизмов защиты информации и тестирование работоспособности и защищенности. Информационная система имеет следующие составляющие: контроллер домена, автоматизированное рабочее место (далее — АРМ), межсетевой экран, web-сервер организации с функционирующей через web-приложение СУБД, СОА, защищаемый интернет-ресурс (рисунок 4.17). Проектирование выполняется с использованием средств виртуализации.

Перед обучающимися ставятся задачи:

— конфигурирования межсетевого экрана (далее — МЭ) путем создания правил разрешения доступа к Web-серверу и удаленного доступа по протоколу PPTP во внутреннюю сеть из внешней сети (любой другой трафик из внешней сети запрещается), для разрешения любого трафика из внутренней сети и ДМЗ;

— конфигурирования СОА путем создания правил для обнаружения входящих из внешней сети и исходящих во внешнюю сеть ICMP-запросов, попыток атак на web-приложения;

— настройки маршрутизации с использованием виртуальной машины с установленным на ней эмулятором оборудования Cisco GNS3;

— настройка контроллера домена, развертывание и конфигурирование СЗИ от НСД Secret Net.

После выполнения каждого из этапов настройки, а также по завершению работы тестируется корректность конфигурирования сетевого оборудования и ССЗИ, а также возможность выявления атакующего воздействия на ИСЗИ. Для тестирования применяются генератор фонового сетевого тра-

фика и генератор атакующего воздействия.

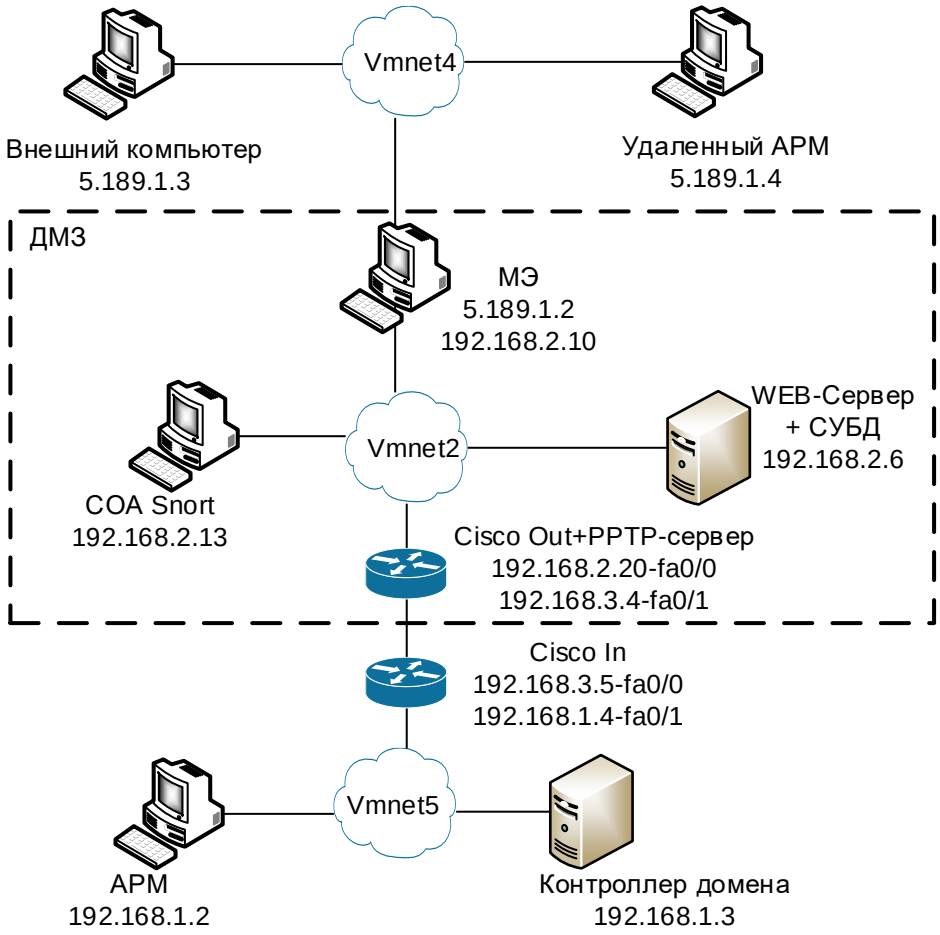

Рисунок 4.17. Структурная схема ИСЗИ

4.3.2. Учебный стенд «Сеть Интернет-провайдера»

Заданием по разделу «Построение инфраструктуры сети Интернет-провайдера» является создание и реализация подсистем идентификации и аутентификации, а также учета биллинговой информации с применением RADIUS – сервера. RADIUS (англ. Remote Authentication in Dial-In User Service) — протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием:

Учебный стенд имеет следующие составляющие (рисунок 4.18): внешний сетевой ресурс (web-сервер), доступ к которому пользователь с АРМ получает только после прохождения идентификации и аутентификации с применением сервера RADIUS (используется FreeRADIUS сервер в ОС Ubuntu

Server), маршрутизатор, сервер RADIUS, АРМ пользователя.

.

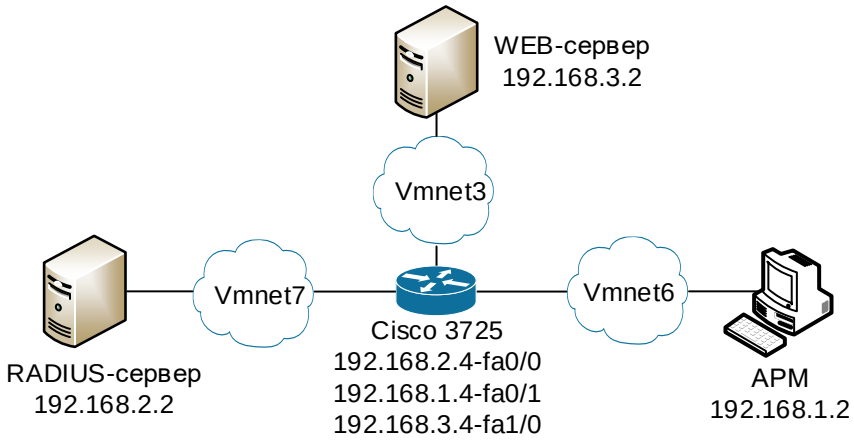

Рисунок 4.18. Структурная схема сети Интернет-провайдера

Также после настройки каждого из компонентов с помощью генератора фонового сетевого трафика и генератора атакующего воздействия тестируется корректность конфигурирования сетевого оборудования.

4.3.3. Учебный стенд «Безопасность АСУ ТП»

С целью формирования практических навыков по моделированию угроз безопасности АСУ ТП на основе технологии виртуализации разработаны мобильные учебно-экспериментальные стенды [288], эмулирующие технологические процессы и системы управления в АСУ ТП (SCADA-системы) с применением сетевых протоколов фирмы Siemens и промышленного протокола Modbus TCP.

Стенды состоят из трех ВМ, которые реализуют функционал типовой структуры АСУ ТП (рисунок 4.19): ВМ «SCADA» (SCADA-система с набором сервисов обработки данных), ВМ «STEP7» (программируемый логический контроллер — ПЛК) и ВМ «Kali Linux», предназначенная для моделирования угроз и атакующих воздействий на АСУ ТП. Коммутационные устройства имитируются виртуальными сетями.

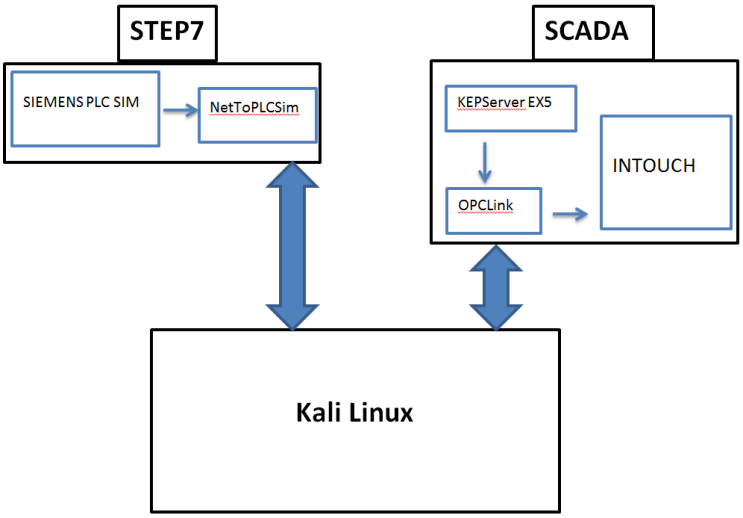

Рисунок 4.19. Структура стенда АСУ ТП

В качестве эмулятора распространенного ПЛК фирмы Siemens используется программное обеспечение Siemens PLC SIM с загружаемыми скриптами, написанными на языке FBD, которые имитируют работу системы подачи теплоносителя. Выбор указанного эмулятора обусловлен широким применением контроллеров фирмы Siemens в АСУ ТП различного назначения.

ВМ «Kali Linux» предназначена для имитации атакующего воздействия, заключающегося в перехвате, модификации и перенаправления команд управления исполнительными устройствами. При моделировании угроз безопасности АСУ ТП исследуются как протоколы передачи управляющих команд (S7comm), так и алгоритмы работы SCADA-систем.

Сетевые атаки моделируются на примере атаки «человек посередине». Применяемая при этом атака типа «ARP-спуфинг» использует недостатки протокола ARP и заключается в том, что компьютер злоумышленника отправляет на атакуемые узлы ARP-ответы, в которых IP-адресу легитимного узла-собеседника ставится в соответствие MAC-адрес машины злоумышленника.

Разработанные стенды позволяют организовать проведение практических занятий и лабораторных работ по тематике безопасности АСУ ТП.

4.3.4. Тестирование систем анализа защищенности с применением технологии Honeypot

Сравнительное тестирование САЗ требует наличия комплекта «эталонных» уязвимых систем, охватывающих все современные технологии обработки информации. При этом перечень уязвимостей должен быть заранее определен. Как и в случае тестирования СОА, очевидным решением является имитация уязвимых систем путем создания генератора ответных пакетов, имитирующего реакцию на запросы САЗ.

Технологическое решение — использование системы Honeynet как совокупности имитаторов уязвимых узлов Honeypot. Honeypot (англ. — «горшочек с медом») — ресурс, представляющий собой сервер, не содержащий защищаемой информации, но отвечающий на запросы атакующих узлов, имитируя работу уязвимой системы. При применении в штатном режиме система Honeypot представляет собой приманку для злоумышленников, позволяющую осуществлять документирование производимых компьютерных атак.

Особенность системы Honeypot — возможность имитировать различные сетевые службы и их уязвимости, наилучшим способом подходит для имитации уязвимой среды. Для САЗ анализируемая удаленная система — это совокупность ответных пакетов, получаемых в ответ на запросы. При этом, получив ответ на один из запросов, демонстрирующий наличие уязвимости на удаленном узле, САЗ использует определенный алгоритм для указанной уязвимости с целью анализа возможности дальнейшего проникновения в систему.

В качестве итогового отчета САЗ формирует схему уязвимостей, иначе называемую графом атак, моделирующую потенциальные возможности нарушителя по проникновению в удаленную систему.

Для тестирования САЗ применяется массив данных, полученный в процессе формирования графов атак (п. 2.3.1), который имитирует уязвимую ИТС путем загрузки профиля сети в систему Honeynet.

4.3.5. Стенд синтеза массивов данных для тестирования ИАСБ

С целью тестирования ИАСБ разработан программный комплекс для синтеза массивов биллинговой информации и массивов условно-реальных данных о взаимодействии пользователей социальных сетей, состоящих из фонового биллинга и ситуационных задач (тестов). Для создания статической структуры социального графа, дополненной сгенерированными текстовыми атрибутивными компонентами учетных записей, в разработанном ПО используется модификация алгоритма Барабаши-Альберт, для создания динамической компоненты — алгоритм имитации процесса взаимодействия пользователей, основанный на использовании аппарата сетей Петри.

Для тестирования поисково-аналитических алгоритмов и методик, реализованных в ИАСБ, на стенде используется программное обеспечение формирования ситуационных задач. Ситуационная задача — это набор абонентов, связанный общими событиями, распределенными во временном промежутке и в пространстве.

В основе стенда лежит ряд виртуальных систем (рисунок 4.20), в том числе сервер NoSQL СУБД Neo4j (генерация и хранение модели социальной сети) и сервер социальной сети Diaspora (аналог социальной сети twitter).

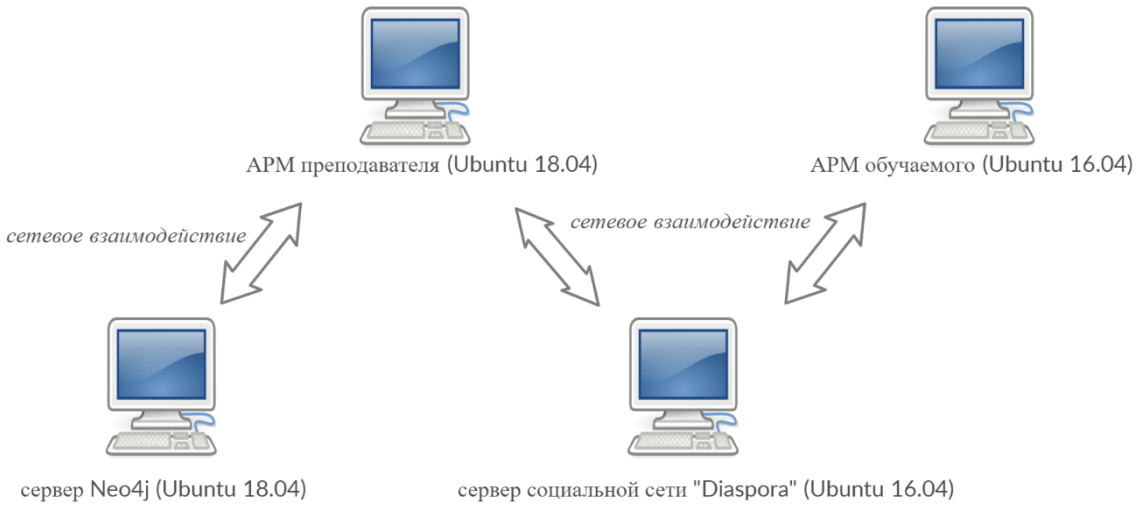

Рисунок 4.20. Стенд формирования массивов условно-реальных данных для тестирования ИАСБ

Для создания массива ситуационного биллинга оператору необходимо загрузить в приложение базу абонентов, в которой записаны их ФИО, IMSI, IMEI, MSISDN и т.д. К основным (фоновым) действиям абонента могут быть добавлены события, обусловленные моделируемой ситуацией. Результатом является граф коммуникационных событий в ИТС, описывающих ситуационную задачу.

Интерфейс программы позволяет редактировать уже созданную ситуацию или менять параметры только отдельно взятого соединения абонентов. Также пользователь может создать неограниченное количество шаблонов передвижения для конкретной ситуации, тем самым придавая большей реалистичности событиям, которые будут описаны и добавлены к фоновому биллингу.

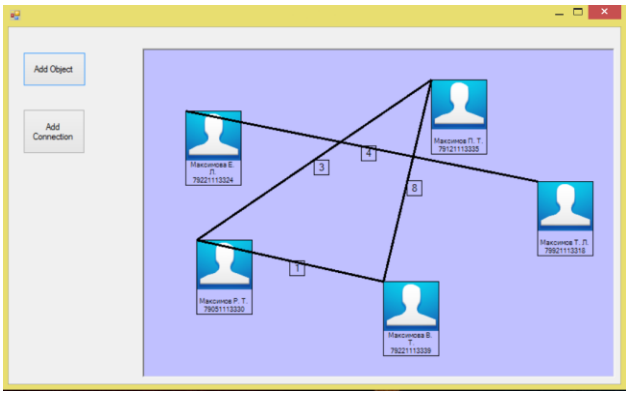

Рисунок 4.21. Интерфейс модуля формирования ситуационной задачи

Разработанное ПО позволяет создавать социальную модель, автоматически регистрировать пользователей в социальной сети Diaspora, динамически добавлять пользователей в контакты по их связям, создавать диалоги между пользователями и генерировать статистически распределенные события отправки приватных сообщений и публичных постов.

Файл выходных данных о взаимодействии пользователей в ИТС является файлом JSON-формата: [{"…":"…", "…":"…"], описывается следующим перечнем полей:

Поле	Пример заполнения
Идентификатор съёмника. Число	"72":1
Время UTC. Число	"73":1456902187
Тип объекта. Число. Для социальных сетей — 8	"79":8
Логин	"305":"250027111222333@INTERNET"
MSISDN номер телефона	"306":"79111222333"
Идентификатор объекта соцсети. Имеет различный формат в зависимости от типа. Для типа сообщений имеет префикс private	"3088":"private295363359_15160@vk.com"
Идентификатор родительского объекта. Для типа сообщений имеет префикс dialog	"3089":"dialog295363359_254927646@vk.com"
Идентификатор пользователя соцсети. Имеет формат: <число>@vk.com	"3090":"295363111@vk.com"
Тип объекта соцсети. Число. 0 – сообщение 5 – контакт	"3092":0
IP1	"24576":"100.80.229.104"
IP2	"24577":"87.240.131.119"
port1	"24578":38757
port2	"24579":80
Сторона сервера. 1 или 2	"24580":2
Сторона отправителя. 1 или 2	"24581":2
Сторона пользователя (какой IP принадлежит телефону/логину). 1 или 2	"24582":1
Отправитель. Строка	"24583":"295363111@vk.com"
Получатели. Массив строк	"24584":["295363222@vk.com"]
Текст сообщения	"12290":"Привет"

Элемент массива в формате JSON объекта из примера заполнения:

[{"72":1,"73":1456902187,"79":8,"305":"250027111222333@INTERNET","306":"79111222333","3088":"private295363359_15160@vk.com","3089":"dialog295363359_254927646@vk.com","3090":"295363111@vk.com","3092":0,"24576":"100.80.229.104","24577":"87.240.131.119","24578":38757,"24579":80,"24580":2,"

24581":2,"24582":1,"24583":"295363111@vk.com","24584":["295363222@vk.com"],"12290":"Привет"}]

Для анализа сгенерированных массивов условно-реальных данных применяются ИАСБ I2, Lampyre, которые позволяют выделять из массива данных информацию искомого формата, искать связи, отмечать интересующие объекты (рисунок 4.22).

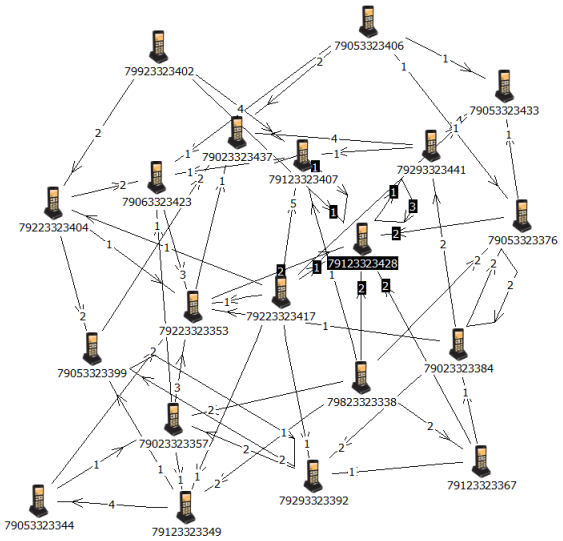

Рисунок 4.22. Примеры работы ИАСБ при анализе сформированного биллинга и массивов данных взаимодействия в социальных сетях

После импорта ситуационных задач и фоновых массивов данных о взаимодействии пользователей социальной сети в базу данных комплекса возможно построение графов, решение тестовых задач и тестирование методик поиска и анализа. В том числе просмотр информации о круге общения абонентов в сети Интернет на основе построения графа связей по задаваемым пользователем параметрам. На графе идентификаторы отображаются как вершины, изображенные в форме круга, а связи — в виде соединяющих ребер.

4.3.6. Архитектура и программное обеспечение автоматизированной обучающей системы киберполигона

Как указано выше, АОС киберполигона разработана в концепции децентрализованного программного обеспечения в среде операционных систем семейства Linux (в том числе, операционной системы Astra Linux) с применением технологии виртуализации на базе системы VMware vSphere.

Отдельные ресурсы представлены совокупностью образов виртуальных машин системы VMware Workstation, содержащих разнообразные операционные системы, сетевые приложения и системы защиты информации, для чего создан репозитарий образов систем, функционирующий в рамках электронной образовательной среды ИРИТ-РТФ УрФУ.

Информационные ресурсы АОС представляют собой децентрализованное хранилище, состоящее из ряда баз данных (далее — БД), предназначенных для хранения статистических характеристик сетевых сред функционирования ССЗИ, массивов сетевого трафика компьютерных атак, типовых сценариев атакующего воздействия и вспомогательных баз данных, образы операционных систем и приложений и средства общего и специального программного обеспечения: система управления учебными курсами Moodle, система виртуализации VMware; генераторы атакующего воздействия, фонового сетевого трафика, массивов информации о взаимодействии пользователей ИТС.

Предложенная архитектура удовлетворяет современным требованиям к построению АОС:

— используется стандартное программное обеспечение, преимущественно российского производства либо свободно распространяемое;

— разработанное и примененное ПО обладает высокой степенью масштабируемости, не зависит от аппаратной платформы.

Предложенный подход по применению технологии виртуализации позволяет существенно упростить процедуры администрирования компьютерных классов и лабораторий, решать задачи не только информационно-

технологического обеспечения, но и организационно-методического обеспечения учебных занятий.

В частности, решается проблема необходимости присутствия различных операционных систем, снабженных соответствующим ПО и средствами защиты информации, на рабочих местах обучающихся. Примененные файлы-образы операционных систем (с учетом поддержки графической оболочки) занимают на рабочей станции либо на сервере не более 10 Гб дискового пространства. Для уменьшения объемов хранения в репозитории образы представлены в сжатом архивном виде. Также путем тиражирования и хранения образов решается актуальная задача сохранения конфигурации операционной системы после проведения ее настроек обучающимся при необходимости использования на следующем занятий. Кроме того, в структуре полигона за счет применения виртуальных интерфейсов минимизировано количество телекоммуникационных устройств при организации соединений между узлами и сегментами.

Структура ПО АОС киберполигона и взаимодействие компонентов в рамках системы виртуализации VMware vSphere предполагает одновременное использование до 300 Гб дискового пространства и до 32 Гб оперативной памяти (таблица 4.1, рисунок 4.23), однако в рамках проведения практических занятий по решению комплексной ситуационной задачи по расследованию инцидентов большинство сегментов используется последовательно, что позволяет при необходимости сократить требуемые вычислительные ресурсы.

Рабочие станции пользователей (студентов) в компьютерном классе подключаются к серверу VMware vSphere, не требуют установки дополнительного ПО. Тип операционной системы на АРМ не имеет значения, возможно использование как Windows, так и Linux.

Таблица 4.1. Структура программного обеспечения АОС киберполигона

Сегмент	Наименование	Вид ОС и ПО	ОЗУ (Гб), НЖМД (файл-образ, Гб)	IP-адрес
Сегменты обеспечения учений	Сценарии АВ и СС, ГКАВ, ГФСТ, ГФМД, ГАБ, ГСЗ	ОС Debian 10, интерпретаторы Python, Ruby	ОЗУ 4, НЖМД 40	192.168.1.1
«Интернет-провайдер»	Сервер RADIUS	ОС Debian 10, FreeRADIUS	ОЗУ 2, НЖМД 10	192.168.3.2
	Коммутатор	ОС Debian 10, ПО iptables	ОЗУ 1, НЖМД 10	192.168.3.1, 192.168.1.2, 192.168.2.1, 192.168.5.1
«Центр мониторинга»	Сервер БД КА	ОС Debian 10, программный комплекс ELK	ОЗУ 8, НЖМД 20	192.168.5.3
«Ситуационный центр»	Карта IP	ОС Debian 10, ПО geoip	ОЗУ 2, НЖМД 10	192.168.5.4
	ИАСБ	ОС Windows 10, ПО Lampyre	ОЗУ 8, НЖМД 20	192.168.5.5
«Безопасность ИТС», блок «ДМЗ»	Межсетевой экран	ОС Debian 10, ПО iptables	ОЗУ 1, НЖМД 10	192.168.4.1, 192.168.2.3
	СОА	ОС Debian 10, ПО Suricata	ОЗУ 2, НЖМД 10	192.168.5.2
	Сервер электронной почты	ОС Windows Server 2016	ОЗУ 2, НЖМД 10	192.168.4.5
	Web-сервер	ОС Debian 10, ПО ngnix	ОЗУ 2, НЖМД 10	192.168.4.4
	DNS-сервер	ОС Debian 10, ПО bind9	ОЗУ 2, НЖМД 10	192.168.4.3
«Безопасность ИТС», блок «VPN-сервер»	VPN-сервер	ОС Debian 10, ПО OpenVPN	ОЗУ 1, НЖМД 10	192.168.2.2
«Безопасность ИТС», блок «Сеть предприятия»	Межсетевой экран	ОС Debian 10, ПО iptables	ОЗУ 1, НЖМД 10	192.168.7.1, 192.168.2.3
	Система DLP	ОС Debian 10, ПО MyDLP	ОЗУ 1, НЖМД 10	192.168.7.2, 192.168.8.1
	СОА	ОС Debian 10, ПО Suricata	ОЗУ 2, НЖМД 10	192.168.5.5
	Коммутатор	ОС Debian 10, ПО iptables	ОЗУ 1, НЖМД 10	192.168.8.2, 192.168.11.1, 192.168.10.1
	Контроллер домена	ОС Windows Server 2016 / ОС Astra Linux	ОЗУ 2, НЖМД 20	192.168.10.1 / 192.168.11.1
	АРМ	ОС Windows 10 / ОС Astra Linux	ОЗУ 2, НЖМД 20	192.168.10.2 / 192.168.11.2

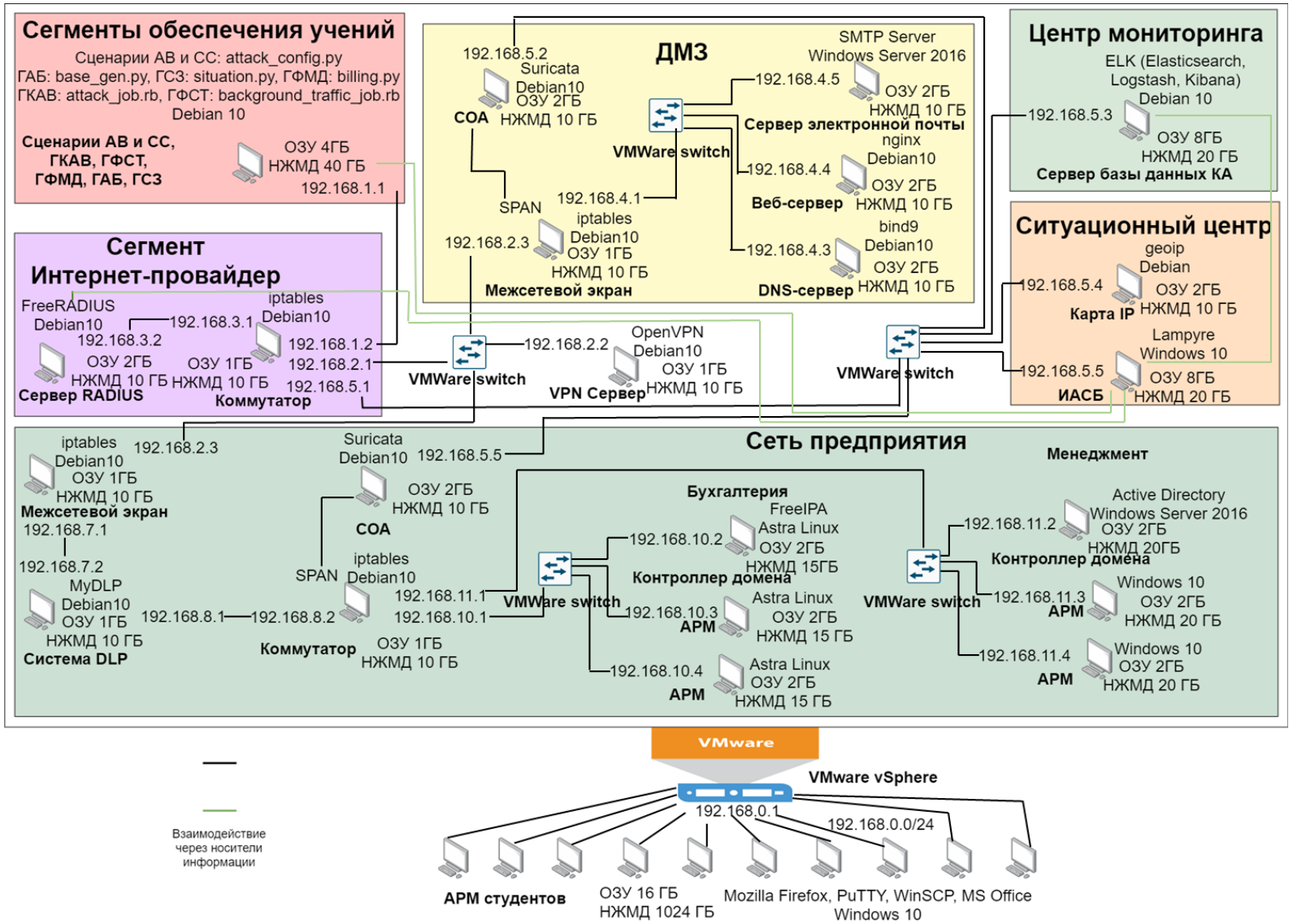

Рисунок 4.23. Схема сетевого взаимодействия компонентов АОС киберполигона

4.4. *Выводы по главе 4*

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 синтеза интерактивной сетевой среды. Предложенный метод, в свою очередь, основан на оригинальной 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 определен-

ных 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 пользователей ИТС, модели синтеза сложных сетей и алгоритмы сетей Петри для формирования 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 информационной безопасности, что отражено в актах внедрения результатов диссертационного исследования в ООО «Уральский центр систем безопасности».

В главе 4 описан комплекс моделей, методик, алгоритмов, программного обеспечения и учебно-экспериментальных стендов компьютерного полигона для тестирования информационно-аналитических систем безопасности и расследования инцидентов информационной безопасности. Представлен разработанный учебно-научный компьютерный полигон по расследованию инцидентов информационной безопасности, комплект входящих в него учебно-экспериментальных стендов тестирования ССЗИ. Стенды используют разработанные модели сетевых сред, генераторы трафика и атакующего воздействия.

Приведена модель компьютерного полигона для тестирования ИАСБ, применяемых при расследовании инцидентов информационной безопасности, описана схема расследования инцидента информационной безопасности.

Представлены модели синтеза условно-реальных данных для ситуационной задачи по расследованию инцидента информационной безопасности и алгоритм анализа взаимодействия пользователей сетей операторов сотовой связи на основе теоретико-графового подхода.

Приведено описание разработанного учебно-научного компьютерного полигона по расследованию инцидентов информационной безопасности, обо-

значены образовательные задачи, требующие моделирования сетевой среды, и их решение в рамках учебно-научного компьютерного полигона.

Описаны структура полигона и единая ситуационная задача по проведению расследования инцидентов информационной безопасности.

Приведено описание ряда учебно-экспериментальных стендов на базе генераторов трафика и атакующего воздействия, развернутых в рамках компьютерного полигона: стенды для построения инфраструктуры сети Интернет-провайдера; для моделирования угроз безопасности АСУ ТП; для изучения ИАСБ, СОА и ТКО, а также для проведения учений по информационной безопасности в формате CTF.

Разработанный компьютерный полигон по расследованию инцидентов информационной безопасности внедрен в образовательный процесс для специальностей 10.05.01 «Компьютерная безопасность» и 10.05.02 «Информационная безопасность телекоммуникационных систем» по дисциплинам «Программно-аппаратные средства обеспечения информационной безопасности», «Предупреждение и обнаружение компьютерных атак», что подтверждено актом о внедрении и демонстрирует адекватность представленных алгоритмов и их программной реализации.

Таким образом, предложено решение частной научной задачи по разработке алгоритмов и программных средств для создания учебно-научного компьютерного полигона по расследованию инцидентов информационной безопасности.

Представленное решение обеспечивает возможность создания комплексной учебной имитационной инфраструктуры для изучения методов расследования инцидентов ИБ, а также учебно-исследовательской имитационной инфраструктуры, позволяющей проводить тестирование ССЗИ для выявления уязвимостей и противодействия компьютерным атакам с целью обеспечения высокого уровня защищенности ИТС, что свидетельствует об эффективности предложенного решения и о достижении поставленной в диссертации цели.

ЗАКЛЮЧЕНИЕ

Представленная диссертация посвящена актуальным вопросам моделирования и синтеза интерактивной сетевой среды при построении компьютерных полигонов в сфере информационной безопасности для обеспечения высокого уровня защищенности объектов ИТС и ИС и проведения тестовых испытаний ССЗИ, в ней рассматривается совокупность параметров, определяющих структуру и наполнение массивов данных, а также автоматизированные методики и алгоритмы синтеза тестовых массивов, позволяющие выявлять уязвимости ССЗИ.

Основными результатами проведенных исследований и обобщений явились следующие.

1. Представлена систематика сетевых компьютерных атак, особенностью которой является возможность использования при моделировании атакующего воздействия. Введена систематика компьютерных атак с точки зрения анализа сетевого трафика СОА. Комплексные компьютерные атаки представляются как совокупность элементарных атакующих воздействий, выполняющихся по определенному сценарию. Практическая значимость представленной систематики состоит в том, что такой подход позволяет при синтезе атакующего воздействия использовать алгоритмы моделирования динамических дискретных систем.

На примере сетевых атак типа «отказ в обслуживании» показано, что особенностью сетевых атак является использование корректного сетевого трафика, соответствующего спецификациям используемых протоколов передачи данных, параметры которого отличаются от штатного либо количественно, либо наличием определенных сигнатур, что позволяет при синтезе тестовых массивов рассматривать атакующее воздействие как вид сетевого трафика с определенным набором параметров.

В качестве объектов тестирования рассмотрены четыре типа ССЗИ — системы обнаружения атак, телекоммуникационное оборудование (на примере маршрутизаторов и систем IP-телефонии), системы анализа защищенности и информационно-аналитические системы безопасности. Показано, что все

рассмотренные типы ССЗИ являются сложными интеллектуальными системами, в которых используются нетривиальные математические алгоритмы, проверка корректности реализации которых требует проведения тестирования различными наборами тестовых данных (трафика). По каждому ССЗИ приведены классификация и основные функции, рассмотрены параметры, подлежащие тестированию.

Для всех рассмотренных типов ССЗИ приведены значимые параметры сетевого трафика (массивов данных), которые должны использоваться при моделировании внешней среды.

2. На основе обзора известных технологий, методов и средств тестирования ССЗИ на примере СОА и ТКО, представленного в главе 1, обозначены основные противоречия, возникающие в процессе тестирования. Показано, что основным общепринятым и единственным эффективно реализуемым подходом к решению задачи тестирования ССЗИ является тестирование в условиях моделирования внешней среды с применением образцов тестового сетевого трафика, что позволяет обеспечить высокую повторяемость результатов, возможность исследования большого количества вариантов и сценариев тестирования. При этом существующие методики тестирования ССЗИ не позволяют в процессе тестирования воспроизводить ряд важнейших особенностей современных компьютерных сетей. Очевидным решением указанных проблем является тестирование ССЗИ на специально разработанных стендах с применением моделируемых внешней среды и атакующего воздействия.

Предложен новый подход к организации атакующего воздействия в задаче тестирования ССЗИ, основанный на формировании базы данных тестовых атак в виде массивов синтезированного сетевого трафика.

Синтез трафика базируется на математической модели сетевой среды функционирования ССЗИ, которая должна учитывать при генерации параметры сетевого трафика заданной сетевой среды функционирования. При этом обеспечивается сходство синтезируемого тестового сетевого трафика с трафиком, циркулирующим в сетевой среде функционирования ССЗИ,

а также учитывается свойство самоподобия сетевого трафика, циркулирующего в существующих компьютерных сетях.

3. Предложен новый метод формирования интерактивной сетевой среды при тестировании ССЗИ. В главе 2 приведены основные элементы метода на примере модели сетевой среды функционирования в задаче тестирования ССЗИ.

Модель ССФ основывается на свойствах ССЗИ, подлежащих тестированию. Тестовые массивы состоят из фоновых массивов данных и массивов атакующего воздействия. Синтез массивов данных осуществляется на основе ранее сохраненных статистических характеристик реального трафика, для чего используется матричная модель хранения характеристик внешней среды.

Тестовая среда должна соответствовать внешней для ССЗИ среде, в качестве критерия соответствия синтезированного фонового массива данным реальных сетей предлагается его самоподобие, измеряемое показателем Херста. При синтезе тестовых массивов данных учитываются как статистические распределения, так и наполнение области данных, для формирования которого применяются алгоритмы марковских цепей.

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.

Синтез массивов данных атакующего воздействия (ситуационных задач) осуществляется на основе алгоритмов сетей Петри, где ситуационные задачи (атаки) представляют собой формируемую по определенным правилам последовательность элементарных событий, распределенных по времени.

Для автоматизации выявления пороговых параметров производительности применяется эволюционно-генетический подход.

Представлены новые модели сетевых сред функционирования для тестирования ТКО и ИАСБ, позволяющие разрабатывать на их основе алгоритмы синтеза тестовых массивов данных.

4. Представлены разработанные подходы к синтезу фоновых массивов данных в задаче тестирования ССЗИ.

Предложен алгоритм определения значений характеристик сетевого трафика и их сохранения в виде матричной модели, что позволяет в дальнейшем формировать структуру СТ на основе алгебраических выражений для полученных составляющих СТ.

В рамках расчета векторов характеристик сетевого трафика на основе матричных операторов предложены способы расчета и формирования графов потоков передачи между источниками и получателями, средних значений длин пакетов и интервалов времени между пакетами.

Предложена методика анализа характеристик сетевого трафика в канале передачи, выделяющая источник, получателя и точку захвата СТ. Введены понятия, характеризующие канал передачи, и предложены способы их расчета: задержка, пропускная способность и частота потерь.

Разработаны и подробно описаны алгоритмы синтеза фоновых массивов данных для тестирования СОА, ТКО и ИАСБ. Алгоритмы имеют схожую структуру и состоят из следующих шагов:

- определение значений характеристик ССФ ССЗИ, запись результатов в виде набора матриц;
- синтез области данных генерируемых массивов;
- синтез потоков пакетов;
- оценка адекватности синтезируемых массивов.

На примере массивов данных для тестирования СОА и ТКО предложены методы анализа реалистичности синтезируемых тестовых массивов, основанные на анализе свойства самоподобия телетрафика с применением показателя Херста.

5. Предложены подходы к синтезу тестирующего массива данных атакующего воздействия и способ автоматизации тестирования с применением аппарата генетических алгоритмов.

Атакующее воздействие (ситуационные задачи) предназначено для реализации двух видов тестов: тесты на анализ корректности реализованных в ССЗИ алгоритмов и тесты на производительность аналитических комплексов.

Для синтеза атакующего воздействия, предназначенного для анализа корректности реализованных алгоритмов в задаче тестирования СОА, предложен аппарат стохастических сетей Петри, в рамках которого дано понятий элементарного атакующего воздействия и комплексной атаки как совокупности элементарных событий. Для тестирования СОА введена стохастическая сеть Петри с задержками, сдерживающими дугами и взвешенными переходами. Показана применимость предложенного аппарата для моделирования комплексных компьютерных атак.

Аналогичный подход впервые предложен для формирования массивов данных для ИАСБ, где аппарат сетей Петри применяется для построения оптимального неповторяющегося маршрута абонентов при синтезе массивов данных биллинговой информации, а также для формирования соединений биллинга на основе шаблонов, каждый из которых описывает типовое поведение абонентов с точки зрения совершаемых действий в сети оператора связи.

Также на основе сетей Петри предложен новый способ формирования графов атак для последующего применения в технологии Honeynet при построении имитаторов уязвимых систем при тестировании САЗ.

С целью определения границ устойчивости ССЗИ к атакующему воздействию (нагрузочное тестирование) предложен метод автоматизации тестирования, основанный на применении эволюционно-генетического подхода.

Представлен модифицированный генетический алгоритм для автоматизации тестирования ТКО на устойчивость к атакующему воздействию типа «отказ в обслуживании». Особенность модифицированного алгоритма заключается в том, что помимо оптимального решения (нахождения макси-

мальных значений параметров атакующего воздействия, приводящих к потере производительности), обнаруживаются области пространства атакующего воздействия, содержащие субоптимальные решения. Практическая значимость решения состоит в возможности нахождения уязвимостей, приводящих к нарушению производительности оборудования при определенных сочетаниях параметров входных данных, не являющихся пороговыми.

Представлен способ анализа результатов работы генетического алгоритма с применением кластерного анализа с использованием алгоритма сдвига среднего. Данный способ позволяет обобщить и очертить границы значений параметров атакующего воздействия, приводящего к превышению заданных требованиями к ССЗИ пороговых значений параметров производительности.

Предложенный подход нашел положительное применение для тестирования ТКО — маршрутизаторов и серверов IP-телефонии.

6. Практическую значимость имеют разработанные методики тестирования ССЗИ и разработанные учебно-экспериментальные стенды, входящие в состав компьютерного полигона по расследованию инцидентов информационной безопасности.

В предложенной методике тестирования СОА применяются критерии, учитывающие вероятности правильного обнаружения атак и вероятности ложных тревог: качество идентификации компьютерных атак, качество обработки сетевого трафика, оптимальная рабочая характеристика СОА.

Описаны экспериментальный стенд и методика тестирования ТКО. Приведено формальное описание автоматизированной методики тестирования защищенности ТКО от сетевых компьютерных атак типа «отказ в обслуживании».

Представлен ряд разработанных учебно-экспериментальных стендов, внедренных в образовательный процесс для специальностей 10.05.01 «Компьютерная безопасность» и 10.05.02 «Информационная безопасность телекоммуникационных систем» и использующих разработанные модели сетевых сред функционирования, генераторы трафика и атакующего воздействия.

Таким образом, в диссертации изложено решение научной проблемы создания научно-методического инструментария проектирования компьютерных полигонов на базе интерактивной сетевой среды, приведено научно обоснованное техническое решение по моделированию интерактивной сетевой среды при создании учебно-научных компьютерных полигонов, позволяющее 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 инциденты информационной безопасности. Предложенное решение по созданию единого научно-методического инструментария моделирования интерактивной сетевой среды при тестировании ССЗИ в виде комплекса моделей, алгоритмов, программного обеспечения и экспериментальных стендов синтеза тестовых массивов данных в составе киберполигона позволяет достичь поставленной цели — повышения показателей защищенности объектов ИТС за счет предупреждения компьютерных атак путем раннего выявления уязвимостей ССЗИ посредством их тестирования, что вносит значительный вклад в повышение безопасности ИТС и ИС. Результаты имеют межотраслевой характер, использованы как на предприятиях и в организациях, в том числе для тестирования ССЗИ, так и в образовательных учреждениях министерства науки и высшего образования Российской Федерации.

Перспективами дальнейшей разработки темы исследования являются модели 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. В рамках развития компьютерных полигонов в сфере ИБ актуальным является создание моделей, имитирующих сетевое взаимодействие в современных мессенджерах и ИТС на базе «облачных» технологий.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

AIM — Advanced Integration Module (улучшенный модуль интеграции)

ARP — Address Resolution Protocol (протокол разрешения адресов)

CDR — Call Data Record (информация о соединении)

CVE — Common Vulnerabilities and Exposures (общеизвестные уязвимости и воздействия)

CVSS — Common Vulnerability Scoring System (общая система оценки уязвимостей)

DNS — Domain Name Service (служба доменных имен)

EVM — Extended Voice Module (модуль поддержки дополнительных голосовых интерфейсов)

HWIC — High-Speed World Area Network Interface Card (интерфейс для высокоскоростного подключения к глобальной сети)

ICMP — Internet Control Message Protocol (протокол контрольных сообщений Интернет)

IDS — Intrusion Detection System (система обнаружения вторжений)

IETF — Internet Engineering Task Force (организация)

IMEI — International Mobile Equipment Identity (международный идентификатор мобильного оборудования)

IMSI — International Mobile Subscriber Identity (международный идентификатор абонента сети подвижной связи)

IP — Internet Protocol (протокол сети Интернет)

ITU-T — International Telecommunication Union Standardization Sector (организация)

LAC — Local Area Code (код локальной зоны)

MAC — Media Access Control (управление доступом к среде)

MSISDN — Mobile Subscriber Integrated Services Digital Number (номер мобильного абонента цифровой сети)

NAT — Network Address Translation (трансляция сетевых адресов)

NME — Network Module Extension (модуль расширения для сетевых интерфейсов)

PVDM — Packet Voice Digital Module (модуль цифровой обработки голосовой информации)

RFC — Request for Comments (документ Internet Engineering Task Force)

SCADA — Supervisory Control and Data Acquisition (диспетчерское управление и сбор данных)

TCP — Transmission Control Protocol (протокол управления передачей данных)

UDP — User Datagram Protocol (протокол пользовательских дейтаграмм)

VoIP — Voice over IP (передача голосовой информации по IP)

АОС — автоматизированная обучающая система

АРМ — автоматизированное рабочее место

ВМ — виртуальная машина

ВСПП — виртуальная среда передачи пакетов

ГИС — государственная информационная система

ГСТ — генератор сетевого трафика

ДМЗ — демилитаризованная зона

ИАД — интеллектуальный анализ данных

ИАСБ — информационно-аналитические системы безопасности

ИБ — информационная безопасность

ИСЗИ — информационная система в защищенном исполнении

ИТС — информационно-телекоммуникационная сеть

ИС — информационная система

КП — канал передачи

КС — канал связи

КСЗ — комплексная ситуационная задача

МАРТ — модуль анализа результатов тестирования

МГА — модуль генетического алгоритма

МТ — модуль тестирования

МЭ — межсетевой экран

ОС — операционная система

ПВ — программа воспроизведения (сетевого трафика)

ПЗ — программа записи (сетевого трафика)

ПЛК — программируемый логический контроллер

ПО — программное обеспечение

ПР — программа распределения (пакетов сетевого трафика)

ПС — программа сопоставления (пакетов сетевого трафика)

САЗ — система анализа защищенности

СВТ — средство вычислительной техники

СЗИ — средство защиты информации

СИ — сетевой интерфейс

СКПБ — система контроля политики безопасности

СОА — система обнаружения атак

СОВ — система обнаружения вторжений

ССЗИ — сетевое средство защиты информации

ССФ — сетевая среда функционирования

СТ — сетевой трафик

ТЗТ — точка захвата сетевого трафика

ТКО — телекоммуникационное оборудование

УВ — узел, взаимодействующий с инициатором

УИ — узел-инициатора процесса передачи данных

УМК — учебно-методический комплекс

УТ — устройство тестирования

УГСНП — укрупненная группа специальностей и направлений подготовки

ФГОС — федеральный государственный образовательный стандарт

ФР — функция распределения

ЭТВ — элементарное тестирующее (атакующее) воздействие

СПИСОК ЛИТЕРАТУРЫ

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

2. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Текст].

3. Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [Текст].

4. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества на 2017–2030 годы» [Текст].

5. 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» [Текст].

6. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Текст].

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

8. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утверждена указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации») [Электронный ресурс]. — Режим доступа: garantf1://72738946.-2147483635/.

9. Постановление Правительства Российской Федерации от 12.10.2019 № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» [Электронный ресурс]. — Режим доступа: garantf1://72761698.0/.

10. 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)) [Электронный ресурс]. — Режим доступа: garantf1://72202278.0/.

11. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ [Текст].

12. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. [Электронный ресурс]. — Режим доступа: garantf1://57869710.0/.

13. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [Электронный ресурс]. — Режим доступа: garantf1://403410768.-2147483647/.

14. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности [Электронный ресурс]. — Режим доступа: garantf1://70146074.0/.

15. СТО БР ИББС-1.3-2016. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств [Электронный ресурс]. — Режим доступа: garantf1://71457690.0/.

16. Информационное письмо ФСТЭК России «Об утверждении требований к системам обнаружения вторжений» [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/305.

17. Методический документ ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты ИТ.СОВ.У5.ПЗ» (утвержден ФСТЭК России 6.03.2012) [Электронный ресурс]. — Режим доступа: garantf1://70059052.0/.

18. Информационное сообщение ФСТЭК России от 12.09.2016 № 240/24/4278 «Об утверждении методических документов, содержащих профили защиты межсетевых экранов» [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/953.

19. Методический документ ФСТЭК России «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты ИТ.МЭ.А4.ПЗ» (утвержден ФСТЭК России 12.09.2016) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/955.

20. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. [Электронный ресурс]. — Режим доступа: garantf1://70986050.0/.

21. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. [Электронный ресурс]. — Режим доступа: garantf1://70952128.0/.

22. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. [Электронный ресурс]. — Режим доступа: garantf1://70952126.0/.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — [Электронный ресурс]. — Режим доступа: garantf1://5821891.0/.

24. Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности [Электронный ресурс]. — Режим доступа: garantf1://70567338.0/.

25. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской федерации. Общие положения [Электронный ресурс]. — Режим доступа: garantf1://70567254.0/.

26. СТО БР ИББС-1.1-2007. Аудит информационной безопасности [Электронный ресурс]. — Режим доступа: garantf1://487314.0/.

27. РС БР ИББС-2.1-2007. Руководство по самооценке соответствия информационной безопасности организации банковской системы РФ требованиям СТО БР ИББС-1.0-2006 [Электронный ресурс]. — Режим доступа: garantf1://487316.0/.

28. СТО БР ИББС-1.2-2014. Методика оценки соответствия информационной безопасности организации банковской системы РФ требованиям СТО БР ИББС-1.0-2014 [Электронный ресурс]. — Режим доступа: garantf1://70567284.0/.

29. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств [Электронный ресурс]. — Режим доступа: garantf1://70046140.-2147483647/.

30. Приказ Министерства науки и высшего образования РФ от 26.11.2020 № 1459 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.01 Компьютерная безопасность» [Электронный ресурс]. — Режим доступа: garantf1://400226001.0/.

31. Приказ Министерства науки и высшего образования РФ от 26.11.2020 № 1458 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем» [Электронный ресурс]. — Режим доступа: garantf1://400225999.0/.

32. Приказ Министерства науки и высшего образования РФ от 26.11.2020 № 1457 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем» [Электронный ресурс]. — Режим доступа: garantf1://400239529.0/.

33. Приказ Министерства науки и высшего образования РФ от 26.11.2020 № 1460 «Об утверждении федерального государственного образо-

вательного стандарта высшего образования - специалитет по специальности 10.05.04 Информационно-аналитические системы безопасности» [Электронный ресурс]. — Режим доступа: garantf1://400005120.0/.

34. Приказ Министерства труда и социальной защиты РФ от 03.11.2016 № 608н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» [Электронный ресурс]. — Режим доступа: garantf1://71450478.-2147483647/.

35. Приказ Министерства труда и социальной защиты РФ от 09.11.2016 № 611н «Об утверждении профессионального стандарта «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности» [Электронный ресурс]. — Режим доступа: garantf1://71447228.-2147483647/.

36. Приказ Министерства труда и социальной защиты РФ от 01.11.2016 № 598н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» [Электронный ресурс]. — Режим доступа: garantf1://71450966.-2147483647/.

37. Приказ Министерства труда и социальной защиты РФ от 15.09.2016 № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» [Электронный ресурс]. — Режим доступа: garantf1://71400328.-2147483647/.

38. Положение «О сертификации средств защиты информации»: утв. постановлением Правительства Российской Федерации от 26.06.1995 № 608 (в ред. от 23.04.96 № 509) [Электронный ресурс]. — Режим доступа: garantf1://2670.0/.

39. Липаев В.В. Качество программных средств. Методические рекомендации [Текст] : под общ. ред. проф., д.т.н. А.А. Полякова. — М. : Янус-К, 2002. — 400 с.

40. Sridhar S. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis [Текст]. — School of Computer Science and Electronic Engineering, University of Essex, 2011.

41. ITU-T E.100: Definitions and terms used in international telephone operation [Электронный ресурс]. — 1988. — Режим доступа: https://www.itu.int/rec /T-REC-E.100-1988-11-I/en.

42. McQuaid S., Bradner J. IETF RFC 2544: Benchmarking methodology for network interconnect devices [Электронный ресурс]. — 1999. — Режим доступа: http://www.ietf.org/rfc/rfc2544.txt.

43. Stopp D., Hickman B. IETF RFC 3918: IP Multicast Throughput No Drop Rate Test [Электронный ресурс]. — 2004. — Режим доступа: http://www.ietf.org/rfc/rfc3918.txt.

44. Bradner S. IETF RFC 1242: Benchmarking terminology for network interconnection devices [Электронный ресурс]. — 1991. — Режим доступа: http://www.ietf.org/rfc/rfc1242.txt.

45. IETF RFC 2889. — Режим доступа: http://www.ietf.org/rfc/rfc2889.txt.

46. Network Working Group H. Schulzrinne Request for Comments: 3550 Columbia ... Schulzrinne, et al. Standards Track [Page 3]. RFC 3550 RTP July 2003. — Режим доступа: http://www.ietf.org/rfc/rfc3550.txt.

47. Avritzer A., Weyuker E.J. The Automatic Generation of Load Test Suites and the Assessment of the Resulting Software [Текст] // IEEE Transactions on Software Engineering. — 1995. — P. 705–716.

48. Jones B.F., Sthamer H.-H., Eyres D.E. Automatic Structural Testing using Genetic Algorithms [Текст] // Software Engineering Journal. — 1996. — Vol. 11, no. 5. — P. 299–306.

49. Pargas R.P., Harrold M.J., Peck R.R. Test-data Generation using Genetic Algorithms [Текст] // Journal of Software Testing, Verification and Reliability. — 1999. — Vol. 9, no. 4. — P. 263–282.

50. Wegener J., Baresel A., Sthamer H. Evolutionary Test Environment for Automatic Structural Testing [Текст] // Journal of Information and Software Technology. — 2001. — Vol. 43, no. 14. — P. 841–854.

51. Tracey N., Clark J., Mander K. Automated Program Flaw finding using Simulated Annealing [Текст] // ACM SIGSOFT Software Engineering Notes. — 1998. — Vol. 23, no. 2. — P. 73–81.

52. Tracey N., Clark J., Mander K. The way Forward for Unifying Dynamic Testcase Generation: The Optimization-based Approach, "Proc. of Int. Workshop on Dependable Computing and its Applications [Текст] // ACM SIGSOFT Software Engineering Notes. — 1998. — P. 169–180.

53. Garousi V., Briand L., Labiche Y. Traffic-aware Stress Testing of Distributed Systems based on UML Models [Текст] // Proceeding (to appear) of International Conference on Software Engineering. — 2006.

54. Столлингс В. Современные компьютерные сети. 2-е изд. [Текст]. — СПб. : Питер, 2003.

55. Батищев, Д.И. Применение генетических алгоритмов к решению задач дискретной оптимизации [Текст] / Д.И. Батищев, Е.А. Неймарк, Н.В. Старостин. — Нижний Новгород : изд-во ННГУ, 2007. — 88 с.

56. Goldberg, D.E. Genetic Algorithms in Search, Optimization, and Machine learning [Текст] / D.E. Goldberg. — Boston : Addison-Wesley, 2009. — 442 p.

57. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский ; пер. с польск. И.Д. Рудинского [Текст]. — М. : Горячая линия-Телеком, 2006. — 452 с.

58. Michalewicz, Z. Genetic Algorithms + Data Structures = Evolution Programs [Текст] / Z. Michalewicz. — Springer-Verlag, 2013. — 432 p.

59. Cerf, R. Critical control of a genetic algorithm [Электронный ресурс] / R. Cerf // CoRR. — Режим доступа: http://arxiv.org/abs/1005.3390 (дата обращения: 20.01.2017).

60. Roeva, O. Influence of the population size on the genetic algorithm performance in case of cultivation process modelling [Электронный ресурс] / O. Roeva, S. Fidanova, M. Paprzycki // Federated Conference on Computer Science and Information Systems (FedCSIS). — Режим доступа: http://ieeexplore.ieee.org/abstract/document/6644027.

61. Holland, J.H. Adaptation in Natural and Artificial Systems [Текст] / J.H. Holland. — Ann Arbor : The University of Michigan Press, 2012. — 183 p.

62. Davis, L. Handbook of Genetic Algorithms [Текст] / L. Davis. — New York : Van Nostrand Reinhold, 2011. — 385 p.

63. Comaniciu, D. Mean shift: A robust approach towards feature space analysis [Текст] / D. Comaniciu, P. Meer // IEEE Trans. Pattern Analysis and Machine Intelligence. — 2002. — Vol. 24. — P. 603–619.

64. Димашова, М.П. Реализация алгоритма сегментации изображения MeanShift на GPU [Текст] / М.П. Димашова // Сборник трудов HPC 2010. Том 1. — Нижний Новгород : Изд-во ННГУ. — С. 214–221.

65. Джонс, М. Программирование искусственного интеллекта в приложениях [Текст] / М. Джонс. — М. : ДМК Пресс, 2013. — 312 с.

66. Анализ данных: учебник для академического бакалавриата / под ред. В.С. Мхитаряна. — М.: Издательство Юрайт, 2016. — 490 с.

67. Рабинович Б.И. Кластерный анализ детализаций телефонных переговоров. [Электронный ресурс] — Режим доступа: http://it-claim.ru/Persons /Rabinovich/klasteranaliz.pdf. — Загл. с экрана.

68. Форман Дж. Много цифр: Анализ больших данных при помощи Excel / Джон Форман ; пер. с англ. А. Соколовой. — М. : Альпина Паблишер, 2016. — 461 с.

69. Лесковец Ю., Раджараман А., Ульман Дж. Анализ больших наборов данных / пер. с англ. Слинкин А.А. — М. : ДМК Пресс, 2016. — 498 с.

70. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / под ред. профессора О.И. Шелухина. — М. : Горячая линия-Телеком, 2013. — 220 с.

71. Никонов В.В., Лось В.П., Росс Г.В. Разработка автоматизированной системы выявления нештатной сетевой активности и обнаружения угроз // Проблемы информационной безопасности. Компьютерные системы. — 2016. № 2. — С. 61-69.

72. Платонов В.В., Семенов П.О. Адаптивная модель распределённой системы обнаружения сетевых атак // Проблемы информационной безопасности. Компьютерные системы. — 2017. № 1. — С. 23-28.

73. Керимова Л.Э. Применение известных классификационных моделей в решении задач обнаружения вторжений с использованием технологии Data Mining. — Информ. технологии — № 3. — 2006. — С. 52-56.

74. Гамаюнов Д.Ю. Обнаружение атак на основе анализа переходов состояний распределенной системы / Д.Ю. Гамаюнов, А.И. Качалин // Искусственный интеллект № 2. — 2004. — С. 49–53.

75. Гамаюнов Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов. Диссертация на соискание ученой степени кандидата физико-математических наук. / Д.Ю. Гамаюнов. — М.: МГУ, 2007. — 89 с.

76. Петровский М.И. Применение методов интеллектуального анализа данных в задачах выявления компьютерных вторжений / Методы и средства обработки информации. Труды Второй Всероссийской научной конференции / Под ред. Л.Н. Королева. — М.: Издательский отдел факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 2005. — 651 с. — С. 158–165.

77. Райх В.В., Синица И.Н., Шарашкин С.М. Макет системы выявления атак на основе обнаружений аномалий сетевого трафика / Методы и средства обработки информации. Труды Второй Всероссийской научной конференции / Под ред. Л.Н. Королева. — М.: Издательский отдел факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 2005. — 651 с. — С. 175–181.

78. Puketza N. J. A methodology for testing intrusion detection systems / N. J. Puketza, K. Zhang, M. Chung, B. Mukherjee, R. A. Olsson // IEEE Transactions on Software Engineering, Volume 22, Issue 10, October 1996. — P. 719–729.

79. Evaluating Intrusion Detection Systems: the 1998 DARPA Off-Line Intrusion Detection Evaluation / R.P. Lippmann, D.J. Fried, I. Graf, J.W. Haines, K.R. Kendall, D. McClung, D. Weber, S.E. Webster, D. Wyschogrod, R.K. Cunningham, M.A. Zissman // DARPA Information Survivability Conference

and Exposition (DISCEX), Volume 2, 2000. — P. 12–26 — http://www.ll.mit.edu/mission/communications/ist/files/dis-cex00_paper.pdf.

80. Kendall K. A database of computer attacks for the evaluation on intrusion detection systems : S. M. Thesis / K. Kendall. — Massachusetts Institute of Technology, Cambridge, 1999. — P.124.

81. Weber D. A Taxonomy of Computer Intrusions : S. M. Thesis / D. Weber. — Massachusetts Institute of Technology, 1998. — P. 69.

82. McHugh J. Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory / J. McHugh // ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4, November 2000. — P. 262–294.

83. Open Security Evaluation Criteria (OSEC). — Neohapsis Labs, 2002. — http://osec.neohapsis.com

84. Ван Трис Г. Теория обнаружения, оценок и модуляции : в 3 т. : [пер. с англ.] / Г. Ван Трис. — Под ред. В. И. Тихонова. — М.: Сов. радио. — 1972. — 744 с.

85. Ulvila J. W. Evaluation of Intrusion Detection Systems / J. W. Ulvila, J. E. Gaffney // Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003. — 21 p.

86. Lippmann R. P. The 1999 DARPA Off-Line Intrusion Detection Evaluation / R. P. Lippmann, D. J. Fried, J. W. Haines, J. Korba, K. Das // Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 34, Issue 4, October 2000. — P. 579–595.

87. Haines J. W. 1999 DARPA Intrusion Detection System Evaluation: Design and Procedures : Technical Report / J.W. Haines, R.P. Lippmann, D.J. Fried, E. Tran, S. Boswell, M.A. Zissman. — MIT Lincoln Laboratory, TR-1062, Cambridge, 2001. — 202 p.

88. Durst R. Testing and evaluating computer intrusion detection systems / R. Durst, T. Champion, B. Witten, E. Miller, L. Spagnuolo // Communications of the ACM, Volume 42, Issue 7, July 1999. — P. 53–61.

89. Massicotte F. Automatic Evaluation of Intrusion Detection Systems / F. Massicotte, F. Gagnon, Y. Labiche, L. Briand, M. Couture // 22nd Annual Computer Security Applications Conference (ACSAC), December 2006. — P. 361–370.

90. Shipley G. ISS Real Secure Pushes Past Newer IDS Players / G. Shipley. Network Computing, May 17, 1999 // Режим доступа: http://www.net-workcomputing.com/1010/1010r1.html, свободный.

91. Shipley G. Intrusion Detection, Take Two / G. Shipley Network Computing, November 15, 1999 // Режим доступа: http://www.networkcomputing.com/1023/1023f1.html, свободный.

92. Mueller P. Dragon claws its way to the top / P. Mueller, G. Shipley. Network Computing, August 20, 2001 // Режим доступа: http://www.network-computing.com/1217/1217f2.html, свободный.

93. Yocom B. Intrusion battleground evolves / B. Yocom, K. Brown. Network World, October 8, 2001 // Режим доступа: http://www.networkworld.com/ reviews/2001/1008bg.html, свободный.

94. Snyder J. An ounce of intrusion prevention may cure your network security ills / J. Snyder, D. Newman, R. Thayer. Network World, February 16, 2004 // Режим доступа: http://www.networkworld.com/reviews/2004/0216, свободный.

95. Thayer R. Network-intrusion detection systems / R. Thayer. Network World, January 31, 2005 // Режим доступа: http://www.networkworld.com/ reviews/2005/013105rev.html, свободный.

96. Newman D. IPS performance tests show products must slow down for safety / D. Newman. Network World, September 11, 2006 // Режим доступа: http: //www.networkworld.com/reviews/2006/091106-ips-test.html, свободный.

97. Snyder J. Sourcefire boasts strong IPS management toolset / J. Snyder. Network World, January 21, 2008 // Режим доступа: http://www.net-workworld.com/reviews/2008/080408-test-checkpoint-ips-how.html, свободный.

98. Snyder J. Check Point IPS-1 fills a gap in its product line / J. Snyder. Network World, August 4, 2008 // Режим доступа: http://www.network-world.com/reviews/2008/080408-test-checkpoint-ips.html, свободный.

99. Фратто М. Тестируем системы предотвращения вторжений уровня сети / М. Фратто // Сети и системы связи, №1 (107), 2004. — С. 76–86.

100. Клозе Р. Snort и ее коммерческие варианты / Р. Клозе // LAN: Журнал сетевых решений, Август 2004. — С. 84–88.

101. Клозе Р. Закрытый код с хорошим набором правил / Р. Клозе // LAN: Журнал сетевых решений, Декабрь 2004. — С. 90–95.

102. Athanasiades N. Intrusion detection testing and benchmarking methodologies / N. Athanasiades, R. Abler, J. Levine, H. Owen, G. Riley // First IEEE International Workshop on Information Assurance (IWIAS), 24 March 2003. — P. 63–72.

103. Mell P. An Overview of Issues in Testing Intrusion Detection Systems : Technical Report / P. Mell, V. Hu, R. Lippmann, J. Haines, M. Zissman. — National Institute of Standard and Technology, NIST IR 7007, June 2003. — 21 p.

104. Debar H. A workbench for intrusion detection systems / H. Debar, M. Dacier, A. Wespi, S. Lampart. // IBM Zurich Research Laboratory, Ruschlikon, Switzerland, March 1998.

105. Aguirre S. J. Intrusion Detection Fly-Off: Implications for the United States Navy : Technical Report / S. J. Aguirre, W. H. Hill. // MITRE, MTR 97W096, McLean, Virginia, September 1997.

106. Network Intrusion Detection System Certification Methodology. Version 5.20. — NSS Labs, May 2008. — 30 p. // Режим доступа: http:// nsslabs.com/certification/ips/NIPS%20Methodology_v5_20.pdf, свободный.

107. Ranum M.J. Experiences Benchmarking Intrusion Detection Systems / M.J. Ranum. – NFR Security. December 2001 // Режим доступа: www.snort.org/docs/Benchmarking-IDS-NFR.pdf, свободный.

108. Balzarotti D. Testing network-based intrusion detection signatures using mutant exploits / G. Vigna, W. Robertson, D. Balzarotti // 11th ACM conference on Computer and communications security, 2004. — P. 21–30.

109. Lee M. LARIAT: Lincoln Adaptive Real-time Information Assurance Testbed / M. Lee, J. C. Rabek, R.K. Cunningham, D.J. Fried, R.P. Lippmann, M.A. Zissman // In proc. of IEEE Aerospace conference, Vol.6, 2002. — P. 6–2671–2676.

110. Benzel T. Experience with DETER: A testbed for security research / T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower // In proc. of 2nd international IEEE conference on testbeds and research infrastructure for the development of networks and communities, 2006.

111. EMIST — Evaluation Methods for Internet Security Technology // Режим доступа: http://emist.ist.psu.edu, свободный.

112. Scriptable Event System (SES from EMIST) // Режим доступа: http://cs.purdue.edu/homes/fahmy/software/emist/documentation.html, свободный.

113. Hong S. TCP transform: property-oriented TCP traffic transformation / S. Hong, F. Wong, Wu S. Felix // Detection of Intrusion and Malware & Vulnerability Assessment (DIMVA) conference, 2005.

114. Chinchani R. RACOON: Rapid generating user command data for anomaly detection from customizable templates / R. Chinchani, A. Muthukrishnan, M. Chandrasekaran, S. Upadhyaya // Proceedings of 20th annual computer security application conference, 2004.

115. Michiel H. Teletraffic Engineering in a Broad-Band Era / H. Michiel, K. Laevens // Proceedings of the IEEE, vol. 85, № 12, 1997.

116. Lv J. Network traffic prediction and fault detection based on adaptive linear model / J. Lv, X. Li, C. Ran, T. He // IEEE International conference on industrial technology (ICIT), 2004.

117. Dong-Yan Z. A network traffic model based on measurement / Z. Dong-Yan, H. Ming-Zeng, Z. Hong-Li, K. Ting-Biao // Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, 2005. — P.18–21.

118. Geist R. Correlational and distributional effects in network traffic models / R. Geist, J. Westall. — 2006.

119. Zhang B. Simulation of network traffic and its application / B. Zhang, Y. Sun // 8th International Conference on Control, Automation, Robotics and Vision. Kunming, China, 2004.

120. Mandelbrot B.B. Long-Run Linearity, Locally Gaussian Processes, H-Spectra and Infinite Variances / B.B. Mandelbrot // International Economic Review, Vol.10, 1969. — P. 82–113.

121. Willinger W. Self-Similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level / W. Willinger, M.S. Taqqu, R. Sherman, D.V. Wilson // IEEE Transactions on Networking, Vol. 5, № 1, 1997. — P. 71–86.

122. Liu Z. Asymptotic Behavior of a Multiplexer Fed by a Long-Range Dependent Process / Z. Liu, P. Nain, D. Towsley, Z.L. Zhang // CMPSCI Tehnical Report 97-16, University of Massachusetts at Amherst, 1997.

123. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса / Б.С. Цыбаков // Радиотехника, № 5, 1999. — С. 24–31.

124. Петров В.В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия: диссертация на соискание ученой степени кандидата технических наук / В.В. Петров // Москва, 2004.

125. Соколов Д.Е. Характер сетевого трафика на клиентском участке распределенной клиент-серверной системы / Д.Е. Соколов, Н.Г. Треногин // Материалы Международной научно-технической конференции «Информатика и проблемы телекоммуникаций». — Новосибирск: СибГУТИ, 2001. — С. 34–35.

126. Витяев Е.Е. Обнаружение закономерностей и распознавание аномальных событий в потоке данных сетевого трафика / Е.Е. Витяев, Б.К. Ковалерчук, А.М. Федотов, В.Б. Барахнин, С.Д. Белов, Д.С. Дурдин, А.В. Демин // Вестник Новосибирского государственного университета. Серия: Информационные технологии, том 6, номер 2, 2008. — С. 57–68.

127. Назаров Н.А., Сычев К.И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. — Красноярск, 2010. — 389 с.

128. Hernandez-Campos F. Generating realistic TCP workloads / F. Hernandez-Campos, F.D. Smith, K. Jeffay // In Proceedings of Computer Measurement Group Conference, 2004.

129. Lan K.C. Rapid model parameterization from traffic measurements / K.C. Lan, J. Heidemann // ACM Trans. Model. Comput. Simul., № 12(3), 2002. — P. 201–229.

130. Sommers J. A framework for malicious workload generation / J. Sommers, V. Yegneswaran, P. Barford // In Proceedings of ACM SIGCOMM Internet Measurement Conference, ACM Press, 2004. — P. 82–87.

131. Paxson V. Wide area traffic: the failure of Poisson modeling / V. Paxson, S. Floyd // IEEE/ACM Transactions on Networking, № 3(3), 1995. — P. 226–244.

132. Floyd S. Internet research needs better models / S. Floyd, E. Kohler // ACM Computer Communication Review, № 33(1), 2003. — P. 29–34.

133. Tcpreplay: Pcap editing and replay tools for *nix // Режим доступа: http://tcpreplay.sourceforge.net, свободный.

134. Jain R. Characteristics of destination address locality in computer networks: a comparison of caching schemes / R. Jain // Computer Networks and ISDN Systems, № 18(4)б, 1990. — P. 243–254.

135. Feldmeier D. Improving gateway performance with a routing-table cache / D. Feldmeier // In Proceedings of IEEE Infocom, 1988. — P. 27–31.

136. Gopalan K. Improving route lookup performance using network processor cache / K. Gopalan, T. Chiueh // In Proceedings of the ACM/IEEE Conference on Supercomputing, IEEE Computer Society Press, Los Alamitos, CA, USA, 2002. — P. 1–10.

137. Rupp A. Packet trace manipulation framework for test labs / A. Rupp, H. Dreger, A. Feldmann, R. Sommer // In Proceedings of ACM SIGCOMM Internet Measurement Conference, ACM Press, 2004. — P. 251–256.

138. McCanne S. The bsd packet filter: A new architecture for user-level packet capture / S. McCanne, V. Jacobson // In Proceedings of the Winter USENIX Technical Conference, 1993. — P. 259–269.

139. Tcpdump public repository // Режим доступа: http://www.tcpdump.org, свободный.

140. The DAG Project // Режим доступа: http://dag.cs.waikato.ac.nz, свободный.

141. Graham I. The dag: an atm measurement board / I. Graham, J. Martens, M. Pearson // In 4th Electronics New Zealand Conference, 1997.

142. Micheel J. Precision timestamping of network packets / J. Micheel, S. Donnelly, I. Graham // In Proceedings of ACM SIGCOMM Internet Measurement Workshop, ACM Press, New York, NY, USA, 2001. — P. 273–277.

143. Internet Traffic Archive // Режим доступа: http://ita.ee.lbl.gov, свободный.

144. NLANR's Passive Measurement and Analysis (PMA) project. [Электронный ресурс] // Режим доступа: http://pma.nlanr.net, свободный.

145. Chandola V. Anomaly detection: A survey / V. Chandola, A. Banerjee, V. Kumar // ACM Comput. Surv., № 41(3), 2009.

146. Ye T. Divide and conquer: PC-based packet trace replay at OC-48 speeds / T. Ye, D. Veitch, G. Iannaccone, S. Bhattacharyya // In Tridentcom, Italy, 2005.

147. Leland W. On the self-similar nature of Ethernet traffic / W. Leland, M. Taqqu, W. Willinger, D. Wilson // In Proceedings of SIGCOMM '93, 1993. — P. 183–193.

148. Paxson V. Fast, approximate synthesis of fractional gaussian noise for generating self-similar network traffic / V. Paxson // ACM Computer Communication Review, № 27(5), 1997. — P. 5–18.

149. Erramilli A. Experimental queueing analysis with long-range dependent packet traffic / A. Erramilli, O. Narayan, W. Willinger // IEEE/ACM Transactions on Networking, № 4(2), 1996. — P. 209–223.

150. Aida M. Pseudo-address generation algorithm of packet destinations for Internet performance simulation / M. Aida, T. Abe // In Proceedings of IEEE Infocom, 2001. — P. 1425–1433.

151. Kohler E. Observed structure of addresses in IP traffic / E. Kohler, J. Li, V. Paxson, S. Shenker // In Proceedings of ACM SIGCOMM Internet Measurement Workshop, ACM Press, 2002. — P. 253–266.

152. Dasgupta D. An Immunity-Based Technique to Characterize Intrusions in Computer Networks / D. Dasgupta, F.A. Gonzalez // IEEE Transactions on Evolutionary Computation, 2002. — P. 1081–1088.

153. Sommers J. Improving accuracy in end-to-end packet loss measurement / J. Sommers, P. Barford, N. Duffield, A. Ron // In Proceedings of ACM SIGCOMM, 2005.

154. Floyd S. Random early detection gateways for congestion avoidance / S. Floyd, V. Jacobson // IEEE/ACM Transactions on Networking, № 1(4), 1993. — P. 397–413.

155. Appenzeller G. Sizing router buffers / G. Appenzeller, I. Keslassy, N. McKeown // In Proceedings of ACM SIGCOMM, 2004.

156. Padhye J. Modeling TCP throughput: a simple model and its empirical validation / J. Padhye, V. Firoiu, D. Towsley, J. Kurose // In Proceedings of ACM SIGCOMM, ACM Press, New York, NY, USA, 1998. — P. 303–314.

157. Budhiraja A. Stochastic differential equation for tcp window size: Analysis and experimental validation / A. Budhiraja, F. Hernandez-Campos, V.G. Kulkarni, F.D. Smith // Probab. Eng. Inf. Sci., № 18(1), 2004. — P. 111–140.

158. Caceres R. Characteristics of wide-area TCP/IP conversations / R. Caceres, P.B. Danzig, S. Jamin, D.J. Mitzel // In Proceedings of ACM SIGCOMM, ACM Press, 1991. — P. 101–112.

159. Danzig P.B. tcplib: A library of TCP/IP traffic characteristics / P.B. Danzig, S. Jamin // USC Networking and Distributed Systems Laboratory TR CS-SYS-91-01, 1991.

160. Joo Y. On the impact of variability on the buffer dynamics in IP networks / Y. Joo, V. Ribeiro, A. Feldmann, A. Gilbert, W. Willinger // In Allerton Conference on Communication, Control and Computing, 1999.

161. Joo Y. Tcp/ip traffic dynamics and network performance: a lesson in workload modeling, flow control, and trace-driven simulations / Y. Joo, V. Ribeiro, A. Feldmann, A.C. Gilbert, W. Willinger // ACM Computer Communication Review, № 31(2), 2001. — P. 25–37.

162. Christiansen M. Tuning RED for Web traffic / M. Christiansen, K. Jeffay, D. Ott, F.D. Smith // In Proceedings of ACM SIGCOMM, 2000. — P. 139–150.

163. Paxson V. Empirically derived analytic models of wide-area TCP connections / V. Paxson // IEEE/ACM Transactions on Networking, № 2(4), 1994. — P. 316–336.

164. Annaureddy S. Shark: Scaling File Servers via Cooperative Caching / S. Annaureddy, M.J. Freedman, D. Mazieres // Proceeding: 2nd conference on Symposium on Networked Systems Design & Implementation, v. 2, 2005. — P. 129–142.

165. Arlitt M.F. A synthetic workload model for Internet Mosaic traffic / M.F. Arlitt, C.L. Williamson // In Summer Computer Simulation Conference, — 1995. — P. 24–26.

166. Cunha C. Characteristics of WWW client-based traces / C. Cunha, A. Bestavros, M. Crovella // Technical report, Boston University, 1995.

167. Crovella M.E. Self-similarity in world wide Web traffic: evidence and possible causes / M.E. Crovella, A. Bestavros // In Proceedings of ACM SIGMETRICS, ACM Press, New York, NY, USA, 1996. — P. 160–169.

168. Baker M.G. Measurements of a distributed file system / M.G. Baker, J.H. Hartman, M.D. Kupfer, K.W. Shirriff, J.K. Ousterhout // In Proceedings of the ACM Symposium on Operating Systems Principles (SOSP), ACM Press, New York, NY, USA, 1991. — P. 198–212.

169. Guo L. The war between mice and elephants / L. Guo, I. Matta // In Proceedings of the IEEE International Conference on Network Protocols (ICNP), IEEE Computer Society, Washington, DC, USA, 2001. — P. 180–181.

170. Marron J.S. Mice and elephants: visualization of Internet traffic / J.S. Marron, F. Hernandez-Campos, F.D. Smith // In Proceedings of 15th Conference on Computational Statistics, 2002.

171. Estan C. New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice / C. Estan, G. Varghese // ACM Transactions on Computer Systems, № 21(3), 2003. — P. 270–313.

172. Misra V. Fluid-based analysis of a network of aqm routers supporting tcp flows with an application to red / V. Misra, W.B. Gong, D. Towsley // In Proceedings of ACM SIGCOMM, ACM Press, New York, NY, USA, 2000. — P. 151–160.

173. Downey A.B. The structural cause of file size distributions / A.B. Downey // In Proceedings of the ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), IEEE Computer Society, Washington, DC, USA, 2001. — P. 361–362.

174. Downey A.B. Evidence for long-tailed distributions in the internet / A.B. Downey // In Proceedings of ACM SIGCOMM Internet Measurement Workshop, ACM Press, New York, NY, USA, 2001. — P. 229–241.

175. Mitzenmacher M. A brief history of generative models for power law and lognormal distributions / M. Mitzenmacher // Internet Mathematics, № 1(2), 2004. — P. 226–251.

176. Nuzman C. A compound model for TCP connection arrivals for LAN and WAN applications / C. Nuzman, I. Saniee, W. Sweldens, A. Weiss // Computer Networks, № 40(3), 2002. — P. 319–337.

177. Barford P. Generating representative Web workloads for network and server performance evaluation / P. Barford, M. Crovella // In Proceedings of ACM SIGMETRICS, 1998. — P. 151–160.

178. Mah B.A. An empirical model of HTTP network traffic / B.A. Mah // In Proceedings of IEEE Infocom, v. 2, 1997. — P. 592–600.

179. Hernandez-Campos F. Tracking the evolution of Web traffic: 1995-2003 / F. Hernandez-Campos, K. Jeffay, F.D. Smith // In Proceedings of the ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), 2003.

180. Barford P. A performance evaluation of hyper text transfer protocols / P. Barford, M. Crovella // In Proceedings of ACM SIGMETRICS, 1999. — P. 188–197.

181. Barford P. Changes in Web client access patterns: Characteristics and caching implications / P. Barford, A. Bestavros, A. Bradley, M. Crovella // World Wide Web, № 2(1-2), 1999. — P. 15–28.

182. Smith F.D. What TCP/IP protocol headers can tell us about the Web / F.D. Smith, F. Hernandez-Campos, K. Jeffay, D. Ott // In Proceedings of ACM SIGMETRICS, 2001. — P. 245–256.

183. Le L. The effects of active queue management on Web performance / L. Le, J. Aikat, K. Jeffay, F.D. Smith // In Proceedings of ACM SIGCOMM, ACM Press, New York, NY, USA, 2003. — P. 265–276.

184. Breslau L. Advances in Network Simulation / L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, H. Yu // IEEE Computer, № 33(5), 2000. — P. 59–67.

185. Feldmann A. Dynamics of IP traffic: A study of the role of variability and the impact of control / A. Feldmann, A.C. Gilbert, P. Huang, W. Willinger // In sigcomm, 1999. — P. 301–313.

186. Cao J. Stochastic Models for Generating Synthetic HTTP Source Traffic / J. Cao, W.S. Cleveland, Y. Gao, K. Jeffay, F.D. Smith, M. Weigle // In Proceedings of IEEE Infocom, 2004.

187. Cheng Y.C. Monkey see, monkey do: A tool for tcp tracing and replaying / Y.C. Cheng, U. Hoelzle, N. Cardwell, S. Savage, G.M. Voelker // In USENIX Annual Technical Conference, 2004.

188. Kamath P. Generation of high bandwidth network traffic traces / P. Kamath, K. Lan, J. Heidemann, J. Bannister, J. Touch // In Proceedings of the ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), USC/Information Sciences Institute, IEEE. Fort Worth, Texas, USA, 2002. — P. 401–410.

189. Крижановский А.В. Предотвращение компьютерных атак на основе ассоциаций иммунной системы человека и операционной системы ЭВМ / А.В. Крижановский, А.М. Марасанов // Матем. моделирование, 19:12 (2007). — С. 3–12.

190. Willinger W. Self-similarity in high-speed packet traffic: Analysis and modeling of Ethernet traffic measurements / W. Willinger, M. Taqqu, W. Leland, D. Wilson // Statistical Science, № 10(1), 1995. — P.67–85.

191. Заборовский В.С. Методы и средства исследования процессов в высокоскоростных компьютерных сетях: диссертация на соискание ученой степени доктора технических наук / В.С. Заборовский // СПб, 1999.

192. Коллеров А.С. Критерий оценки качества синтезированного трафика на основе параметра Херста / А.С. Коллеров // Безопасность информационного пространства VI: сборник трудов межвузовской научно-практической конференции студентов, аспирантов и молодых ученых. — Тюмень: Изд-во ТюмГУ, 2007. — С. 32–34.

193. Коллеров А.С. Фоновый трафик при тестировании систем обнаружения атак (СОА) / А.С. Коллеров, М.Ю. Щербаков // Безопасность информационного пространства: материалы международной научно-практической конференции. — Екатеринбург: ГОУ ВПО УрГУПС, 2006. — С. 107.

194. Поршнев С.В., Божалкин Д.А. Математическое и алгоритмическое обеспечение для анализа характеристик информационных потоков в магистральных интернет-каналах. — М.: Горячая линия – Телеком, 2021. — 214 с.

195. Поршнев С.В., Соломаха Э.В., Пономарева О.А. Об особенностях оценок показателя Херста классического броуновского движения, вычисляемых с помощью метода R/S-анализа // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 8, no.10, 2020.

196. Smith W.L. Regenerative Stochastic Processes / W.L. Smith // Proc. Roy. Soc. Ser. A, №232, 1955. — P. 6–31.

197. Цыбаков Б.С. Наилучшая и наихудшая дисциплины передачи пакетов / Б.С. Цыбаков, П. Папантони-Казакос // Проблемы передачи информации, т. 32, вып. 4, 1996. — С.72–92.

198. Duffield N.G. Queueing at Large Resources Driven by Long-Tailed M/G/∞-modulated Processes / N.G. Duffield // manuscript, 1996.

199. Erdo˝s, P., and A. Re´nyi, On Random Graphs. Publicationes Mathematicae (Debrecen), volume 6, 1959, pp. 290-297.

200. Watts, D. J., Small Worlds: The Dynamics of Networks between Order and Randomness (Princeton University, Princeton, NJ), 1999.

201. R. Albert, A-L. Barabasi. Statistical mechanics of complex networks. Reviews of modern physics, volume 74, January 2002.

202. Гурдзибеева А.Р. Исследование и разработка методов и алгоритмов имитационного моделирования для тренажеров операторов сложных

объектов: диссертация на соискание ученой степени кандидата технических наук / А.Р. Гурдзибеева // Владикавказ, 2004.

203. Клыков В.В. Интерактивные компьютерные тренажеры по математическим дисциплинам: диссертация на соискание ученой степени кандидата технических наук / В.В. Клыков // Томск, 2005.

204. Кручинин В.В. Методы и алгоритмы построения компьютерных учебных программ и систем на основе генераторов информационных объектов: диссертация на соискание ученой степени доктора технических наук / В.В. Кручинин // Томск, 2005.

205. Монахов М.Ю. Методы и модели обработки и представления информации в распределенных образовательных системах: диссертация на соискание ученой степени докт. техн. наук / М.Ю. Монахов // Владимир, 2005.

206. Соэ Моэ Лвин. Разработка элементов виртуального полигона моделирования окружающей морской среды в гетерогенном вычислительном окружении: диссертация на соискание ученой степени кандидата технических наук / С.М. Лвин // СПб, 2011.

207. Угаров В.В. Компьютерные модели и программные комплексы в проектно-ориентированном обучении: диссертация на соискание ученой степени кандидата технических наук / В.В. Угаров // Ульяновск, 2005.

208. Цуканов М.В. Совершенствование системы обучения курсу "Компьютерные коммуникации и сети" на основе применения мультиагентных технологий: диссертация на соискание ученой степени кандидата технических наук / М.В. Цуканов // Курск, 2005.

209. Clark D. The design philosophy of the DARPA Internet Protocols / D. Clark // In ACM Sigcomm, 1988.

210. Zukerman M. Internet Traffic Modeling and Future Technology Implications / M. Zukerman, T.D. Neame, R.G. Addie // Proceedings of Infocom. 2003.

211. Коллеров А.С. Метод формирования значений параметров сетевого трафика, характеризующих канал передачи, в задаче тестирования сетевых систем обнаружения атак / А.С. Коллеров // Вопросы защиты информации: Науч.-практ. журн. — М.: ФГУП «ВИМИ», 2010. — С. 24–30.

212. Vahdat A. Scalability and Accuracy in a Large-Scale Network Emulator / A. Vahdat, K. Yocum, K. Walsh, P. Mahadevan, D. Kostic, J. Chase, D. Becker // Proceeding: 5th symposium on Operating systems design and implementation, v. 36, 2002. — P. 271–284.

213. Karagiannis T. BLINC: Multilevel Traffic Classification in the Dark / T. Karagiannis, K. Papagiannaki, M. Faloutsos // Proceeding: Applications, technologies, architectures and protocols for computer communications, 2005. — P. 229–240.

214. Шредер М. Фракталы, хаос, степенные законы. Миниатюры из бесконечного рая / М. Шредер // Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. — 528 с.

215. Советов Б. Я. Моделирование систем: Учеб. для вузов / Б. Я. Советов, С. А. Яковлев. — М.: Высш. шк., 2007. — 343 с.

216. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. / Дж. Питерсон. — М.: Мир, 1984. — 264 с.

217. Горбатов В.А. Основы дискретной математики: Учеб. пособие для вузов / В. А. Горбатов. — М.: Высш. шк., 1986. — 311 с.

218. Farber D. J. Recoverability of communication protocols: Implications of a theoretical study / P. M. Merlin, D. J. Farber // IEEE Transactions on Communications, vol. 24(9), September 1976. — P. 1036–1043.

219. Noe J. D. Macro e-nets representation of parallel systems / J. D. Noe, G. J. Nutt // IEEE Transactions on Computers, vol. 31(9), August 1973. — P. 718-727.

220. Ajmone Marsan M. Modelling with Generalised Stochastic Petri Nets / M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli, G. Franceschinis. — John Wiley and Sons, 1995. — 324 p.

221. Florin G. Les reseaux de Petri stochastiques / G. Florin, S. Natkin // Science Informatiques, vol. 4(1), February 1985.

222. Molloy M. K. On the Integration of Delay and Throughput Measures in Distributed Processing Models: PhD thesis / M. K. Molloy. — UCLA, Los Angeles, CA, 1981.

223. Frost V. Traffic Modeling For Telecommunications Networks / V. Frost, B. Melamed // IEEE Communications Magazine, March 1994. — P. 70–81.

224. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. — М.: Техносфера, 2003. — 512 с.

225. Тихонов В.И. Статистическая радиотехника / В.И. Тихонов. — М.: Сов. радио, 1966. — 690 с.

226. Асанов М.О. Дискретная математика: графы, матроиды, алгоритмы / М.О. Асанов, В.А. Баранский, В.В. Расин. — М.: Регулярная и хаотическая динамика, 2001. — 288 с.

227. Dale R. Authoring on Demand Natural Language Generation of Hypermedia Documents / R. Dale, M. Milosavljevic // In Proceedings of the First Australian Document Computing Symposium. ADCS, Australia, 2005.

228. Математический энциклопедический словарь. / Гл. ред. Ю.В. Прохоров; ред. кол.: С.И. Адян, Н.С. Бахвалов, В.И. Битюцков, А.П. Ершов, Л.Д. Кудрявцев, А.Л. Онищик. — М.: Сов. энциклопедия, 1988. — 847 с., ил.

229. Коллеров А.С. Модель Web-сервера как сеть массового обслуживания с открытой очередью и запросами различных классов / А.С. Коллеров // Безопасность информационного пространства: материалы региональной научно-практической конференции. — Екатеринбург: ГОУ ВПО УрГУПС, 2008. — С. 189.

230. Коллеров А.С. Временные параметры, описывающие работу Web-сервера / А.С. Коллеров // Безопасность информационного пространства: материалы VIII регион. науч.-практ. конф. студ., аспирантов и молодых ученых, 17-18 ноября 2009 г. — Челябинск: Издательский центр ЮУрГУ, 2009. — С. 180.

231. Менаске Д., Алмейда В. Производительность Web-служб. Анализ, оценка и планирование: Пер. с англ./ Д.А. Менаске, В.А.Ф. Алмейда. — СПб: ООО «ДиаСофтЮП», 2003. — 480 с.

232. RFC 791 (IP) / Режим доступа: http://www.ietf.org/rfc/rfc791.txt.

233. RFC 793 (TCP) / Режим доступа: http://www.ietf.org/rfc/rfc791.txt.

234. RFC 2068 (HTTP) / Режим доступа: http://www.ietf.org/rfc/rfc2068.txt.

235. A Complete Guide to the Common Vulnerability Scoring System Version 3.0 [Электронный ресурс] http://www.first.org/cvss/cvss-guide.html.

236. Котенко И.В., Степашкин М.В. Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. INSIDE, вып. 3. — 2006 — С. 2-11.

237. Павленко Е.Ю., Ярмак А.В., Москвин Д.А. Контроль безопасности информационных систем на основе анализа графа событий, полученных в результате мониторинга // Проблемы информационной безопасности. Компьютерные системы. — 2017. № 2. — С. 31-38.

238. Марков А.С., Цирлов В.Л., Барабанов А.В. Разработка методики испытаний межсетевых экранов по требованиям безопасности информации // Вопросы защиты информации. — 2011. № 3. — С. 19-24.

239. Сухов А. М., Горбачев И. Е., Якунин В. И. Методика моделирования процесса функционирования системы обнаружения вторжений в компьютерную сеть в задачах исследования эффективности // Проблемы информационной безопасности. Компьютерные системы. — 2017. № 2. — С. 23-30.

240. Veldman I. Matching Profiles from Social Network Sites. Master's thesis, University of Twente, 2009.

241. Бартунов С.О., Коршунов А.В. Идентификация пользователей социальных сетей в Интернет на основе социальных связей // Доклады Всероссийской научной конференции "Анализ изображений, сетей и текстов". — АИСТ'2012. Екатеринбург, 16-18 марта 2012 г.

242. Сваровский С.Т. Аппроксимация функций принадлежности значений лингвистической переменной // Математические вопросы анализа данных. – Новосибирск, ВЦ СО АН СССР, 1980. – С. 127-131.

243. Круглов В.В. Нечеткая логика и искусственные нейронные сети: Учеб. пособие / В.В. Круглов, М.И. Дли, Р.Ю. Голунов – М.: Издательство Физико-математической литературы, 2001. – 224 с.

244. Захаров А.А., Захарова И.Г. Компетентностный подход к определению содержания образования в области информационных технологий для специальности «Компьютерная безопасность» // Материалы Международной научно-методической конференции «Формирование инновационного потенциала вузов в условиях болонского процесса». — Тюмень, Тюменский государственный университет, 2007. — С. 219-221.

245. Попов Е.Ф., Тюкова А.А., Фучко М.М., Захаров А.А. Выявление нетипичных событий средствами статистического анализа. — Вестник УрФО. Безопасность в информационной сфере. — 2015. № 1 (15). — С. 44-47.

246. Соколов А.Н., Лужнов В.С. Специализированные инструменты автоматизированного анализа защищенности информационных систем. — Вестник УрФО. Безопасность в информационной сфере. — 2016. № 2 (20). — С. 33-38.

247. Соколов А.Н., Лужнов В.С. Математическая модель атак на информационные ресурсы корпоративных автоматизированных систем. — Инновационные технологии: теория, инструменты, практика. — Пермский национальный исследовательский политехнический университет, 2015. № 1. — С. 299-304.

248. Алабугин С.К., Пятницкий И.А., Соколов А.Н. Применение рекуррентных и сверточных нейронных сетей для выявления аномалий технологического процесса // Вестник УрФО. Безопасность в информационной сфере, 2019. — Вып. 32. — № 2. — С. 60-65.

249. Асяев Г.Д., Соколов А.Н. Обнаружение вторжений на основе анализа аномального поведения локальной сети с использованием алгоритмов машинного обучения с учителем // Вестник УрФО. Безопасность в информационной сфере, 2020. — Вып. 35. — № 1. — С. 77-83.

250. Попов Е.Ф., Тюкова А.А., Фучко М.М., Захаров А.А. Выявление нетипичных событий средствами статистического анализа // Вестник УрФО. Безопасность в информационной сфере, 2014. — Вып. 14. — № 4. — С. 24-27.

251. Титов С.С., Медведев Н.В. К вопросу об информационной безопасности при делегировании прав // Дискуссия, 2012. — № 8 (26). — С. 111-114.

252. Титов С.С., Геут К.Л. О рекуррентных соотношениях в информационной безопасности // Вестник УрФО. Безопасность в информационной сфере, 2017. — Вып. 23. — № 1. — С. 24-27.

253. Гайдамакин Н.А., Хорьков Д.А. Модель атакующего воздействия на автоматизированные системы в рамках развития аппарата сетей Петри // Проблемы информационной безопасности. Компьютерные системы. — 2013. № 1. — С. 73-80.

254. Гайдамакин Н.А., Синадский Н.И. Теоретико-графовый подход к задачам количественного анализа защиты информации в компьютерных системах // Научно-техническая информация. Серия 2: Информационные процессы и системы. — 2000. № 9. — С. 12–19.

255. Хорьков Д.А. Методы тестирования сетевых систем обнаружения компьютерных атак // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2012. № 6. — С. 9-15.

256. Хорьков Д.А. О возможности использования математического аппарата сетей Петри для моделирования компьютерных атак // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2009. Т. 1. № 2. — С. 49-50.

257. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности. М.: — Гелиос АРВ, 2005. — 224 с.

258. Царегородцев А.В., Кислицын А.С. Основы синтеза защищенных телекоммуникационных систем / Под ред. Е.М. Сухарева. Кн. 6. — М.: Радиотехника, 2006. — 256 с.

Публикации автора по теме диссертации

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

259. 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 Engi-

neering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0559-0562. (0,4 п.л./0,1 п.л.) (Scopus).

260. 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).

261. 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).

262. 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.)

263. 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.)

264. 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.)

265. **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)

266. 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.)

267. 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.)

268. **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.)

269. 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.)

270. 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.)

271. 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.)

272. 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 государственной регистрации программ для ЭВМ

273. 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.

274. 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.

275. 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.

276. 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.

Иные публикации

277. Зайникаев А.Р., Муратов А.А., **Синадский Н.И.** Количественная оценка защищенности объектов информационно-телекоммуникационных систем и сетей на основе формирования графов атак с применением перечней уязвимостей и карты сетевой топологии. — Вестник УрФО. Безопасность в информационной сфере. — 2011. № 2. — С. 62-68.

Издания по материалам конференций

278. Агафонов А.В., **Синадский Н.И.** Представление модели сетевой среды как особи генетического алгоритма в задаче тестирования телекоммуникационного оборудования // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 9-14.

279. Безуглая М.В., Патрушева О.М., **Синадский Н.И.**, Сушков П.В. Расчет показателя сходства учетных записей пользователей социальных сетей на основе анализа атрибутов и структуры социальных связей // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 19-23.

280. Богданов В.В., **Синадский Н.И.** Разработка элемента автоматизированной системы активного аудита: сканер портов / В.В. Богданов, Н.И. Синадский // Информационная безопасность региона, сборник научных трудов I Всероссийской научно-практической конференции 5–7 октября 2004 г. — Челябинск: Изд-во ЮУрГУ, 2005. — С. 200.

281. Богданов В.В., **Синадский Н.И.** Многоагентная система обнаружения компьютерных атак с учетом внешних и внутренних воздействий / В.В. Богданов, Н.И. Синадский // Безопасность информационного пространства: материалы Всероссийской научно-практической конференции. — Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2005. — С. 45–46.

282. Власов А.О., **Синадский Н.И.** Формирование набора метрик для тестирования Web Application Firewalls // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 30-34.

283. Гуков К.В., **Синадский Н.И.** Генератор массива данных, имитирующего телетрафик потоков вызова абонентов сети сотовой связи // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 183-184.

284. Карпенко Д.А., Борисенко П.Н., **Синадский Н.И.** Функциональная схема вычислительного кластера на основе модификации операционной системы Pelican Linux // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 112-114.

285. Пименов Е.Д., **Синадский Н.И.** Повышение интенсивности генерации трафика в задаче нагрузочного тестирования сетевого оборудования // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 131-132.

286. Семенищев И.А., Синадский А.Н., **Синадский Н.И.** Алгоритм формирования массива биллинговой информации на основе статистической модели поведения абонентов сотовой связи // Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. — Курган: Курганский ГУ, 2016. — С. 199-203.

287. Семенищев И.А., Синадский А.Н., **Синадский Н.И.** Статистические характеристики массива биллинговой информации при моделировании поведения абонентов сетей сотовой связи // Сборник материалов 12-ой между-

народной молодежной научно-технической конференции «РТ–2016». — Севастополь, Севастопольский государственный университет, 2016. — С. 207;

288. Семенищев И.А., Синадский А.Н., **Синадский Н.И.** Моделирование угроз безопасности АСУ ТП на основе учебно-экспериментального стенда // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 239-242.

289. Синадский А.Н., Семенищев И.А., **Синадский Н.И.** Создание учебных массивов условно-реальных данных о взаимодействии пользователей сетей сотовой связи // Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства»: в 2 томах. — Челябинск: ЧелГУ, 2018. — С. 217-223;

290. Синадский А.Н., **Синадский Н.И.** Формальная математическая модель синтеза массива биллинговой информации // Сборник материалов XVI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». — Екатеринбург: УрФУ, 2017. — С. 258-261;

291. Синадский А.Н., **Синадский Н.И.,** Семенищев И.А. Статистико-событийная модель синтеза биллинговой информации // Сборник материалов VI Международной научной конференции «Математическое и компьютерное моделирование», посвященной памяти Б.А. Рогозина. — Омск: ОмГУ, 2018. — С. 95-98;

292. Синадский А.Н., Сушков П.В., **Синадский Н.И.** Применение моделей сложных сетей в задаче синтеза массивов данных о взаимодействии пользователей информационно-телекоммуникационных сервисов // Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых: в 2 томах. — Челябинск: ЧелГУ, 2018. — С. 223-228;

293. **Синадский Н.И.**, Сушков П.В. Выделение максимальной общей части социальных графов на основе модифицированного метода определения

частичного изоморфизма. — В сборнике: Инновационный транспорт - 2016: специализация железных дорог. Материалы Международной научно-технической конференции, посвященной 60-летию основания Уральского государственного университета путей сообщения. — 2017. — С. 766-771.

294. **Синадский Н.И.**, Щелконогов Е.Г. Применение модели «input m/g/∞» для генерации самоподобного трафика // Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. — Курган: Курганский ГУ, 2016. — С. 221-224.

295. **Синадский Н.И.**, Щелконогов Е.Г. Сравнение характеристик сетевого оборудования на основе результатов тестирования синтезируемым трафиком // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 165-168.

296. Сушков П.В., **Синадский Н.И.** Алгоритм формирования статической структуры социальных графов для создания массивов условно-реальных данных // Журнал «Современные проблемы радиоэлектроники и телекоммуникаций». — 2018. № 1. — С. 199;

297. Сушков П.В., **Синадский Н.И.** Модифицированный метод оценки частичного изоморфизма социальных графов // Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. — Курган: Курганский ГУ, 2016. — С. 207-210.

298. Фартушный А.В., **Синадский Н.И.** Визуализация связей взаимодействующих объектов компьютерных систем // Безопасность информационного пространства: сборник трудов XIV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / сост. А.А. Захаров. — Тюмень: Издательство Тюменского государственного университета, 2016. — С. 249-251.

299. Гибилинда Р.В., **Синадский Н.И.** Идентификация воздействий на файлы и верификация массивов данных, содержащих информацию о воздействиях, при расследовании инцидентов информационной безопасности // Со-

временные проблемы радиоэлектроники и телекоммуникаций: сб. науч. Тр. / под ред. Ю.Б. Гимпилевича. — Севастополь: Изд-во РНТОРЭС им. А.С. Попова, СевГУ, 2020. — № 3. — С. 219.

300. Гибилинда Р.В., **Синадский Н.И.** Автоматизация процессов идентификации воздействий на файлы с применением кластеризационного метода при расследовании инцидентов информационной безопасности // II Всероссийская научная конференция (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (FISP-2020), 2020. — С. 284-287.

Учебные пособия

301. Андрончик А.Н., Богданов В.В., Домуховский Н.А., Коллеров А.С., **Синадский Н.И.**, Хорьков Д.А., Щербаков М.Ю. Защита информации в компьютерных сетях. Практический курс: учебное пособие / под ред. Н.И. Синадского. — Екатеринбург : УГТУ-УПИ, 2008. — 248 с.

302. Коллеров А.С., **Синадский Н.И.**, Хорьков Д.А. Системы обнаружения компьютерных атак. Учебное пособие для вузов. — М.: Горячая линия – Телеком, 2021. — 124 с.: ил.

303. Гибилинда Р.В., Коллеров А.С., **Синадский Н.И.**, Хорьков Д.А., Фартушный А.В. Аудит информационной безопасности компьютерных систем. Учебное пособие для вузов. — М.: Горячая линия – Телеком, 2021. — 126 с.: ил.

304. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие / А.Н. Андрончик, А.С. Коллеров, **Н.И. Синадский**, М.Ю. Щербаков ; под общ. ред. Н.И. Синадского. — Екатеринбург : Изд-во Урал. ун-та, 2014. — 180 с.

305. **Синадский Н.И.** Информационно-методическое обеспечение учебного процесса «Комплект учебных материалов и заданий для самостоятельной работы для слушателей курсов повышения квалификации "Методы и средства защиты компьютерной информации"» [Электронный ресурс] / Н.И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А.М.

Горького, ИОНЦ «Информационная безопасность», [и др.]. — Электрон. дан. и прогр. (1,8 ГБ). — Екатеринбург : [б. и.], 2008.

306. **Синадский Н.И.** Учебно-методический комплекс дисциплины «Защита информации в компьютерных сетях» [Электронный ресурс] / Н.И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А.М. Горького, ИОНЦ «Информационная безопасность» [и др.]. — Электрон. дан. (13,3 Мб). — Екатеринбург : [б. и.], 2008.

307. **Синадский Н.И.** Учебно-методический комплекс дисциплины «Специализированные программно-аппаратные средства защиты информации» [Электронный ресурс] / Н.И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ «Информационная безопасность» [и др.]. — Электрон. дан. (13,2 Мб). — Екатеринбург : [б. и.], 2008.

308. **Синадский Н.И.** Системы мониторинга, управления и обнаружения атак в компьютерных сетях : учебное пособие / Е.А. Гузенкова, А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков. — Екатеринбург : УрГУПС, 2016. — 292 с.

309. **Синадский Н.И.** Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106 / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков ; науч. ред. Н. А. Гайдамакин ; Урал. гос. техн. ун-т - УПИ. — Екатеринбург : УГТУ-УПИ, 2008. — 182 с.

310. **Синадский Н.И.** Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н.И. Синадский ; науч. ред. В.В. Бакланов. — Екатеринбург : УГТУ-УПИ, 2007. — 136 с.

311. Анализ и восстановление данных в операционной системе MS Windows : учебное пособие / Ю.Д. Корольков, **Н. И. Синадский**. — Иркутск : ИГУ, 2012. — 112 с.

312. Духан Е. И. и др. Средства криптографической защиты информации : учеб. пособие / Е.И. Духан, Ю.Д. Корольков, **Н.И. Синадский**. — Иркутск : Изд-во ИГУ, 2012. – 113 с.

ПРИЛОЖЕНИЕ 1. АКТЫ ВНЕДРЕНИЯ

Уральский Центр Систем Безопасности
Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

620100
г. Екатеринбург
ул. Ткачей, д. 6

тел.: +7(343) 379-98-34
факс: +7(343) 382-05-63

info@ussc.ru
www.USSC.ru

УТВЕРЖДАЮ

Заместитель генерального директора по производству ООО «УЦСБ» к.т.н
В.В. Богданов

15. 12 2015 г.

АКТ ВНЕДРЕНИЯ

Аппаратно-программного комплекса обнаружения уязвимостей телекоммуникационного оборудования к атакующему воздействию типа «отказ в обслуживании»

г. Екатеринбург 15. 12 2015 г.

Аппаратно-программный комплекс обнаружения уязвимостей телекоммуникационного оборудования к атакующему воздействию типа «отказ в обслуживании», разработанный аспирантом А.В. Агафоновым и к.т.н., доцентом Н.И. Синадским, был внедрен в 2015 году в Обществе с ограниченной ответственностью «Уральский Центр Систем Безопасности» в тестовом режиме эксплуатации с целью тестирования образцов телекоммуникационного оборудования, применяемого в автоматизированных системах управления технологическими процессами (АСУ ТП).

С помощью комплекса был протестирован промышленный коммутатор MOXA EDS-408A-PN. В результате были обнаружены сочетания параметров сетевого трафика, при которых значительно возрастают (в сравнении со штатным режимом функционирования) задержки передачи данных и потери пакетов, что может привести к нарушениям функционирования приложений АСУ ТП, требующих передачи данных в реальном масштабе времени.

Применение комплекса позволяет повысить эффективность мероприятий по оценке защищенности технологической инфраструктуры предприятий промышленности.

Данный комплекс оценивается как эффективный инструмент для выявления уязвимостей телекоммуникационного оборудования к атакующему воздействию типа «отказ в обслуживании».

Согласовано:
Руководитель перспективного направления Департамента системной интеграции С.Н. Кацапов

УТВЕРЖДАЮ

Генеральный директор ООО «УЦСБ»
к.т.н. В.В. Богданов

____.____ 2021 г.

АКТ ВНЕДРЕНИЯ

Комплекса программных средств идентификации воздействий на файлы при расследовании инцидентов информационной безопасности

г. Екатеринбург ____.____ 2021 г.

Комплекс программных средств идентификации воздействий на файлы, разработанный Р.В. Гибилиндой и к.т.н., доцентом Н.И. Синадским, был внедрен в 2020 году в обществе с ограниченной ответственностью «Уральский центр систем безопасности» в режиме опытной эксплуатации с целью использования комплекса для расследования инцидентов информационной безопасности, возникающих, в том числе, в процессе эксплуатации автоматизированных систем управления технологическими процессами.

Применение комплекса программных средств позволило восстановить ход инцидента (определить файлы, которые подвергались воздействиям и установить временной интервал возникновения инцидента), сократив временные затраты аналитика на проведение расследования инцидента информационной безопасности до 20 минут.

Использование комплекса значительно ускоряет проведение мероприятий по реагированию / расследованию инцидентов информационной безопасности, возникающих в, в том числе, в информационной инфраструктуре промышленных предприятий.

Директор Корпоративного центра мониторинга ИБ средств и систем информатизации ООО «УЦСБ» Амиров Р.М.

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина» (УрФУ)

ул. Мира, 19, Екатеринбург, 620002,
факс: +7 (343) 375-97-78; тел.: +7 (343) 374-38-84
контакт-центр: +7 (343) 375-44-44, 8-800-100-50-44 (звонок бесплатный)
e-mail: rector@urfu.ru, www.urfu.ru
ОКПО 02069208, ОГРН 1026604939855, ИНН/КПП 6660003190/667001001

17.02.2022 № 33.02-32/120

На № _____ от _____

УТВЕРЖДАЮ
Проректор по науке
_____ А.В. Германенко
«___» _____ 2022 года

АКТ

О внедрении результатов диссертационного исследования
Синадского Николая Игоревича

Мы, нижеподписавшиеся, представители Уральского Федерального университета имени первого Президента России Б.Н. Ельцина (УрФУ) директор Института Радиоэлектроники и Информационных технологий–РтФ (ИРИТ-РтФ) Илья Николаевич Обабков и директор учебно-научного центра Информационная безопасность (УНЦ ИБ) Поршнев Сергей Владимирович составили настоящий акт о том, что результаты диссертационного исследования Синадского Н.И. используются при реализации учебного процесса по дисциплинам «Программно-аппаратные средства обеспечения информационной безопасности» и «Предупреждение и обнаружение компьютерных атак» по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»,

- в том числе компьютерный полигон по расследованию инцидентов информационной безопасности, развернутый на лабораторной базе УНЦ ИБ, применяется при проведении практических занятий по обнаружению комплексных компьютерных атак, проведению аудита безопасности и расследованию инцидентов в компьютерных системах.

Директор ИРИТ-РтФ _____ И.Н. Обабков

Директор УНЦ ИБ _____ С.В. Поршнев

202752

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО – ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ
« Гамма »
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

620078, г. Екатеринбург, ул. Студенческая, д. 51
620078, г. Екатеринбург, а/я 65

Тел / факс: (343) 362-40-04
E-mail: info@gammaural.ru,

«28» июня 2022 г. № 557

АКТ
об использовании результатов диссертационного исследования Синадского Николая Игоревича

Мы, представители Екатеринбургского научно-технического центра ФГУП «НПП «Гамма» первый заместитель директора Аникин Д.В. и начальник отдела информационных технологий Елаков Д.О. составили настоящий акт об использовании результатов диссертационного исследования Синадского Н.И. «Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности» в рамках проведения проектных работ по созданию учебного стенда, предназначенного для проведения практических занятий курсов переподготовки специалистов в области информационной безопасности по программам: «Техническая защита информации, содержащей сведения, составляющие государственную тайну» (в части защиты от несанкционированного доступа), «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

Предложенный Синадским Н.И. научно-методический инструментарий позволил осуществить проектирование компьютерного полигона (учебного стенда) для проведения практических занятий, обеспечивающего имитацию условий функционирования защищенных сетей в условиях компьютерных атак различной интенсивности.

Проведение практических занятий на данном учебном стенде существенно повысит уровень практических навыков обучаемых (переподготавливаемых) специалистов в области информационной безопасности.

Первый заместитель директора Д.В. Аникин

Начальник отдела информационных технологий Д.О. Елаков

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
Институт Радиоэлектронных Систем

620137, г. Екатеринбург, ул. Июльская, д. 41.
Тел./факс: 8 (343) 374-24-64, 374-86-67
E-mail: roman@irsural.ru, WWW: http://www.irsural.ru/
ИНН: 6659060370, КПП: 667801001
р/с 40702810316540007885 в УРАЛЬСКИЙ БАНК ПАО "СБЕРБАНК"
БИК 046577674, к/с 30101810500000000674, ОКВЭД 73.10, ОКПО 54128475

11001 от 10.06.2022 г.

АКТ

об использовании результатов диссертационного исследования

Синадского Николая Игоревича

Результаты диссертационного исследования Синадского Н.И. «Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности» использованы в ООО «Институт Радиоэлектронных Систем» в рамках проведения проектных работ по созданию учебного стенда, предназначенного для проведения практических занятий на курсах профессиональной переподготовки специалистов в области информационной безопасности по программам: «Техническая защита информации, содержащей сведения, составляющие государственную тайну» (в части защиты от несанкционированного доступа), «Технологии и средства обеспечения компьютерной безопасности».

Предложенные Синадским Н.И. программные компоненты применены при создании учебного стенда для проведения практических занятий по изучению систем обнаружения вторжений, обеспечивающего имитацию компьютерного атакующего воздействия различной интенсивности.

Проведение практических занятий на данном учебном стенде существенно повысит уровень практических навыков обучаемых в сфере обеспечения компьютерной безопасности.

Генеральный директор Р.В. Гильмияров

Уральский Центр Систем Безопасности
Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

620100
г. Екатеринбург
ул. Ткачей, д. 6

тел.: +7(343) 379-98-34
факс: +7(343) 382-05-63

info@ussc.ru
www.USSC.ru

АКТ

о внедрении результатов диссертационного исследования

Синадского Николая Игоревича

Результаты диссертационного исследования Синадского Н.И. «Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности» использованы в ООО «Уральский центр систем безопасности» в рамках проведения проектных работ по созданию учебного компьютерного полигона, предназначенного для проведения практических занятий со студентами, обучающимися по направлению «Информационная безопасность».

Предложенные Синадским Н.И. программные компоненты внедрены в структуру полигона и позволяют изучать и проводить тестирование средств обнаружения компьютерных атак, средств анализа защищенности и телекоммуникационного оборудования с применением специализированных стендов.

Проведение практических занятий на учебных стендах полигона существенно повышает уровень практических навыков обучаемых в сфере обеспечения компьютерной безопасности.

Генеральный директор В.В. Богданов