П.И. ТУТУБАЛИН, В.С. МОИСЕЕВ

ВЕРОЯТНОСТНЫЕ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ

Казань
2008

УДК 004.056:004.94
ББК 67.408
Т 91

Редактор серии:

В.С. Моисеев – заслуженный деятель науки и техники Республики Татарстан, доктор технических наук, профессор.

Рецензенты:

О.В. Есиков – заместитель начальника кафедры математического, информационного и программного обеспечения АСУ Тульского артиллерийского инженерного института, доктор технических наук, профессор полковник;

В.И. Глова – доктор технических наук, профессор кафедры средств информационной безопасности Казанского государственного технического университета им. А.Н. Туполева.

Тутубалин П.И., Моисеев В.С.

Т 91 Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления: Монография. – Казань: РИЦ «Школа», 2008. – 144 с., ил. (Серия «Современная прикладная математика и информатика»)

ISBN 5-94712-002-X

В монографии рассмотрены теоретические и практические основы создания максимально информационно безопасных с точки зрения вероятностных критериев автоматизированных систем обработки информации и управления, а так же разработаны подходы и методы повышения эффективности использования средств информационной безопасности.

Монография предназначена для широкого круга инженерно-технических работников, занимающихся вопросами разработки автоматизированных систем специального назначения.

ISBN 5-94712-002-X

Предисловие редактора серии

Современный этап развития общества характеризуется у нас в стране и за рубежом активным переходом от компьютеризации к информатизации практически всех сфер его деятельности

При этом главным его препятствием, на наш взгляд, является отсутствие глубоко проработанных теоретических основ информатизации деятельности человека, организации, региона, государства общества в целом и, в частности, теории оптимального проектирования эксплуатации и развития больших и сложных систем, в которые внедряются информационные технологии.

Основу такой теории и технологии должны составить современные модели, методы и средства прикладной математики и информатики. При этом рассмотрение вопросов автоматизации формирования и оптимизации всевозможных решений должно ориентироваться на широкое применение математических моделей, методов и алгоритмов, реализуемых в составе соответствующих прикладных информационных технологий.

К настоящему времени нельзя говорить об информатике как о завершённой области научного знания с четко определенными предметом, целями, задачами и методами исследований. При этом практически отсутствуют научно обоснованные рекомендации по организации эффективной разработки, внедрения, эксплуатации и развития создаваемых информационных систем. Выход из этого положения видится нам в опережающем развитии такой ее составляющей, как «прикладная информатика».

Главной целью прикладной информатики является создание инженерных методик разработки современных информационных систем и технологий различного назначения. В этих методиках должны найти глубокое применение современные и перспективные модели и методы прикладной математики, языки программирования, инструментальные средства и технологии разра-

ботки защищенных программ и баз данных, операционные системы и среды, системы управления базами и банками данных, аппаратно-программные средства хранения, обработки и передачи информации.

Активное развитие прикладной информатики позволит обобщать получаемые результаты в рамках соответствующих теорий, а это будет являться стимулом к развитию, как теоретической информатики, так и прикладной математики. Полученные при этом модели и методы будут использоваться в соответствующих методиках создания, эксплуатации и развития информационных систем и технологий их функционирования.

В серии книг «Современная прикладная математика и информатика», ориентированных на специалистов в этих областях, а также на студентов и аспирантов соответствующих специальностей, выходит очередная монография, посвящённая некоторым математическим моделям и методам, позволяющим обеспечить информационную безопасность автоматизированных систем обработки информации и управления специального назначения. Полученные научные результаты могут быть положены в основу методик разработки эффективных информационных систем и прикладных информационных технологий различного назначения.

В серии “Современная прикладная математика и информатика” вышли книги:

Моисеев В.С., Козар А.Н. Основы теории применения управляемых артиллерийских снарядов. Казань: изд-во КВАКУ, 2004.

Рассмотрена теория применения управляемых артиллерийских снарядов, даны модели и методы их оптимального планирования. Особое внимание уделяется методам преодоления управляемыми артиллерийскими снарядами зон активной защиты целей и планированию одновременного удара по цели несколькими управляемыми артиллерийскими снарядами.

Книга может быть полезна как для слушателей и курсантов высших военных учебных заведений, так и для работников научно-исследовательских институтов.

Медведев В.И. Программирование на C++, C++.NET и C#. Казань: Мастер Лайн, 2005.

Излагаются основные понятия и методика разработки объектно-ориентированных программ на языках C++, C++.NET и C# с использованием библиотеки классов Framework .NET платформы. Особое внимание уделено разработке Windows приложений из потоковых объектов и компонентов.

Монография предназначена для студентов вузов по направлению вычислительная техника и информатика, а также для всех, владеющих языком программирования C и желающих освоить .NET технологию программирования.

Зайдуллин С.С., Моисеев В.С. Математические модели и методы управления территориально распределёнными системами. Казань: Мастер Лайн, 2005.

Рассмотрены теоретические основы управления сложными территориально распределёнными организационно-техническими системами. Решение задач анализа, синтеза и управления такими системами выполняется на основе специальных прикладных информационных технологий.

Монография предназначена для широкого круга инженерно-технических работников, занимающихся вопросами разработки территориально распределённых систем.

Медведев В.И. Разработка компонентов и контейнеров на C++.NET и C#.. Казань: Мастер Лайн, 2005.

Углублённо рассмотрено построение компонентов, контейнеров и объединение компонентов в контейнере с предоставлением сервисных услуг на базе библиотеки классов .NET Framework.

Монография имеет практическую направленность и предназначена для всех, владеющих объектно-ориентированным программированием на языках C++.NET и C# и желающих освоить программирование .NET компонентов.

Рахматуллин А.И., Моисеев В.С. Математические модели и методы оптимизации нестационарных систем обслуживания. Казань: РИЦ «Щкола», 2006.

Рассмотрены теоретические основы оптимизации и адаптивного управления процессами обслуживания в сложных информационных и организационно-технических системах. Применение разработанных математических моделей, методов и алгоритмов иллюстрируется на практических задачах оптимизации и адаптивного управления функционированием систем обслуживания.

Монография предназначена для широкого круга инженерно-технических работников, занимающихся вопросами исследования и оптимизации нестационарных процессов в сложных системах различного назначения.

Медведев В.И. .NET компоненты, контейнеры и удаленные объекты. Казань: РИЦ «Щкола», 2006.

Книга посвящена компонентам – основным программным единицам при построении Windows-приложений в .NET технологии. Кроме компонентов и контейнеров, объединяющих компоненты в коллекции, значительное внимание уделено удалённым объектам и событиям, а также разработке использующих их распределённых приложений.

Для студентов и преподавателей вузов по направлению вычислительной техники и информатики. Представляет интерес для всех, знающих основы языков C++.NET и C# и желающих овладеть технологией создания и использования .NET компонентов для распределённых Windows приложений.

Козар А.Н., Борзов Г.Е., Рахматуллин А.И., Сотников СВ. Информатика ракетных войск и артиллерии. -Казань: «Отечество», 2006.

Работа посвящена применению современных программных оболочек типа Delphy для создания информационных технологий управления действиями ракетных войск и артиллерии тактического звена.

Габитов Р.И., Емалетдинова Л.Ю. Модели и методы разработки автоматизированных систем организационного управления: Монография. – Казань: РИЦ «Школа», 2007. - с.120, ил. (Серия «Современная прикладная математика и информатика»).

В монографии рассмотрены теоретические основы проектирования унифицированного программного обеспечения автоматизированных систем организационного управления технологическими процессами деятельности специалистов, а также оптимизационные модели, методы и алгоритмы, обеспечивающие эффективное функционирование проектируемой распределенной системы.

Монография предназначена для широкого круга инженерно-технических работников, занимающихся вопросами разработки автоматизированных систем организационного управления.

Валеев М.Ф., Емалетдинова Л.Ю. Автоматизация организационного управления технологическими процессами налогообложения граждан: Монография. – Казань:РИЦ «Школа», 2007. - с.136, ил. (Серия «Современная прикладная математика и информатика»).

В монографии рассмотрены теоретические основы проектирования программного обеспечения автоматизированных систем организационного управления технологическими процессами налогообложения граждан, а также предлагается методика краткосрочного прогнозирования доходов граждан на основе автоматизированного построения моделей временных рядов.

Монография предназначена для широкого круга инженерно-технических работников, занимающихся вопросами разработки автоматизированных систем организационного упроавления.

Заслуженный деятель
науки и техники РТ,
доктор технических наук,
профессор В.С.Моисеев

Введение

Проблема информационной безопасности является одним из важнейших аспектов развития современного общества. И конечно же эта проблема актуальна при разработке и эксплуатации автоматизированных систем обработки информации и управления (АСОИУ) в связи с тем, что в подобных системах хранится и обрабатывается конфиденциальная и секретная информация, порой составляющая государственную и военную тайны. Следует отметить, что в настоящее время работа в этих направлениях ведется в основном на эмпирической базе. Одной из причин последнего является отсутствие теоретических основ информационной безопасности (ИБ) современных АСОИУ. В этой связи весьма актуальным является создание прикладной теории безопасности информационных систем. Вопросам оценки и повышения ИБ при решении практических задач посвящены работы Воробьева А. А., Гераси-менко В.А., Гловы В.И., Есикова О.В., Зегжды Д.П., Зима В.М., Ивашко А.М., Казарина О.В., Киселева В.Д., Кислицина А.С., Кузнецов Н.А., Кульба В.В., Микрин Е.А., Мельникова В.В., Молдовяна А.А., Молдовяна Н.А., Романец Ю.В., Тимофеева П.А., Шаньгина В.Ф., Тейлора Д.Д., Ван Дер Спека Г.А., Миллера С.Н., Отто В.Л. и других отечественных и зарубежных авторов.

Как показал анализ состояния проблемы, в настоящее время существует огромное количество средств информационной безопасности (СИБ) предназначенных для различных объектов, использующих и обрабатывающих конфиденциальную информацию. Набор этих СИБ может образовывать сложные, многоуровневые, территориально-распределенные системы обеспечения ИБ. Задача оценки уровня ИБ данных систем является первостепенной, но на сегодняшний день слабо проработанной.

Отметим, что задача разработки АСОИУ с учетом требований, предъявляемым к ним с точки зрения ИБ на сегодняшний день не достаточно изучена и остается не решенной в полном объеме.

Неотъемлемым аспектом разработки систем обеспечения ИБ является их испытание на устойчивость при попытках несанкционированного доступа (НСД) к информации, обрабатываемой в АСОИУ. В доступной литературе описано мало перспективных подходов и методов, позволяющих повысить ИБ АСОИУ обрабатывающих конфиденциальную информацию. Отметим, что для определения степени ИБ АСОИУ в настоящее время в основном используются экспертные оценки. Это связано с отсутствием общепринятых подходов и методов получения количественных оценок ИБ АСОИУ. Вместе с тем к настоящему времени накоплена достаточно большая статистика эксплуатации СИБ АСОИУ. Это позволяет использовать аппарат теории вероятностей и математической статистики для получения количественных оценок ИБ СИБ АСОИУ.

В монографии рассмотрены основные задачи прикладной теории ИБ, введены принципы и основные модели прикладной теории ИБ. Приведены базовые теоретико-множественные модели такой теории, включающие в себя: концептуальную модель АСОИУ и концептуальную модель СИБ информационно технических продуктов.

Так же приведена методика определения компромиссного значения требуемой вероятности обеспечения ИБ АСОИУ с использованием двухкритериальной задачи оптимизации, учитывающей стоимость разрабатываемой системы и защищенность от НСД. Описана методика формирования допустимых значений вероятностей обеспечения конфиденциальности, целостности и доступности процессов обработки данных АСОИУ на основании прогнозируемых интенсивностей атак на соответствующие компоненты АСОИУ. Сформированы требования, предъявляемые к данным, задачам и техническим средствам с точки зрения ИБ.

Третья глава монографии посвящена описанию предлагаемых вероятностных моделей и методов обеспечения ИБ АСОИУ. Рассмотрена математическая модель выделения критических элементов АСОИУ. Описан метод оптимального выбора СИБ АСОИУ на основе решения двухкритериальной задачи нелинейного булевского программирования. Для размещения конфиденциальной информации на серверах АСОИУ предлагается использовать двухкритериальную теоретико-игровую модель, рассмотрен вопрос реализации случайного механизма размещения конфиденциальных данных. Предложены методы и алгоритмы маскировки конфиденциальных данных в АСОИУ.

В работе отмечается важность задачи контроля работы СИБ, то есть их испытания на устойчивость при попытках НСД. Сформулированы цели и задачи автоматизированных испытаний СИБ. Приведена структура и функции автоматизированной системы испытаний СИБ. Разработаны алгоритм и методика проведения автоматизированных испытаний СИБ. Разработан состав программного обеспечения автоматизированных испытаний СИБ. Приведена классификация возможных наборов тестов СИБ.

Глава 1. Основные задачи прикладной теории информационной безопасности АСОИУ.

Проблема ИБ является одним из важнейших аспектов развития современного общества. В настоящее время решение этой проблемы в области разработки и эксплуатации информационных систем различного назначения (военных, технических, экономических, медицинских, социальных и др.) связано с разработкой всевозможных требований к обеспечению их безопасности [1–5] и созданием разнообразных аппаратных и программных СИБ от НСД [1–5,11,24,30,34].

Следует отметить, что работа в этих направлениях ведется в основном на эмпирической базе в связи с отсутствием теоретических основ ИБ современных АСОИУ. При этом существующие работы в области теории безопасности АСОИУ используют весьма абстрактный математический аппарат, использование которого при решении реальных задач анализа и синтеза СИБ практически невозможно. В работах [11,14,28,99,107] используется математический аппарат методики обработки экспертных оценок для формирования рисков, теоретикомножественный аппарат для описания оценки различных методов доступа к конфиденциальной информации. Применение их не позволяет получить достоверные количественно обоснованные оптимальные решения при построении СИБ. Использование абстрактных моделей СИБ позволяет использовать их за счет громоздкости применяемого математического аппарата только для решения задач малой размерности. В существующих работах очень редко встречается использование вероятностных моделей и методов, хотя к настоящему времени накоплен значительный объем статистики по видам атак.

1.1. Обзор состояния вопроса.

Вопросам применения количественных методов для оценки ИБ посвящено значительное число работ отечественных и зарубежных ученых. В ра-

ботах [1,2,4,5,41] введены основные понятия и определения ИБ компьютерных систем, приведено описание некоторых СИБ. Работа [3] раскрывает теоретические и прикладные аспекты проблемы обеспечения безопасности программного обеспечения компьютерных систем различного назначения. Особое внимание в ней уделено моделям и методам создания высокозащищенных и алгоритмически безопасных программ для применения в системах критических приложений. В той же работе приведена статистика реализаций нарушения ИБ.

Отметим, что существуют ряд руководящих документов [6,7, 52-54], регламентирующих выбор СИБ вычислительной техники, методы предотвращения НСД к информации, показатели защищенности от НСД к информации, а так же в них приведена классификация СИБ.

Монография [23] посвящена исследованиям в области управления разделением ресурсов распределенных информационных и телекоммуникационных систем. В работе предложены модели и алгоритмы обеспечения ИБ. Отмечены недостатки существующих СИБ. Приведены модели принципов проникновения и разрушения АСОИУ, а так же система ИБ информационных ресурсов от атак. Приведено несколько нетрадиционных подходов к обеспечению ИБ. В работе сделан упор на криптографические методы обеспечения ИБ и нет упоминания о возможности использования вероятностных методов для обеспечения ИБ.

В работах [8,15] сделана попытка описать выбор системы безопасности с учетом ее стоимости и качества полученной ИБ, однако не приводится математический вид этих критериев. Для выбора оптимального комплекса СИБ в работе [9] рассмотрено два критерия – стоимость системы и риск ее нарушения. Для их использования применена линейная свертка этих критериев. Решение находится методом градиентного спуска. При этом отмечается возможность использования ограничения по стоимости СИБ. Сделано допущение, что эффективность СИБ является функцией только их стоимости.

Проблеме обнаружения вторжений в систему ИБ посвящены работы [10,14]. В работе [10] используется вероятностный подход, который предусматривает использование набора однотипных средств обнаружения вторжения (СОВ). При этом количество видов СОВ может быть произвольным и определятся в зависимости от возможных типов атак. Для минимизации вероятности ложной идентификации вторжения используется мажоритарный подход. В работе [14] не конкретизированы способы получения вероятности выбора нарушителем способа атаки В работе [16] приведена модель нарушения ИБ в следствии воздействия внутренних угроз, но в не указан порядок определения вероятностей событий используемых в модели.

В современной литературе встречаются работы использующие игровые модели для обеспечения и анализа ИБ [13,51]. Так, например, в работе [13] на основе игровой модели предлагается осуществлять выбор стратегии ИБ. При этом в работе не учтено, что противник может предпринять несколько одновременных атак на различные подсистемы СИБ. Использование в работе игры с нулевой суммой тоже не всегда правомерно, так как конечные цели противника могут отличаться от целей СИБ. Не учтен факт того, что набор предопределенных ходов может меняться с течением времени. Кроме того, необходимо учитывать расходование времени и других ресурсов противника. В работе [51] игровая модели используется для анализа защищенности.

В литературе отмечается сложность проблемы моделирования процесса нарушения ИБ. В связи с этим в работе [17] представлен метод функциональной декомпозиции, позволяющий оценить взаимосвязь и взаимозависимость критериев безопасности на различных уровнях иерархической структуры информационной системы и таким образом, упростить процедуру построения обобщенной математической модели безопасности локальной либо глобальной информационной системы.

В работе [19] описаны методы формализации состояний, автоматизации моделирования и поиска функционально нестабильных состояний с

формальным доказательством отсутствия запрещенных траекторий, приводящих систему в опасные состояния.

Работа [20] посвящена описанию методов и экспериментальных средств комплексной оценки эффективности и универсальности способов мониторинга безопасности, базовой технологии предупреждения и обнаружения атак при динамических информационно-вычислительных процессах. Однако в работе не приведен математический аппарат для оценки собираемых данных.

На сегодняшний день множество работ посвящено СИБ, их использованию [11,12,18,21,22,24–35,38–41]. Однако в этих работах отсутствует описание выбора конкретных наборов СИБ для обеспечения ИБ АСОИУ. В работе [22] используются экспертные оценки для ранжирование возможных угроз ИБ по их опасности, при этом с изменением рангов уязвимостей изменится оценка защищенности ЛВС, то есть метод зависит от эксперта, назначающего ранги уязвимостей. В работах [11,32] приведена методика оценки защищенности с использованием экспертной оценки величины угрозы и качества СИБ и описано ПО необходимое для разработки экспертных систем (ЭС). Работа [34] содержит классификацию СИБ, угроз конфиденциальной информации и потенциальных нарушителей ИБ.

В доступной литературе [42–50] говорится о необходимости испытаний СИБ, но не указываются пути реализации этого важного этапа в создании и эксплуатации СИБ. В работе [42] приведен ряд критериев, для оценки стоимостно эффективных параметров системы и описан подход для выделения СИБ из предложенного перечня с учетом этих критериев. Отметим, что в работе для выбора СИБ используется эвристическое правило, не позволяющее найти точное решение поставленной задачи. При этом найденное решение является единственным. Предлагается получать информации о ИБ АСОИУ из протоколов испытаний фирм ее производителей, но не описаны, подходы и методики, позволяющие сделать это. Для надежной ИБ АСОИУ при по-

пытках НСД необходимо разрабатывать и использовать нормативные документы. В работе [44] приведена методика оценки ИБ АСОИУ военного назначения. Введены количественные значения уровней ИБ по принадлежности к классу защищенности АС. Суть метода состоит в использовании экспертных оценок эффективности СИБ, которые могут быть использованы для обеспечения ИБ.

Отметим некоторые задачи, которые не были рассмотрены, не смотря на большое количество публикаций посвященных вопросам ИБ. На сегодняшний день нет конкретной методики определение количественных характеристик ИБ. Не рассмотрены такие задачи как нахождение наиболее уязвимых узлов АСОИУ и оптимальный выбор программных, технических и других СИБ. Разработаны далеко не все методы размещения конфиденциальной информации в АСОИУ, позволяющие повысить ее защищенность от НСД. Остается открытым вопрос разработки методов и средств автоматизированных испытаний СИБ, позволяющих получать количественные оценки ИБ разрабатываемых и модифицируемых АСОИУ.

1.2. Предмет, основные принципы и цели прикладной теории информационной безопасности.

В настоящее время существуют различные определения понятия ИБ[108] В работе под информационной безопасность будем понимать защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям конфиденциальной (секретной) информации, за счет предупредительных действий, по выявлению и устранению уязвимых мест системы, в которой хранятся или обрабатываются данные конфиденциального характера. В данной работе основной акцент делается на решение инфраструктурных задач ИБ.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем [109]. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на компьютере, не связанном с сетью. Исходя из этого, отметим следующие важные выводы [109]:

1) задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

2) информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

Существуют работы, в которых рассматриваются отдельные задачи оптимального выбора СИБ. Однако отметим, что к настоящему времени отсутствует единая теория обеспечения ИБ систем различного вида и назначения. На наш взгляд такая теория должна быть ориентирована на разработчиков и эксплуатантов систем обеспечения ИБ. Такая будущая теория может быть названа прикладной теорией информационной безопасности (ПТИБ).

На наш взгляд в математическом аппарате этой теории вероятностные модели и методы должны занять значительное место. Это связано с тем, что к настоящему времени накоплен значительный объем статистики по видам атак, при этом событие нарушения ИБ АСОИУ является случайным из-за квалификации нарушителя ИБ СИБ, администратора ИБ СИБ, априорных знания нарушителя об СИБ ОИ, конфигурация СИБ и т.д. Поэтому может быть использован аппарат теории вероятностей для определения и формирования требований к ИБ АСОИУ.

Основным назначением такой теории является оптимизация решений по обеспечению ИБ конкретных систем. Как любая теория в области технических наук ПТИБ должна основываться на определенных принципах: принцип комплексности применяемых СИБ, который состоит в том что, для обеспечения ИБ конкретного информационного ресурса должна быть использована совокупность различных СИБ; принцип экономичности СИБ, состоящий в том, что стоимость СИБ должна быть минимальной при обеспечении требуемого уровня безопасности; принцип максимальной ИБ критических компонентов АСОИУ, который состоит в том, что в любой системе должны быть выделены критические компоненты вывод из строя которых разрушает всю систему в целом. Для таких компонентов должен быть обеспечен максимальный доступный в настоящее время уровень ИБ; принцип прогнозирования угроз и применения средств нападения, состоящий в необходимости мониторинга существующих и перспективных угроз и средств нападения, их статистической обработки с целью выявления на прогнозируемый период наиболее опасных угроз и возможных средств нападения; принцип обеспечения максимальной неопределённости для противника применяемых стратегий по обеспечению ИБ, состоящий в том чтобы применяемые СИБ АСОИУ эксплуатировались на основе случайного механизма, который не может быть вскрыт противником за определённый период времени; принцип применения экспертных и статистических оценок, позволяющий использовать аппарат теории вероятностей и математической статистики для формирования требований к АСОИУ, с точки зрения ИБ и оценки ее уровня ИБ. В работе [108] предложен ряд принципов, подобных тем, которые даны выше, однако в их состав не входят принципы 4–6, приведенные в данной работе.

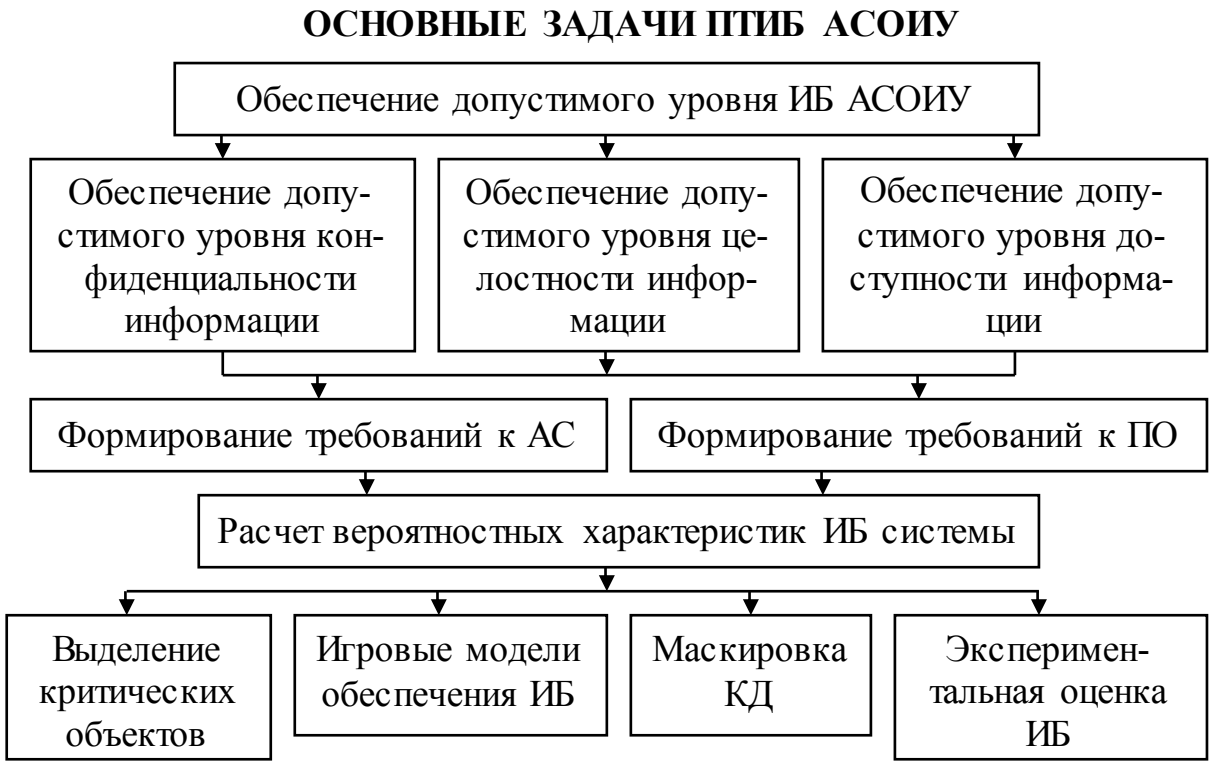

Рис. 1.1.

Для реализации этих принципов в составе разрабатываемой теории нужно провести системный анализ проблемы обеспечения безопасности АСОИУ. Декомпозиция целей и задач, решаемых в рамках разработки ПТИБ, в работе, представлена на рис. 1.1.

Отметим, что задачи обеспечения ИБ являются очень важными для АСОИУ в составе, которых кроме конфиденциальной информации хранятся и обрабатываются данные, составляющие государственную и военную тайну [108]. К таким системам относятся в основном системы военного назначения, МВД, МЧС, а так же ряд гражданских систем (АСУ атомной электростанции, АСУ скорой помощи и др.) [98]. Именно в спектре обеспечения ИБ АСОИУ будут рассматриваться приводимые ниже модели и методы. Отметим, что в последней работе рассматривались вопросы применения против АСУ СН информационного оружия и только технические средства (ТС) защиты от его образцов.

Для систем такого рода характерны очень жесткие требования по обеспечению ИБ [98], которые должны быть формализованы количественными

величинами, которые в свою очередь могут представлять собой вероятности нарушения ИБ СИБ АСОИУ.

1.3. Базовые теоретико-множественные модели прикладной теории информационной безопасности.

Математическое моделирование является мощным инструментом решения задач современной науки и техники [55–57]. При всех успехах практической информатики можно сделать вывод об отсутствии теоретических основ разработки АСОИУ, базирующихся на методах математического моделирования протекающих в них процессов. Основными причинами этого являются: сложность и практическая невозможность использования аппарата «классической непрерывной» математики из-за объективной дискретности информационных процессов, значительное многообразие используемых на практике видов информации информационных систем и технологий, что не позволяет выбрать единую схему информационной системы для ее последующего математического описания.

Главная причина, на наш взгляд, состоит в слабом развитии теоретической информатики, которая должна закладывать математические основы для формального анализа и синтеза информационных систем и средств их ИБ. В основу математического моделирования АСОИУ можно положить понятие абстрактной математической модели вида:

$$m = \{M, R_1, R_1, \ldots, R_n\} \qquad (1.1)$$

Здесь M – множество объектов и процессов, отражаемых в рассматриваемой модели; $R_1, R_2, \ldots, R_n$ - совокупность отношений, связывающих между собой элементы множества M. Эти отношения описывают интересующие исследователя свойства моделируемого объекта, процесса или явления. Будем называть отношения $R_i, i = (\overline{1,n})$ первичными отношениями.

Новые знания об изучаемом объекте, процессе или явлении будем описывать системой вторичных отношений $Q_1, Q_2, .., Q_m$, которые получаются с

помощью некоторой совокупности правил вида π. Таким образом, схема использования модели вида (1.1) записывается как

$$\{R_1, R_2, \dots R_n\} \overset{\pi}{\rightarrow} \{Q_1, Q_2, \dots Q_m\} \qquad (1.2)$$

Процесс построения и использования модели (1.1) включает в себя следующие этапы:

1. Выделение в исследуемом объекте, процессе или явлении существенных факторов и представлении их с помощью элементов множества *M*.

2. Построение множества первичных отношений $R_1, R_2, ..., R_n$, связывающих между собой определенные элементы множества *M*.

3. Выбор или разработка системы правил π вывода для построения вторичных отношений $Q_1, Q_2, .., Q_m$, отражающих цели моделирования исследуемого объекта, процесса или явления.

4. Построение вывода отношений $Q_1, Q_2, .., Q_m$ с помощью формальных процедур.

5. Анализ полученных результатов.

При несоответствии результатов целям моделирования происходит корректировка действий, проводимых на этапах 1)-4). Этот процесс повторяется до получения удовлетворяющих исследователя результатов.

Отметим, что для использования модели (1.1) для формального описания информационных процессов и систем предлагается использовать, при учете описанных выше особенностей, математический аппарат теории множеств и бинарных отношений над ними [55–57]. При этом будем использовать метрическое представления использованных отношений [56,57]. Пусть $R \subseteq M \times M$ некоторое отношение на множестве М. Это отношение конкретизируется булевской матрицей $R = [r_{ij}]$ с элементами:

$$r_{ij} = \begin{cases} 1, \textit{если пара элементов } m_i \in M \textit{ и } m_j \in M \textit{ связана отношением } R; \\ 0, \textit{в противном случае}; \end{cases}$$

Матричное представление первичных отношений $R_1 R_2,...,R_n$ позволяет реализовать на практике правило вывода π при построении вторичных отношений $Q_1, Q_2,..,Q_m$ в форме матричных машинных алгоритмов.

Построение базовых моделей теории безопасности АСОИУ естественно начать с моделирования объектов ИБ – информационных систем и реализованных в их составе информационных технологий.

Концептуальная модель АСОИУ. Как показал анализ литературы [1,2,4,5,41] в настоящее время практически отсутствуют модели АСОИУ, учитывающие современные концепции их построения.

Построим концептуальную модель современной АСОИУ, используя в качестве основы модель вида (1.1). В составе множества элементов модели выделим следующие подмножества: Л - множество подразделений организации, охваченных рассматриваемой версией АСОИУ, П - множество пользователей АСОИУ, А - множество аппаратных средств системы, Р - множество системных и прикладных программ АСОИУ, В - множество локальных банков данных, содержащих всю необходимую информацию для выполнения всех функций данной версии АСОИУ. Как известно, любая система представляет собой совокупность элементов и связей между ними [58]. Эти связи будем описывать следующими отношениями:

1) закрепление пользователей за конкретными аппаратными средствами (АРМ):

$$R_1 \subseteq \text{П} \times \text{А} \tag{1.3}$$

2) распределение ПО системы по ее аппаратным средствам:

$$R_2 \subseteq A \times P \tag{1.4}$$

3) связь программ и данных в системе:

$$R_3 \subseteq P \times B \tag{1.5}$$

4) размещение аппаратных средств системы по подразделениям (отделам, служебным и т.п.) организации:

$$R_4 \subseteq \Lambda \times \mathrm{A} \tag{1.6}$$

Тогда модель АСОИУ с учетом абстрактной математической модели (1.1) можно представить в виде [102]:

$$IS = \{\Lambda, \Pi, \mathrm{A}, \mathrm{P}, \mathrm{B}, \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3, \mathrm{R}_4\} \tag{1.7}$$

Представление АСОИУ в такой форме позволяет достаточно просто получить с помощью известных операций над отношениями [55-57] дополнительную информацию о рассматриваемой АСОИУ. Вторичные отношения, описывающие взаимодействия АРМ и конкретных пользователей с банками данных системы определяются с помощью операций композиции отношений как:

$$\begin{aligned} Q_1 &= R_2 \circ R_3 \subseteq (A \times P) \circ (P \times B) = A \times B \\ Q_2 &= R_1 \circ R_2 \circ R_3 \subseteq (\Pi \times A) \circ (A \times P) \circ (P \times B) = \Pi \times B \end{aligned} \tag{1.8}$$

Взаимодействие аппаратных средств в процессе функционирования АСОИУ получаем с помощью следующих преобразований:

$$Q_3 = R_2 \circ R_3 \circ Q_1^{-1} = (A \times P) \circ (P \times B) \circ (A \times B)^{-1} \equiv A \times A \tag{1.9}$$

Здесь была использована операция построения обратного отношения

$$Q_1^{-1} \subseteq (A \times B)^{-1} = B \times A \tag{1.10}$$

Взаимосвязь локальных банков данных, определяющую структуру РБД, получаем как

$$Q_4 = R_3^{-1} \circ R_2^{-1} \circ Q_1 \subseteq (B \times P) \circ (P \times A) \circ (A \times B) = B \times B \tag{1.11}$$

Структура системы обработки данных, определяемая взаимодействующими между собой программами АСОИУ формально описывается вторичным отношением вида:

$$Q_5 = R_3 \circ Q_1^{-1} \circ R_2 \subseteq (P \times B) \circ (B \times A) \circ (A \times P) = P \times P \tag{1.12}$$

Взаимодействие пользователей АСОИУ происходит с помощью электронного обмена данными между АРМ и их работы с общими данными. Структуру такого взаимодействия можно формально получить как:

$$Q_6 = R_1 \circ Q_1 \circ Q_2^{-1} \subseteq (П \times A) \circ (A \times B) \circ (B \times П) = П \times П \qquad (1.13)$$

Аналогичным образом можно формально описать структуру взаимодействия подразделений организации в рамках АСОИУ:

$$Q_7 = R_4 \circ R_1^{-1} \circ Q_2 \circ Q_1^{-1} \circ R_4^{-1} \subseteq (\Lambda \times A) \circ (A \times П) \circ \\ \circ (П \times B) \circ (B \times A) \circ (A \times \Lambda) = \Lambda \times \Lambda \qquad (1.14)$$

Производные отношения $Q_1, Q_1, \ldots Q_7$ можно визуализировать, используя представление отношений в форме графов [55,59].

Модель прикладной информационной технологии. В настоящее время широкое применение нашли следующие виды общих информационных технологий (ИТ): технологии обработки текстов, технологии обработки изображений, технологии обработки звука, мультимедийные технологии, Web-технологии, инфокоммуникационные технологии [108]. Эти технологии определяются нами как общие ИТ в связи тем, что они практически не связаны со спецификацией решаемых с их помощью задач. В 90-х годах сформировалось понятие ИТ [3], включающие в себя три основных компонента: человеко-машинные технологии сбора, хранения и передачи данных, вычислительные технологии, определяемые алгоритмами решения прикладных задач, человеко-машинные технологии принятия решений. Отметим, что при реализации этих видов технологий в качестве элементов, используются рассмотренные выше общие ИТ. Прикладные ИТ в качестве выходного результата всегда имеет некоторое управленческое, проектное и другое решение. Субъектами прикладной ИТ являются лица, готовящие решения (ЛГР), лица, принимающие решения (ЛПР), а также лица, реализующие решения (ЛРР) [98].

Важность рассмотрения прикладных ИТ как объектов ИБ состоит в том, что эффективность деятельности организации существенно зависит от эффективности работы ее ЛПР. Будем считать, что объектом любой прикладной ИТ, то есть средством ее реализации в составе любой системы является вполне определенный ИТ – продукт [3]. В его состав входят определен-

ные элементы множеств А, Р и В. Введем в рассмотрение следующие множества: $П_1 \subset П$ - множество ЛГР; $П_2 \subset П$ - множество ЛПР; $П_3 \subset П$ - множество ЛРР; $\Re$ - множество решений принимаемых ЛПР в рассматриваемой АСОИУ. Отметим, что при этом должно иметь место условие $П_1 \cup П_2 \cup П_3 = П$, где П – множество пользователей АСОИУ. Совокупность используемых в АСОИУ прикладных ИТ опишем отношением вида:

$$ИТ \subseteq П_1 \times A \times B \times P \times П_2 \times П_3 \times \Re \qquad (1.15)$$

Элементами этого отношения являются кортежи $(\pi_{1i}, a_j, b_k, p_r, \pi_{2s}, \pi_{3s}, \rho_l)$, где $\pi_{1i} \in П_1$, $a_j \in A$, $b_k \in B$, $p_r \in P$, $\pi_{2s} \in П_2$, $\pi_{3s} \in П_3$, $\rho_l \in \Re$. Графическое представление отношения (1.15) представлено на рис. 1.2.

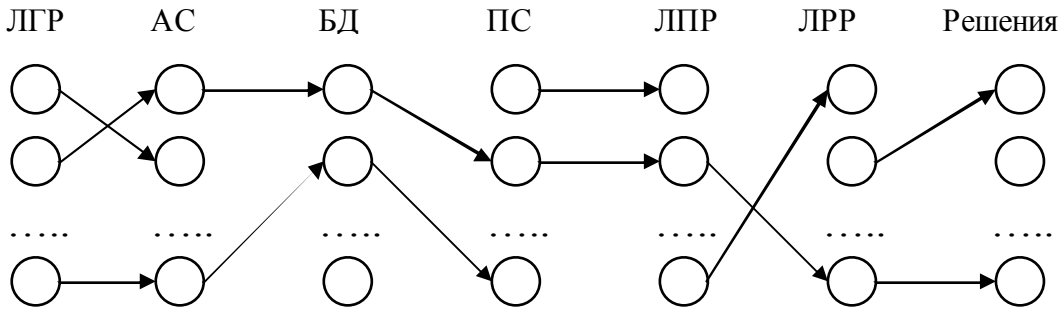

Рис. 1.2.

В любой АСОИУ все прикладные ИТ должны выполняться в определенные (фиксированные и случайные) моменты времени. График выполнения ИТ во времени будем описывать отношением вида:

$$Г \subseteq ИТ \times T_{кал}, \qquad (1.16)$$

где $T_{кал} = \{t_1, t_2, \ldots t_N\}$ - рабочий календарь организации, в составе которой реализована рассматриваемая АСОИУ. С точки зрения обеспечения безопасности принятия решений в АСОИУ отношение (1.15) позволяет при использовании соответствующих методов выделить в совокупности используемых в системе прикладных ИТ наиболее уязвимые компоненты ИТ–продуктов, а отношение (1.16) сформировать график работ по обеспечению ИБ процессов принятия наиболее ответственных решений. Наиболее распро-

странённой процедурой прикладных ИТ является работа пользователей системы с определёнными файлами РБД.

Пусть множество пользователей *П* могут выполнять с множеством файлов *Ф* следующие действия: «чтение» содержимого конкретных файлов, «изменение» содержимого файлов, «запись» данных в определённые файлы. Возможности пользователей при работе с файлами будем описывать с помощью следующих первичных отношений: «чтение» файлов:

$$G_1 \subseteq \Pi \times \Phi \qquad (1.17)$$

б) “изменение” файлов:

$$G_2 \subseteq \Pi \times \Phi \qquad (1.18)$$

в) “запись” данных в файлы:

$$G_3 \subseteq \Pi \times \Phi \qquad (1.19)$$

Будем считать, что в рассматриваемой АСОИУ имеется четыре уровня конфиденциальности данных, описываемых множеством:

$$Y = \{y_0, y_1, y_2, y_3\} \qquad (1.20)$$

где y_0 - уровень открытости данных; y_1 - уровень “Для служебного пользования”; y_2 - уровень “Секретно”; y_3 - уровень “Совершенно секретно”. Элементы множества (1.20) упорядочены следующим образом:

$$y_0 \prec y_1 \prec y_2 \prec y_3.$$

Соответствующие в АСОИУ допуски пользователей к соответствующей информации и степени “закрытости” её файлов будем описывать отношениями вида:

$$G_4 \subseteq \Pi \times \mathrm{Y}, \quad G_5 \subseteq \Phi \times \mathrm{Y} \qquad (1.21)$$

На основе отношений (1.17)-(1.21) можно построить ряд вторичных отношений для использования в системе проверки полномочий пользователей АСОИУ. Например, выявление пользователей, которые могут и “читать” и “изменять” содержимое файлов можно проводить с использованием вторичного отношения $Q_1 = G_1 \cap G_2$, которое в матричной форме реализуется как

$Q_1 = G_1 \otimes G_2$, где $\otimes$- операция поэлементного двоичного умножения булевских матриц G_1 и G_2. Возможность работы пользователей с учётом их допусков с “открытыми” и “закрытыми” файлами АСОИУ определяется с помощью отношения $Q_2 = G_4 \circ G_5^{-1} = = (\Pi \times Y) \circ (Y \times \Phi) \subseteq \Pi \times \Phi$. Таким образом, теоретико-множественная модель работы пользователей с конфиденциальной информацией в составе соответствующих прикладных ИТ с учетом абстрактной математической модели (1.1) примет вид:

$$\Pi_{РП} = \{\Pi, \Phi, Y, G_1, G_2, ..., G_5\} \qquad (1.22)$$

Предложенные в данном разделе модели (1.7),(1.15) так же выступают в качестве исходных данных для решения задач анализа и синтеза систем ИБ АСОИУ.

Концептуальная модель систем ИБ ИТ – продуктов. В настоящее время создано и эксплуатируется значительное число АСОИУ [1-5,60]. В литературе [13–17,23,34,42,] имеются описания моделей СИБ. На наш взгляд, основным недостатком существующих моделей является их значительная абстрактность, которая не позволяет их использовать для построения инженерных методик оценки проектных и эксплутационных решений по применяемым СИБ. Рассмотрим концептуальную модель системы ИБ, основанную на рассмотренных выше моделях АСОИУ и прикладных ИТ. Пусть используемые в составе рассматриваемой АСОИУ объекты ИБ представляют собой ИТ – продукты, включающие в себя множество аппаратных (А), программных (Р) средств и файлов (Ф), используемых при реализации соответствующих задач АСОИУ. Для территориальных распределенных АСОИУ в множество объектов ИБ необходимо включить множество линий (каналов) связи L. Введём в рассмотрение множество Z объектов ИБ в рассматриваемой АСОИУ, которое определим как

$$Z = A \cup P \cup \Phi \cup L \qquad (1.23)$$

Отметим, что здесь не учитывается взаимодействие аппаратных и программных средств с требуемыми данными и линиями связи в процессе выполнения прикладных и инфокоммуникационных технологий. Обозначим через U множество угроз АСОИУ, которые в общем случае включают в себя следующие элементы [1-5,23,60]: u_1 - перехват электромагнитных излучений работающих аппаратных средств АСОИУ; u_2 - принудительное облучение (“подсветка”) линий связи с целью получения паразитной модуляции несущей; u_3 - применение подслушивающих устройств (“закладок”); u_4 - дистанционное фотографирование; u_5 - хищение носителей информации; u_6 - считывание данных из файлов пользователей; u_7 - чтение остаточной информации в памяти ЭВМ после выполнения санкционированных запросов; u_8 - копирование носителей с преодолением мер ИБ; u_9 - маскировка под зарегистрированного пользователя (подбор паролей); u_{10} - маскировка под запросы системы; u_{11} - использование программных “ловушек”; u_{12} - использование недостатков языков программирования и операционных систем; u_{13} - использование “троянского коня”; u_{14} - незаконное подключение к аппаратуре и линиям связи; u_{15} - разрушение механизмов ИБ; u_{16} - использование компьютерных вирусов; u_{17} - разглашение сотрудниками АСОИУ служебной и конфиденциальной информации.

Для исключения этих и других потенциальных угроз в АСОИУ используется множество M средств ИБ, которые в общем случае включают в себя следующие элементы [1–5,23,60]: m_1 - препятствия (физическое ограничение доступа противнику к аппаратуре, носителям информации и т.п.); m_2 - управление доступом к ИТ - продуктам системы; m_3 - регламентация работы с системой; m_4 - маскировка (криптографическая защита); m_5 - принуждение (соблюдение правил работы под угрозой ответственности); m_6 - побуждение (то же за счёт выполнения моральных и этических норм). Все существующие

СИБ можно в общем случае разбить на следующие подмножества: M_1 - физические средства; M_2 - аппаратные средства; M_3 - программные средства; M_4 - организационные средства; M_5 - законодательные средства; M_6 - морально-этические средства, удовлетворяющие условию $\bigcup_{i=1}^{6} M_i = M$. Зададим первичные отношения модели видов «угроза–объект» и «объект–СИБ» как:

$$V_1 \subseteq U \times Z,\ V_2 \subseteq Z \times M \tag{1.24}$$

Тогда концептуальную модель системы ИБ с учетом абстрактной математической модели (1.1) можно представить в виде:

$$M_{ИБ} = \{Z, V_1, V_2\} \tag{1.25}$$

Взаимосвязь угроз и СИБ можно описать, строя вторичное отношение:

$$W_1 = V_1 \circ V_2 \subseteq U \times M \tag{1.26}$$

Это отношение описывается, как было указано выше, булевской матрицей $W_1 = [w_{ij}^1]$ с элементами:

$$w_{ij}^{(1)} = \begin{cases} 1, & \textit{если от } i-\textit{ой угрозы АСОИУ СН защищает } j-\textit{ое средство}; \\ 0, & \textit{в противном случае.} \end{cases}$$

Построение матрицы W_1 позволяет формальным образом провести первичный анализ системы ИБ АСОИУ. В частности, наличие в этой матрице нулевой строки с номером S говорит о том, что для угрозы $u_S \in U$ отсутствует СИБ. Вторичное отношение W_2 определяемое как

$$W_2 = W_1 \circ V_2^{-1} \subseteq U \times M \times Z \tag{1.27}$$

позволяет построить трёхдольный ориентированный граф (рис. 1.3).

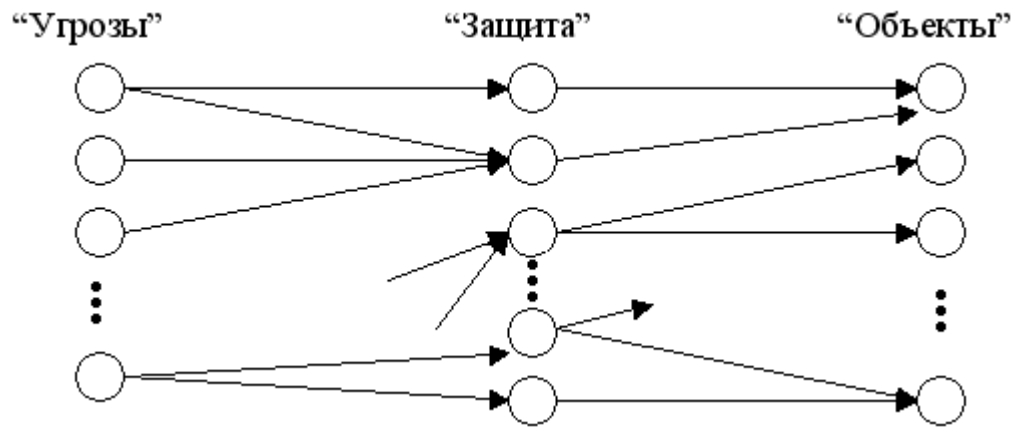

Рис. 1.3.

Выводы по главе 1.

В данной главе получены следующие результаты:

1. Приведен обзор работ посвященных вопросам обеспечения ИБ, а так же обзор и анализ основных СИБ.

2. Обоснована необходимость создания прикладной теории ИБ предметом, которой является разработка методик эффективного применения существующих и перспективных СИБ в процессе разработки и эксплуатации АСОИУ.

3. Приведено определение понятия ИБ. Сформулированы основные принципы прикладной теории ИБ: принцип комплексности применяемых СИБ, принцип экономичности СИБ, принцип обеспечения максимальной ИБ критических компонентов АСОИУ, принцип прогнозирования угроз, принцип обеспечения максимальной неопределённости применяемых стратегий ИБ для противника, принцип применения экспертных и статистических оценок.

4. Предложены следующие базовые модели прикладной теории ИБ: абстрактная математическая модель, концептуальная модель АСОИУ, модель прикладной информационной технологии, концептуальная модель систем ИБ ИТ – продуктов.

Глава 2. Вероятностные характеристики информационной безопасности АСОИУ.

Для решения задачи анализа и синтеза СИБ с применением широкоразвитых в настоящее время вероятностных методов необходимы методы определения допустимых, с точки зрения Заказчика значений вероятностей обеспечения ИБ создаваемой АСОИУ [61] и ее компонент. В данной главе предлагаются модели и методы, позволяющие сформировать эти требования.

2.1. Определение компромиссного значения требуемой вероятности обеспечения информационной безопасности АСОИУ.

Пусть q- вероятность обеспечения ИБ при функционировании АСОИУ. Обозначим через $Z_ф$ - затраты (потери) от несанкционированного вмешательства в функционирование системы, которые зависят от имеющегося в АСОИУ уровня ИБ, описываемого значением вероятности q. Будем считать, что эта величина принимает максимальное значение при $q = 0$ (отсутствие СИБ) и значение равное нулю при $q = 1$ (наличие «абсолютной» СИБ). Таким образом, имеем функцию вида:

$$Z_ф = Z_ф(q), \quad q \in [0,1] \tag{2.1}$$

Пусть Z_c - затраты на создание СИБ, которые описываются функцией вида:

$$Z_c = Z_c(q), \quad q \in [0,1] \tag{2.2}$$

Эта функция является возрастающей функцией, которая при $q = 0$ равна нулю, а при $q = 1$ принимает максимальное значение. При разработке СИБ естественным требованием является минимизация затрат $Z_ф$ и Z_c путём выбора устраивающего заказчика значения вероятности q, удовлетворяющего условию:

$$0 < q < 1 \tag{2.3}$$

Здесь граничные значения $q=0$ и $q=1$ не рассматриваются как не имеющие практического значения с точки зрения решаемой задачи. Последнее означает, что с точки зрения отмеченных выше свойств зависимостей (2.1) и (2.2) однокритериальные задачи выбора значения q видов

$$Z_{ф}(q)\to\min_{0<q<1},\quad Z_{c}(q)\to\min_{0<q<1} \tag{2.4}$$

не имеют практически значимых решений. Вместе с тем целевые функции (2.1) и (2.2) являются противоречивыми, так как с ростом значения q затраты $Z_{ф}$ убывают, а затраты Z_{c} возрастают. Это позволяет определить некоторый, устраивающий заказчика компромисс между значениями затрат $Z_{ф}$ и Z_{c}. Для реализации такого подхода сформулируем двухкритериальную задачу оптимизации вида:

$$\left(Z_{ф},Z_{c}\right)\to\min_{0<q<1}. \tag{2.5}$$

Паретооптимальное решение этой задачи будем строить путём минимизации линейной свёртки критериев[62]:

$$L\left(q,\lambda\right)=\lambda Z_{ф}(q)+\left(1-\lambda\right)Z_{c}(q)\to\min_{0<q<1} \tag{2.6}$$

Здесь $\lambda\in(0,1)$ - параметр свёртки критериев (2.1) и (2.2). Отметим, что в отличии от существующей теории оптимизации по Парето [62] значения $\lambda=0$ и $\lambda=1$, соответствующие решению однокритериальных задач вида (2.4), не используются при построении паретооптимальных решений. Отметим, что в случае непрерывных дифференцируемых функций (2.1) и (2.2) для решения задачи (2.6) можно использовать необходимое условие экстремума[63] функции $L\left(q,\lambda\right)$, которое записывается как:

$$\frac{\partial L}{\partial q}=\lambda Z_{ф}^{'}(q)+\left(1-\lambda\right)Z_{c}^{'}(q)=0 \tag{2.7}$$

Решая, это уравнение относительно q получаем параметрическую зависимость вида:

$$q = q(\lambda), \quad \lambda \in (0,1), \tag{2.8}$$

которая описывает множество паретооптимальных решений задачи (2.5) в пространстве решений. Подставляя, её в выражение (2.1) и (2.2) имеем:

$$Z_ф = Z_ф(q(\lambda)) = \varphi_ф(\lambda), Z_c = Z_c(q(\lambda)) = \varphi_c(\lambda) \tag{2.9}$$

Исключая из (2.9) параметр λ, получаем множество паретооптимальных вариантов решений задачи (2.5) в пространстве критериев:

$$Z_ф = \Psi(Z_c), \tag{2.10}$$

вид которого представлен на рис. 2.1.

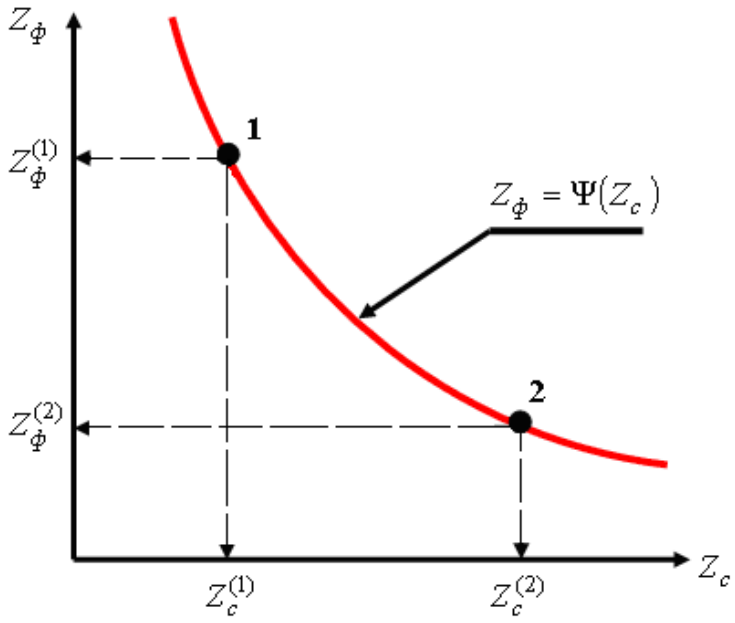

Рис. 2.1.

Анализируя зависимости (2.8)-(2.10), заказчик может выбрать значения вероятности q, которые обеспечивают ему приемлемые значения потерь от нарушения ИБ и затрат на создание СИБ. Рассмотрим один из подходов к построению зависимостей вида (2.1),(2.2). Пусть при отсутствии СИБ ($q = 0$) потери от несанкционированного вмешательства в работу АСОИУ составляют C_1 единиц. Будем считать, что с ростом вероятности q значение потерь $Z_ф$ уменьшается по экспоненциальному закону и при $q = 1$ становиться практически равным нулю. Этим требованиям удовлетворяют функции вида:

$$Z_{\phi}(q) = C_1 e^{-\alpha q}, \quad \alpha \in (0,1) \tag{2.11}$$

Параметр α, входящий в это выражение можно вычислить из уравнения:

$$C_1 e^{-\alpha} = \varepsilon,$$

где ε - достаточно малое заданное число. Решая, это уравнение имеем:

$$\alpha = \ln\left(\frac{C_1}{\varepsilon}\right). \tag{2.12}$$

Будем считать, что затраты на создание СИБ пропорциональны величине q, то есть имеют вид:

$$Z_c(q) = C_2 q. \tag{2.13}$$

Здесь C_2 - стоимость создания «абсолютной» СИБ, при которой уровень ИБ АСОИУ $q = 1$. В связи с тем, что такой уровень ИБ на практике является не достижимым, но разработчик стремится обеспечить такой уровень, то значение C_2 можно формировать двумя путями: заданием разработчиком величины C_2, при которой с его точки зрения будет, достигнут максимально возможный уровень ИБ АСОИУ, (30-50% стоимости АСОИУ), использование значения C_2 из практики разработки и функционирования «хорошо защищённых» АСОИУ. Для функций (2.11) и (2.13) уравнение (2.7) записывается в виде: $-\lambda\alpha C_1 e^{-\alpha q} + (1-\lambda)C_2 = 0$. Решая это уравнение, получим конкретный вид зависимости (2.8):

$$q(\lambda) = \frac{1}{\alpha}\ln\frac{\lambda\alpha C_1}{(1-\lambda)C_2}, \quad \lambda \in (0,1). \tag{2.14}$$

Определим интервал допустимых значений параметра свёртки λ, входящего в это выражение. Пусть заказчиком задано значение q^* определяющее границу вероятности q, то есть минимально допустимый с его точки зрения уровень ИБ АСОИУ. Тогда паретооптимальные значения вероятности $q(\lambda)$ должны удовлетворять неравенству вида: $q^* \le q(\lambda) < 1$. При этом мини-

мальное значение $\lambda^* \in (0,1)$ определяется с учётом выражения (2.14) из уравнения: $\frac{1}{\alpha}\ln\frac{\lambda^*\alpha C_1}{(1-\lambda^*)C_2} = q^*$. Решая его, получаем, что

$$\lambda^* = \frac{C_2 e^{\alpha q^*}}{\alpha C_1 + C_2 e^{\alpha q^*}}. \qquad (2.15)$$

Условие того, что $q(\lambda) < 1$ даёт следующее ограничение на значение параметра λ:

$$\lambda^{**} = \frac{C_2 e^{\alpha}}{\alpha C_1 + C_2 e^{\alpha}}, \qquad (2.16)$$

которое было получено из выражения (2.15) при замене q^* на величину $q(\lambda) = 1$. Таким образом, множество вариантов вероятности q получается путём варьирования значений параметра λ в интервале $[\lambda^*, \lambda^{**}]$.

Предложенную методику определения уровня общей ИБ АСОИУ можно конкретизировать для нахождения вероятности обеспечения таких частных свойств ИБ [5] как конфиденциальность $q_К$, целостность $q_Ц$ и достоверность данных $q_Д$.

2.2. Формирование допустимых значений вероятностей обеспечения конфиденциальности, целостности и доступности.

Обеспечение собственной безопасности является задачей первостепенной важности для любой системы, независимо от её сложности и назначения, будь то биологический организм, физический эксперимент, или любой другой программно аппаратный комплекс[64,65]. Вместе с тем в условиях бурного развития АСОИУ, а также повсеместного применения информационных технологий практически любую АСОИУ можно рассматривать как систему обработки информации. Возникает задача, связанная с формированием требований к ИБ компонент АСОИУ конфиденциальности, целостности и доступности.

В разделе 2.1 был предложен подход к формированию допустимого значения вероятности нарушения ИБ разрабатываемой АСОИУ, которую обозначим как $P_{ИБ}^{доп}$. Предполагая, что хотя бы одно нарушение таких основных свойств ИБ, как конфиденциальность, целостность или доступность данных ведёт к потере безопасности АСОИУ, имеем, что [103, 104]:

$$P_{ИБ} = 1 - (1 - P_{конф})(1 - P_{цел})(1 - P_{дост}), \qquad (2.17)$$

где $P_{конф}, P_{цел}, P_{дост}$ - соответственно вероятности нарушения конфиденциальности, целостность и доступности информации в АСОИУ. Определим значения вероятностей $P_{конф}, P_{цел}, P_{дост}$, удовлетворяющих, с учётом выражения (2.17) условиям вида: $(1 - P_{конф})(1 - P_{цел})(1 - P_{дост}) = = 1 - P_{ИБ}^{доп}$. Переходя к вероятностям противоположных случайных событий эти условия можно переписать как:

$$Q_{конф} Q_{цел} Q_{дост} = Q_{ИБ}^{доп} \qquad (2.18)$$

Заказчик АСОИУ может определить, руководствуясь статистикой попыток нарушения ИБ реальных АСОИУ [3,66], среднюю интенсивность атак на компоненты конфиденциальности, целостности и доступности АСОИУ. Будем считать, что количество попыток нарушения конфиденциальности информации в АСОИУ в единицу времени по оценкам Заказчика равно $\lambda_{конф}$, а для целостности и доступности информации соответственно $\lambda_{цел}$ и $\lambda_{дост}$. При этом заказчик может руководствоваться статистикой об атаках собранной за некоторые интервалы времени (например, час, сутки, неделю, месяц, год). Тогда можно определить среднее время между попытками нарушения конфиденциальности, целостности и доступности информации в АСОИУ:

$$\tau_{конф} = \frac{1}{\lambda_{конф}}, \tau_{цел} = \frac{1}{\lambda_{цел}} \text{ и } \tau_{дост} = \frac{1}{\lambda_{дост}}. \qquad (2.19)$$

Будем считать, что заказчик задал параметры α, β и γ, определяющие важность для разрабатываемой АСОИУ обеспечения условий конфиденци-

альности, целостности и доступности информации в АСОИУ. Эти параметры должны удовлетворять следующим условиям: $0<\alpha<1$, $0<\beta<1$, $0<\gamma<1$ и $\alpha+\beta+\gamma<1$. Определим оценки важности рассматриваемых аспектов обеспечения ИБ, с учетом проведенных выше рассуждений, в следующем виде: $\alpha=\dfrac{\tau_{конф}}{\tau_{конф}+\tau_{цел}+\tau_{дост}}$, $\beta=\dfrac{\tau_{цел}}{\tau_{конф}+\tau_{цел}+\tau_{дост}}$, $\gamma=\dfrac{\tau_{дост}}{\tau_{конф}+\tau_{цел}+\tau_{дост}}$. Тогда вероятности $Q_{конф}^{доп}$, $Q_{цел}^{доп}$ и $Q_{дост}^{доп}$ можно определить по формулам вида:

$$Q_{конф}^{доп}=\left(Q_{ИБ}^{доп}\right)^{\alpha},\quad Q_{цел}^{доп}=\left(Q_{ИБ}^{доп}\right)^{\beta},\quad Q_{дост}^{доп}=\left(Q_{ИБ}^{доп}\right)^{\gamma} \qquad (2.20)$$

Отметим, что если $\alpha=\beta=\gamma$, то $Q_{конф}^{доп}=Q_{цел}^{доп}=Q_{дост}^{доп}=\left(Q_{ИБ}^{доп}\right)^{1/3}$. Обобщим предложенный подход. Допустим, что в АСОИУ имеется M элементов $m_1,m_2,\ldots,m_i,\ldots,m_M$, для каждого из которых заказчиком задана величина $\tau_m=\dfrac{1}{\lambda_m}$, где λ_m - прогнозируемое заказчиком число атак на m_i-й элемент АСОИУ за единицу времени, определяющая среднее время между попытками нарушения ИБ элемента m_i. Определим оценки важности обеспечения ИБ рассматриваемых элементов $m_1,m_2,\ldots,m_M$ АСОИУ в следующем виде:

$$\alpha_m=\frac{\tau_m}{\sum\limits_{m=1}^{M}\tau_m}. \qquad (2.21)$$

Таким образом, можно найти вероятности обеспечения ИБ элементов рассматриваемой АСОИУ:

$$Q_m^{доп}=\left(Q_{ИБ}^{доп}\right)^{\alpha_m}. \qquad (2.22)$$

Можно легко убедится в том, что полученное решающее правило удовлетворяет обобщённому условию вида (2.18):

$$\prod_{m=1}^{M}Q_m^{доп}=Q_{ИБ}^{доп}.$$

Как известно основными составными частями любой АСОИУ являются данные, программы и ТС автоматизации[58].

Формирование допустимых значений вероятностей обеспечения конфиденциальности процессов обработки данных АСОИУ. Рассмотрим методику формирования допустимых значений вероятностей обеспечения конфиденциальности процессов обработки информации для компонент АСОИУ, обеспечивающих требуемый уровень конфиденциальности $Q_{конф}^{доп}$.

Конфиденциальность данных – это статус, представленный данным и определяющий требуемую степень ИБ [1]. Для описания процесса обработки информации введем в рассмотрение следующие множества [58]: D - множество данных, циркулирующих в системе, Z - множество задач (прикладных программ, процедур, приложений и т.д.), реализующих функции рассматриваемой АСОИУ; T - множество ТС рассматриваемой системы. Перечень элементов входящих в эти множества определен в разделе 1.3. при описании объектов модели(1.23) и моделей вида «угроза–объект» и «объект–СИБ» (1.24). В множестве D выделим подмножества входных D^B и выходных (результирующих) D^V данных таких, что:

$$D = D^B \bigcup D^V .$$

Структуру формирования в рассматриваемой АСОИУ выходных данных D^V на основе решения множества задач Z, использующих определенные входные данные D^B будем в общем виде представлять с использованием аппарата n - арных отношений [55] как:

$$R = D^B \times Z \times Z \times D^V . \qquad (2.23)$$

Известно, что решение любой задачи $z \in Z$ в АСОИУ предусматривает использование определённых ТС (АРМ, линии связи, маршрутизаторы, концентраторы, серверы и т.п.). Пусть в рассматриваемой АСОИУ предусмотрено использование множества ТС T. Пусть в рассматриваемой системе используется определённое заказчиком упорядоченное по возрастанию множе-

ство K уровней конфиденциальности информации. Например, это множество может иметь вид $K=\{k_0,k_1,k_2\}$, где $k=0$ - «открытая информация», $k=1$ - «секретно», $k=2$ - «совершенно секретно». Сделаем следующие предположения: в множестве задач Z, решаемых в АСОИУ не используются «закрытые» алгоритмы, уровни конфиденциальности задач и формируемых при их решении выходных данных зависят только от уровней конфиденциальности используемых входных данных, если некоторый элемент АСОИУ имеет несколько уровней конфиденциальности, то ему должен быть присвоен максимальный из имеющихся у него уровень. Разобьем множество данных D^B на подмножества D_k^B, $k\in K$. Здесь каждый элемент $d^B\in D_k^B$ имеет k-ый уровень конфиденциальности. Исключим из дальнейшего рассмотрения «открытые» данные D_o^B, соответствующие уровню конфиденциальности $k=0$. Тогда множество конфиденциальных входных данных определится как

$$D_{конф}^B = D^B \setminus D_o^B .$$

Для каждого множества данных $D_k^B \subseteq D_{конф}^B$ введем в рассмотрение вероятности Q_k^B обеспечения заданного уровня их конфиденциальности $k\in K$, $k\neq 0$. Значения Q_k^B можно определять с использованием подхода предложенного выше. Для каждого уровня конфиденциальности $k\in K$, $k\neq 0$ можно определить, например, из практики работы реальных АСОИУ, предполагаемое среднее время $\tau_k^{конф}$ между попытками нарушения ИБ данных k-го уровня конфиденциальности. И с использованием решающих правил (2.21),(2.22) получить значения вероятностей Q_k^B:

$$Q_k^B = \left(Q_{конф}^{доп}\right)^{\alpha_k^{конф}}, \qquad (2.24)$$

где $\alpha_k^{конф} = \dfrac{\tau_k^{конф}}{\sum\limits_{k=1}^{K} \tau_k^{конф}}$. В формуле (2.24) величина $Q_{конф}^{доп}$ - это значение вероятности обеспечения конфиденциальности информации в АСОИУ, вычисляемое по первой формуле выражения (2.20). Отметим, что при $k = 0, \quad Q_k^B \equiv 0$. Для формирования требуемых уровней конфиденциальности задач Z и выходных данных D^V выделим из состава отношения (2.23) частные бинарные отношения вида:

$$R_1 = D^B \times Z, \quad R_2 = Z \times D^V, \tag{2.25}$$

описывающие используемые при решении каждой задачи $z_j \in Z$ входные данные $d_i^B \in D^B$, а так же формируемые при этом выходные данные $d_r^V \in D^V$. Пусть мощности (число элементов) рассматриваемых множеств соответственно равны $\left|D^B\right| = n$, $\left|Z\right| = m$, $\left|D^V\right| = l$, $\left|T\right| = t$. Тогда следуя работе [55] отношения (2.25) могут быть описаны булевскими матрицами $B_1 = [b_{ij}^{(1)}]_{n \times m}$ и $B_2 = [b_{jr}^{(2)}]_{m \times l}$. Используя матрицу, B_1 определим для каждой задачи $z_j \in Z$ подмножество $D_j^B \in D^B$ используемых ею входных данных как:

$$D_j^B = \left\{ d_i^B \in D^B \middle| b_{ij}^{(1)} = 1, i = \overline{(1,n)} \right\}, \quad j = \overline{(1,m)}. \tag{2.26}$$

Сформируем для фиксированного значения $j \in \overline{(1,m)}$ совокупность множеств, определяемых по формуле вида: $D_{jk}^B = D_j^B \bigcap D_k^B$, $k \in K$. Здесь рассматриваются и входные данные при $k = 0$. Если для некоторого фиксированного значения k множество $D_{jk}^B \neq 0$, то данные этого уравнения используются при решении задачи $z_j \in Z$. Пусть для задачи $z_j \in Z$ не пустыми оказались множества $D_{jk_1}^B, D_{jk_2}^B, \ldots, D_{jk_p}^B$, где $k_1 > k_2 > \ldots > k_p$ - отдельные

элементы множества K. Тогда этой задаче назначается наивысший из полученных уровень конфиденциальности равный $k_1 \in K$. Таким образом, получаем следующее решающее правило для определения вероятностей обеспечения требуемого уровня конфиденциальности Q_j^{ZB} задачи $z_j \in Z$ по ее входным данным:

$$Q_j^{ZB} = \arg\max_{k \in K} \left\{ Q_k^B \middle| D_{jk}^B \neq \varnothing \right\}, \quad j = \overline{1,m}. \tag{2.27}$$

Аналогичным образом назначаются уровни конфиденциальности выходным данным $d_r^V \in D^V$. Используя матрицу, B_2 выделим для каждой задачи $z_j \in Z$ подмножество формируемых ею выходных данных:

$$D_j^V = \left\{ d_r^V \in D^V \middle| b_{jr}^{(2)} = 1, r = \overline{1,l} \right\}, \quad j = \overline{1,m}. \tag{2.28}$$

Для назначения уровней конфиденциальности выходным данным АСОИУ предлагается использовать следующие решающие правила:

1) Если задача $z_j \in Z$ имеет определенный выше k–й уровень конфиденциальности, то такой же уровень должны иметь все данные, входящие в множество D_j^V, то есть

$$Q\left(d_r^V \in D_j^V\right) = Q_j^{ZB}, \quad j = \overline{1,m},$$

2) если какой-либо элемент $d_r^V \in D^V$ формируется более чем одной задачей, например задачами z_{j1}, z_{j2}, …, z_{jq}, то вероятность обеспечения требуемого уровня конфиденциальности этого элемента определяется как:

$$Q\left(d_r^V \in D_j^V\right) = \max\left\{ Q_{j1}^{ZB}, Q_{j2}^{ZB}, \ldots, Q_{jq}^{ZB} \right\}, \quad j = \overline{1,m}. \tag{2.29}$$

В общем случае уровень конфиденциальности любой задачи $z \in Z$ будет зависеть и от уровня конфиденциальности предшествующих ей по принятой в АСОИУ технологии задач и используемых ею выходных данных смежных задач.

Введем в составе отношения (2.23) частное бинарное отношение $R_3 \subseteq Z \times Z$, которое представляет собой ориентированный граф $G(Z)$ связи задач по технологии их решения. Связь любой пары вершин $z_h \in Z$ и $z_j \in Z$ этого графа представим с помощью матрицы смежности графа $B_3 = [b_{hj}^{(3)}]_{m \times m}$. Для каждой задачи $z_j \in Z$ выделим подмножество смежных ей задач:

$$Z_j = \left\{ z_h \in Z \middle| b_{hj}^{(3)} = 1, \quad h = \overline{(1,m)} \right\}, \quad j = \overline{(1,m)}. \tag{2.30}$$

Тогда задача $z_j \in Z$ должна иметь окончательное значение вероятности обеспечения требуемого уровня конфиденциальности, которое с учетом (2.27),(2.29) определяется как:

$$\begin{array}{l} Q_j^z = \arg \max\limits_{z_h \in Z_j} \{ \max\limits_{k \in K} \left(Q_k^{ZB}, Q\left(d_r \in D_h^V \right) \right) \middle| Z_j \neq \varnothing, D_h^V \neq \varnothing \}, \\ j = \overline{(1,m)}, \quad h = \overline{(1,m)} \end{array} . \tag{2.31}$$

Если $Z_j = \varnothing$, то $Q_j^z = \arg \max\limits_{k \in K} Q_k^{ZB}$. Перейдем к определению вероятностей обеспечения требуемого уровня конфиденциальности применяемых в АСОИУ устройств, входящих в множество T. Рассмотрим множества задач Z и ТС T. Построим частное бинарное отношения вида

$$R_4 \subseteq Z \times T. \tag{2.32}$$

Тогда следуя работе [55] отношение (2.32) может быть описано булевской матрицей $B_4 = [b_{jf}^{(4)}]_{m \times t}$. Обозначим через Q_{jf} - вероятности обеспечения требуемого уровня конфиденциальности ТС $t_f \in T$ при его использовании для решения задачи $z_j \in Z$. По аналогии с рассуждениями, представленными выше, получим решающие правила для определения значений вероятностей Q_{jf}:

$$Q_{jf} = b_{jf}^{(4)} \left(Q_j^z \right)^{\alpha_{jf}}, \quad j = (\overline{1,m}), \tag{2.33}$$

где $\alpha_{jf} = \dfrac{b_{jf}^{(4)}\tau_{jf}}{\sum_{f=1}^{t} b_{jf}^{(4)}\tau_{jf}}$, а вероятность Q_j^z определяется по формуле (2.31), а τ_{jf} это среднее время между попытками нарушения ИБ компоненты t_f прогнозируемое заказчиком АСОИУ. В связи с тем, что одно и тоже ТС $t_f \in T$, может быть использовано при решении нескольких задач с различными уровнями конфиденциальности. Окончательное значение вероятности Q_{jf}^o обеспечения требуемого уровня конфиденциальности каждого применяемого в АСОИУ ТС вычисляется как:

$$Q_{jf}^o = \max_{z_j \in Z} Q_{jf}, f = \overline{(1,t)}, j = \overline{(1,m)}.$$

Формирование допустимых значений вероятностей обеспечения целостности данных и процессов обработки информации в АСОИУ. Рассмотрим требования, предъявляемые к целостности информации. В работе [1] сказано, что целостность информации - это свойство информации быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий. Определим допустимую вероятность обеспечения ИБ компоненты целостности $Q_{цел}^{доп}$ по формуле (2.4). Пусть заказчик спрогнозировал следующие интенсивности атак нарушения целостности множества данных D и множества задач Z, которые соответственно равны λ_D и λ_Z. Тогда используя методику, предложенную выше можно определить требования, предъявляемые к ИБ данных и задач с точки зрения целостности информации. Определим среднее интервалы времени между попытками нарушения ИБ данных и задач:

$$\tau_D = \frac{1}{\lambda_D}, \quad \tau_Z = \frac{1}{\lambda_Z}.$$

Далее найдем значения вероятностей обеспечения ИБ данных D и задач Z:

$$Q_D = \left(Q_{цел}^{доп}\right)^{\alpha}, \quad Q_Z = \left(Q_{цел}^{доп}\right)^{\beta} \tag{2.34}$$

где $\alpha = \dfrac{\tau_D}{\tau_D + \tau_Z}, \beta = \dfrac{\tau_Z}{\tau_D + \tau_Z}$.

При работе АСОИУ в ней могут использоваться данные разных уровней конфиденциальности. Отметим что, нарушение целостности входных данных любого уровня конфиденциальности ведет к нарушению целостности выходных данных задач, использующих эти входные данные. Пусть в рассматриваемой АСОИУ используется определённое заказчиком упорядоченное по возрастанию множество K уровней конфиденциальности информации. Для каждого множества данных $D_k^B \subseteq D^B$ введем в рассмотрение вероятности обеспечения целостности $Q_k^{ЦВ}$ заданного уровня их конфиденциальности $k \in K$. Значения $Q_k^{ЦВ}$ можно определять с использованием подхода предложенного выше. Для каждого уровня конфиденциальности $k \in K$ можно определить, например, из практики работы реальных АСОИУ, интенсивности $\lambda_k^{цел}$ и следовательно среднее интервалы $\tau_k^{цел} = \dfrac{1}{\lambda_k^{цел}}$ между попытками нарушения целостности данных k-го уровня конфиденциальности. Далее можно определить вероятность обеспечения целостности входных данных k - го уровня конфиденциальности:

$$Q_k^{ЦВ} = \left(Q_D\right)^{\alpha_k^{цел}}, \tag{2.35}$$

где $\alpha_k^{цел} = \dfrac{\tau_k^{цел}}{\sum\limits_{k=0}^{K} \tau_k^{цел}}$. В формуле (2.35) величина Q_D - это значение вероятности обеспечения целостности данных $z_j \in Z$ в АСОИУ, которая определяется из первого выражения формулы (2.34). Таким образом, для каждого уровня

конфиденциальности $k \in K$ получен требуемый уровень целостности данных $w \in W$, где $|K| = |W|$, при этом наивысший уровень конфиденциальности данных может не являться наивысшим уровнем целостности данных. Например, открытые данные могут иметь наивысший уровень целостности. Для формирования требуемых уровней целостности задач Z и выходных данных D^V сформируем ряд правил: уровни целостности задач и формируемых при их решении выходных данных зависят только от уровней целостности используемых входных данных, если некоторый элемент АСОИУ имеет несколько уровней целостности, то ему должен быть присвоен максимальный из имеющихся у него уровень.

Сформируем для фиксированного значения $j \in \overline{(1,m)}$ совокупность множеств, определяемых по формуле вида: $D^B_{jw} = D^B_j \bigcap D^B_w$, $w \in W$, где подмножество $D^B_j \in D^B$ определяется по формуле (2.26). Если для некоторого фиксированного значения w множество $D^B_{jw} \neq 0$, то данные этого уровня целостности используются при решении задачи $z_j \in Z$. Пусть для задачи $z_j \in Z$ не пустыми оказались множества $D^B_{jw_1}, D^B_{jw_2}, \ldots, D^B_{jw_p}$, где $w_1 > w_2 > \ldots > w_p$ - отдельные элементы множества W. Тогда этой задаче назначается наивысший из полученных уровень обеспечения целостности данных равный $w_1 \in W$. Таким образом, получаем следующее решающее правило для формирования вероятностей обеспечения требуемого уровня целостности $Q^{ЦZB}_j$ задачи $z_j \in Z$ с использованием ее входным данным:

$$Q^{ЦZB}_j = \arg\max_{w \in W} \left\{ Q^{ЦВ}_w \middle| D^B_{jw} \neq \varnothing \right\}, \quad j = \overline{(1,m)}.$$

Аналогичным образом назначаются уровни целостности выходным данным $d^V_r \in D^V$. Используя матрицу, B_2 выделим для каждой задачи $z_j \in Z$ подмножество D^V_j формируемых ею выходных данных используя

выражение (2.28). Для назначения уровней целостности выходным данным АСОИУ предлагается использовать следующие решающие правила:

1) Если задача $z_j \in Z$ имеет определенный выше w–й уровень целостности, то такой же уровень должны иметь все данные, входящие в множество D_j^V, то есть

$$Q\left(d_r^V \in D_j^V\right) = Q_j^{ЦZB}, \quad j = \overline{1,m}, \tag{2.36}$$

2) если какой-либо элемент $d_r^V \in D^V$ формируется более чем одной задачей, например задачами z_{j1}, z_{j2}, … , z_{jq}, то вероятность обеспечения требуемого уровня целостности этого элемента определяется как:

$$Q\left(d_r^V \in D_j^V\right) = \max\left\{Q_{j1}^{ЦZB}, Q_{j2}^{ЦZB}, \ldots, Q_{jq}^{ЦZB}\right\}, \quad j = \overline{1,m}. \tag{2.37}$$

В общем случае уровень целостности любой задачи $z \in Z$ будет зависеть и от уровня целостности предшествующих ей по принятой в АСОИУ технологии задач и используемых ею выходных данных смежных задач. Рассмотрим частное бинарное отношение $R_3 \subseteq Z \times Z$. Для каждой задачи $z_j \in Z$ выделим подмножество смежных ей задач (2.30). Тогда задача $z_j \in Z$ должна иметь значение вероятности обеспечения требуемого уровня целостности, которое с учетом (2.36)-(2.37) определяется как:

$$\begin{aligned} &Q_j^{Цz} = \arg \max_{z_h \in Z_j} \{\max_{w \in W}\left(Q_w^{ЦZB}, Q\left(d_r \in D_h^V\right)\right) \Big| Z_j \neq \varnothing, D_h^V \neq \varnothing\}, \\ &j = \overline{1,m}, \quad h = \overline{1,m} \end{aligned} \tag{2.38}$$

Если $Z_j = \varnothing$, то $Q_j^{Цz} = \arg \max_{w \in W} Q_w^{ЦZB}$.

В разрабатываемой АСОИУ результаты решения задач могут быть входными данными других задач, поэтому нарушение целостности входных данных либо задач может привести к нарушению работоспособности всей АСОИУ в целом. Зная статистику нарушений ИБ, заказчик спрогнозировал

интенсивности атак λ_{z_j} на каждую из задач $z_j \in Z$. Зная это можно определить средние интервалы между попытками нарушения целостности задач.

$$\tau_{z_j} = \frac{1}{\lambda_{z_j}}, \qquad (2.39)$$

Построим с помощью матрицы смежности задач $B_3 = [b_{hj}^{(3)}]_{m \times m}$, задающей частное бинарное отношение $R_3 \subseteq Z \times Z$, множество путей L в графе $G(Z)$. Данная задача может быть решена с использованием методов теории графов[59].

Рассмотрим некоторый путь $l(z_1, z_2, ..., z_y, ..., z_r) \in L$, где $r \in \overline{(1,R)}$, $R = |L|$, $z_y \in Z$, $y = \overline{(1,r)}$, а $r = |l|$. Определим, вероятности обеспечения целостности задач с учетом значений полученных по формуле (2.39): $Q_{z_y} = (Q_Z)^{\alpha_{z_y}}$, где $\alpha_{z_y} = \frac{\tau_{z_y}}{\sum_1^r \tau_{z_y}}$ и величина Q_Z - это значение вероятности обеспечения целостности задач Z в АСОИУ, которая определяется из второго выражения формулы (2.34). Проведя аналогичные расчеты для каждого пути $l(z_1, z_2, ..., z_y, ..., z_r) \in L$, сформируем требования предъявляемые к уровню целостности задач $z_j \in Z$, $j = \overline{(1,m)}$ решаемых в разрабатываемой АСОИУ. В связи с тем, что одна и тоже задача $z_y \in Z$, $y = \overline{(1,r)}$ может принадлежать нескольким путям графа смежности задач $G(Z)$ окончательной значение вероятности $Q_{z_y}^o$ обеспечения требуемого уровня целостности каждой из задач решаемой в АСОИУ определяется как:

$$Q_{z_y}^o = \max_{l \in L} Q_{z_y}, \quad y = \overline{(1,m)}, l = \overline{(1,L)}. \qquad (2.40)$$

Таким образом, мы получим ряд задач $z_y \in Z$, $y = \overline{(1,r)}$, для которых сформировано два значения вероятностей обеспечения целостности задач по

формуле (2.40) и по формуле (2.38). Назначим задаче $z_y \in Z$, $y = \overline{(1,r)}$ уровень целостности равный:

$$Q_y^{ЦZ} = \max\left(Q_y^{Цz}, Q_{z_y}^{o}\right). \qquad (2.41)$$

Обозначим через $Q_{jf}^{цел}$ - вероятности обеспечения требуемого уровня целостности ТС $t_f \in T$ при его использовании для решения задачи $z_j \in Z$.

Определим уровни обеспечения целостности используемых при решении задачи $z_j \in Z$ ТС исходя из интенсивностей атак $\lambda_{jf}^{цел} = 1/\tau_{jf}^{цел}$ на компоненту целостности ТС. Вероятности обеспечения целостности ТС по аналогии с формулой (2.33) примут вид:

$$Q_{jf}^{цел} = b_{jf}^{(4)}\left(Q_j^{ЦZ}\right)^{\alpha_{jf}^{цел}}, \qquad (2.42)$$

где $\alpha_{jf}^{цел} = \dfrac{b_{jf}^{(4)}\tau_{jf}^{цел}}{\sum\limits_{f=1}^{t} b_{jf}^{(4)}\tau_{jf}^{цел}}$. В формуле (2.42) величина $Q_j^{ЦZ}$ –это значение вероятности обеспечения целостности задачи $z_j \in Z$, которая определяется из формулы (2.41). По аналогии с рассуждениями для компоненты конфиденциальности получим значения вероятностей обеспечения целостности $Q_{jf}^{цел}$ ТС $t_f \in T$. Если для ТС сформировано несколько значений вероятностей обеспечения целостности $Q_{f_1}^{цел}$, $Q_{f_2}^{цел}$,… $Q_{f_g}^{цел}$, то из них выбирается максимальное: $Q_f^{цел} = \max\{Q_{f_1}^{цел}, Q_{f_2}^{цел}, \ldots, Q_{f_g}^{цел}\}$.

Формирование допустимых значений вероятностей обеспечения доступности технических средств и программного обеспечения АСОИУ. Рассмотрим требования, предъявляемые к доступности информации. В работе [1] сказано, что доступность компонента - это свойство компонента быть доступным для авторизованных законных субъектов системы. Сформируем требования, предъявляемые к доступности ТС разрабатываемой АСОИУ. В

качестве исходных данных будем использовать уровни доступности задач Z решаемых в системе и входных данных D, граф связи ТС $G(T)$ и вероятность обеспечения доступности компоненты ИБ разрабатываемой АСОИУ равную $Q_{дост}^{доп}$, ее значение можно определить по формуле (2.4). Определим уровни доступности задач Z аналогично тому, как это было сделано для уровней целостности задач Z:

$$Q_D^{дост} = \left(Q_{дост}^{доп}\right)^{\alpha}, \quad Q_Z^{дост} = \left(Q_{дост}^{доп}\right)^{\beta}, \qquad (2.43)$$

где $\alpha = \frac{\tau_D^{дост}}{\tau_D^{дост} + \tau_Z^{дост}}, \beta = \frac{\tau_Z^{дост}}{\tau_D^{дост} + \tau_Z^{дост}}$, а $\tau_D^{дост}$, $\tau_Z^{дост}$ среднее интервалы времени между попытками нарушения доступности данных и задач, которые определяются из выражений вида: $\tau_D^{дост} = \frac{1}{\lambda_D^{дост}}$, $\tau_Z^{дост} = \frac{1}{\lambda_Z^{дост}}$, где $\lambda_D^{дост}$, $\lambda_Z^{дост}$ интенсивности атак нарушения доступности множества данных D и множества задач Z заданные заказчиком.

Для каждого уровня конфиденциальности $k \in K$ определим, интенсивности $\lambda_k^{дост}$ и следовательно среднее интервалы времени $\tau_k^{дост} = 1/\lambda_k^{дост}$ между попытками нарушения доступности данных k-го уровня конфиденциальности. Далее определим вероятность обеспечения доступности входных данных k - го уровня конфиденциальности:

$$Q_k^{ДВ} = \left(Q_D^{дост}\right)^{\alpha_k^{дост}},$$

где $\alpha_k^{дост} = \frac{\tau_k^{дост}}{\sum_{k=0}^{K} \tau_k^{дост}}$, а величина $Q_D^{дост}$ - вычисляется по формуле (2.43). Для каждого уровня конфиденциальности $k \in K$ получен требуемый уровень доступности данных Q_k^{DB}, $k \in K$, $|K| = |U|$. Для формирования требуемых уровней доступности задач Z и выходных данных D^V сформируем ряд правил:

уровни доступности задач и формируемых при их решении выходных данных зависят только от уровней доступности используемых входных данных, если некоторый элемент АСОИУ имеет несколько уровней доступности, то ему должен быть присвоен максимальный из имеющихся у него уровень.

Сформируем для фиксированного значения $j \in \overline{(1,m)}$ совокупность множеств, определяемых по формуле вида: $D_{ju}^{B} = D_{j}^{B} \cap D_{u}^{B}$, $u \in U$, где подмножество D_{j}^{B} находится по формуле (2.26). Если для некоторого фиксированного значения u множество $D_{ju}^{B} \neq 0$, то данные этого уравнения используются при решении задачи $z_j \in Z$.

Пусть для задачи $z_j \in Z$ не пустыми оказались множества $D_{ju_1}^{B}, D_{ju_2}^{B}, \ldots, D_{ju_p}^{B}$, где $u_1 > u_2 > \ldots > u_p$ - отдельные элементы множества U. Тогда этой задаче назначается наивысший из полученных уровень обеспечения доступности равный $u_1 \in U$. Таким образом, получаем следующее решающее правило для формирования вероятностей обеспечения требуемого уровня доступности $Q_j^{ДZB}$ задачи $z_j \in Z$ с использованием ее входным данным:

$$Q_j^{ДZB} = \arg\max_{u \in U} \left\{ Q_u^{ДВ} \middle| D_{ju}^{B} \neq \varnothing \right\}, \quad j = \overline{(1,m)}.$$

Аналогичным образом назначаются уровни доступности выходным данным $d_r^V \in D^V$. Используя выражение (2.28) выделим для каждой задачи $z_j \in Z$ подмножество формируемых ею выходных данных D_j^V. Для назначения уровней доступности выходным данным АСОИУ предлагается использовать следующие решающие правила:

1) Если задача $z_j \in Z$ имеет определенный выше u - й уровень доступности, то такой же уровень должны иметь все данные, входящие в множество D_j^V, то есть

$$Q\left(d_r^V \in D_j^V\right) = Q_j^{ДZB}, \quad j = \overline{(1,m)},$$

2) если какой-либо элемент $d_r^V \in D^V$ формируется более чем одной задачей, например задачами z_{j1}, z_{j2}, … , z_{jq}, то вероятность обеспечения требуемого уровня доступности этого элемента определяется как:

$$Q\left(d_r^V \in D_j^V\right) = \max\left\{Q_{j1}^{ДZB}, Q_{j2}^{ДZB}, \ldots, Q_{jq}^{ДZB}\right\}, \quad j = \overline{(1,m)}.$$

В общем случае уровень доступности любой задачи $z \in Z$ будет зависеть и от уровня доступности предшествующих ей по принятой в АСОИУ технологии задач и используемых ею выходных данных смежных задач.

Для каждой задачи $z_j \in Z$ выделим, используя выражение (2.30) подмножество смежных ей задач. Проведя рассуждения аналогичные рассуждениям при определении уровней целостности задач, получим решающее правило для определения уровней доступности задач $z_j \in Z$ решаемых в АСОИУ:

$$\begin{aligned} &Q_j^{Дz} = \arg \max_{z_h \in Z_j} \{\max_{u \in U}\left(Q_u^{ДZB}, Q\left(d_r \in D_h^V\right)\right) \Big| Z_j \neq \varnothing, D_h^V \neq \varnothing\}, \\ &j = \overline{(1,m)}, \quad h = \overline{(1,m)} \end{aligned} \tag{2.44}$$

Если $Z_j = \varnothing$, то $Q_j^{Дz} = \arg\max_{u \in U} Q_u^{ДZB}$. В разрабатываемой АСОИУ результаты решения задач могут быть входными данными других задач, поэтому нарушение доступности входных данных (задач) может привести к нарушению работоспособности всей АСОИУ в целом.

Пусть зная статистику нарушений ИБ, заказчик спрогнозировал интенсивности атак $\lambda_{z_j}^{дост}$ нарушения доступности каждой из задач $z_j \in Z$. Используя это можно определить средние интервалы между попытками нарушения доступности задач.

$$\tau_{z_j}^{дост} = \frac{1}{\lambda_{z_j}^{дост}}, \tag{2.45}$$

Рассмотрим описанный выше путь $l(z_1, z_2,...,z_y,...,z_r) \in L$ графа смежности задач. Определим, вероятности обеспечения доступности задач с учетом интервалов полученных по формуле (2.45).

$$Q_{z_y}^{дост} = \left(Q_Z^{дост}\right)^{\alpha_{z_y}^{дост}}, \qquad (2.46)$$

где $\alpha_{z_y}^{дост} = \dfrac{\tau_{z_y}^{дост}}{\sum_1^r \tau_{z_y}^{дост}}$. В формуле (2.46) величина $Q_Z^{дост}$ - это значение вероятности обеспечения доступности задач Z в АСОИУ, которая определяется из второго выражения формулы (2.43). Как уже отмечалось выше (2.40) одна и тоже задача $z_y \in Z$, может принадлежать нескольким путям графа смежности задач $G(Z)$, поэтому по аналогии окончательное значение вероятности $Q_{z_y}^{дост^{\,o}}$ обеспечения требуемого уровня доступности каждой из задач решаемой в АСОИУ определяется как:

$$Q_{z_y}^{дост^{\,o}} = \max_{l \in L} Q_{z_y}^{дост}, \quad y = \overline{(1,m)}, \quad l = \overline{(1,L)}. \qquad (2.47)$$

Таким образом, мы получим ряд задач $z_y \in Z$, $y = \overline{(1,r)}$, для которых сформировано два значения вероятностей обеспечения доступности задач $Q_{z_y}^{дост^{\,o}}$ по формуле (2.47) и $Q_j^{Дz}$ по формуле (2.44). Назначим задаче $z_y \in Z$, $y = \overline{(1,r)}$ уровень доступности равный:

$$Q_y^{ДZ} = \max\left(Q_y^{Дz}, Q_{z_y}^{дост^{\,o}}\right). \qquad (2.48)$$

Проведя аналогичные расчеты для каждого пути $l \in L$, сформируем требования, предъявляемые к уровню доступности задач $z_j \in Z$, $j = \overline{(1,m)}$ решаемых в разрабатываемой АСОИУ. Если в АСОИУ существуют задачи, которые по прогнозу заказчика не будут подвергаться атакам, то им следует назначить интенсивность атак равную максимальной интенсивности атак ис-

пользуемых ею при решении входных данных. Возможен вариант, когда по прогнозу заказчика задача и ее входные данные не будут атаковаться. В этом случае, следует исключить данную задачу и дуги, входящие и исходящие из нее из графа $G(Z)$ и назначить ей вероятность обеспечения целостности и доступности равную нулю. Теперь когда сформированы вероятности обеспечения доступности задач $Q_j^{ДZ}$, можно определить требования предъявляемые к уровням доступности ТС.

Рассмотрим множество, ТС T упомянутое выше такое, что $|T| = t$ и частное бинарное отношения (2.32), которое может быть описано булевской матрицей $B_4 = [b_{jf}^{(4)}]_{m \times t}$. Обозначим через $Q_{jf}^{дост}$ - вероятности обеспечения требуемого уровня доступности ТС $t_f \in T$ при его использовании для решения задачи $z_j \in Z$. Определим уровни обеспечения доступности используемых при решении задачи $z_j \in Z$ ТС исходя из интенсивностей атак $\lambda_{jf}^{дост} = 1/\tau_{jf}^{дост}$ на компоненту доступности ТС. Вероятности обеспечения доступности ТС по аналогии с формулой (2.33) примет вид:

$$Q_{jf}^{дост} = b_{jf}^{(4)} \left(Q_j^{ДZ} \right)^{\alpha_{jf}^{дост}}, \qquad (2.49)$$

где $\alpha_{jf}^{дост} = \dfrac{b_{jf}^{(4)} \tau_{jf}^{дост}}{\sum_{f=1}^{t} b_{jf}^{(4)} \tau_{jf}^{дост}}$. В формуле (2.49) величина $Q_j^{ДZ}$ - это значение вероятности обеспечения доступности задачи $z_j \in Z$, которая определяется из формулы (2.48). Проведя аналогичные расчеты для каждой задачи $z_j \in Z$, получим значения вероятностей обеспечения доступности $Q_{jf}^{дост}$ ТС $t_f \in T$. Если для ТС сформировано несколько значений вероятностей обеспечения доступности $Q_{f_1}^{дост}$, $Q_{f_2}^{дост}$,… $Q_{f_g}^{дост}$, то из них выбирается максимальное: $Q_f^{дост} = \max\{Q_{f_1}^{дост}, Q_{f_2}^{дост}, \ldots, Q_{f_g}^{дост}\}$.

2.3. Примеры вычисления допустимых вероятностных характеристик информационной безопасности АСОИУ.

Пример 1. Пусть введенные выше параметры решения задачи для некоторой условной АСОИУ составляют соответственно C_1=100 млн.руб. в год, а C_2=1 млн.руб. в год. Зададимся значениями ε равным 0.001 и q^* равным 0,95. Из формул (2.15),(2.16) следует, что параметр λ должен варьироваться в интервале $[\lambda^*,\lambda^{**}]$=[0.97994;0.98862]. Факт наличия точки минимума свертки (2.6) для $\overline{\lambda}=\dfrac{\left(\lambda^*+\lambda^{**}\right)}{2}=0.984$ иллюстрируется на рис. 2.2.

Результаты вычислительных экспериментов приведены в таблице 1 Приложения 1 для случая 49 вариантов паретооптимальных решений полученных с шагом $\Delta\lambda=0{,}0021$. Приведённые в таблице результаты иллюстрируют тенденцию увеличения с ростом λ значения q и $Z_C(q)$, а так же уменьшения затрат $Z_\Phi(q)$. Последнее полностью соответствует характеру паретооптимального множества решений представленного на рис. 2.1.

Рис. 2.2.

Пусть по результатам таблицы 1 Приложения 1 заказчиком системы выбран вариант №49. При внедрении данного варианта потери от НСД составят $Z_ф = 1015$ руб. в год, а затраты на разработку СИБ соответственно будут равны $Z_c = 998669$ руб. в год. При этом вероятность безопасного функционирования данной АСОИУ составит величину q_{49}=0,9987. Отсюда вероятность преодоления СИБ определяется как $p = 1 - q$. Это означает что, на 10000 попыток преодоления СИБ только 13 попыток могут будут удачными.

Приведём для сравнения фактические значения вероятностей нарушения ИБ действующих систем по исходным данным работы [3]. В СИБ космического центра NASA им. Джонсона регистрировалось 3-4 попытки НСД в сутки[3]. Оценим имеющуюся в системе вероятность p нарушения ИБ и уровень её ИБ q, с учетом того, что за год, как сообщается, не было ни одной успешной попытки. Последнее позволяет, следуя работе[67] определить верхнюю границу доверительного интервала $(0, p_2)$ для вероятности p. Зададимся доверительной вероятностью для нахождения этой границы β равной 0,95. Так как в день было в среднем $\frac{3+4}{2} = 3{,}5$ попытки НСД, то в год получим соответственно $n = 3{,}5 \cdot 365 \approx 1278$ попыток доступа в систему. Величину p_2 можно найти из выражения вида[67]:

$$p_2 = 1 - \sqrt[n]{1-\beta},$$

В рассматриваемом случае истинное значение веоятности p будет лежать в интервале $0 < p < 0{,}002341$. Используя, равенство $q = 1 - p$ находим крайнюю левую точку для доверительного интервала $q_2 = 1 - p_2 = 0{,}997659$, содержащего значение вероятности q обеспечения ИБ при функционировании СИБ космического центра NASA. В этом случае доверительный интервал для вероятности q имеет вид $(0.997659, 1)$. Можно заметить, что вариант №49 таблицы 1 Приложения 1 с значением вероятности $q_{49} = 0{,}9987$ попада-

ет в построенный интервал. Это говорит о том что, полученная модель позволяет выбрать компромиссное решение адекватное уровню ИБ реальной СИБ.

По данным работы [3] в центре информационной борьбы ВВС США, за первые 3 недели после его создания было зарегистрировано более 150 попыток НСД. Оценим значение q, построив для него доверительный интервал с доверительной вероятностью $\beta = 0.95$. Для этого аналогично найдём предполагаемое число атак в год, которое равно $n = \frac{150}{21} \cdot 365 \approx 2607$. Проводя аналогичные приведенным выше расчёты, получаем, что фактическое значение вероятности p для рассматриваемой системы лежит в интервале $(0;0,001148)$. В этом случае фактическое значение вероятности ИБ этой системы q располагается в интервале $(0,99885;1)$. Сравнивая этот интервал с результатами вычислительных экспериментов(см. таблицу 1 Приложения 1), получаем, что наилучший с точки зрения минимума потерь вариант №49, имеющий значение $q_{49} = 0,9987$, отличается от левой границы этого интервала на достаточно малую величину 0,00009.

Сравнение приведённого в примере априорного значения вероятности обеспечения ИБ с доверительными интервалами для такой безопасности у существующих систем показывает адекватность предлагаемого в работе подхода реально действующим информационным системам.

Пример 2. Рассмотрим АСОИУ, в которой фигурируют данные четырёх уровней конфиденциальности: совершенно секретные данные – 3 уровень, секретные данные – 2 уровень; данные служебного пользования – 1 уровень; открытые данные – 0 уровень. Заказчик задал уровень ИБ для разрабатываемой АСОИУ $Q_{ИБ}^{доп}$=0,9. Так же заказчик спрогнозировал следующие интенсивности попыток нарушения [1,3,66] конфиденциальности, целостно-

сти и доступности компонент ИБ АСОИУ: $\lambda_{конф} = 10$, $\lambda_{цел} = 5$ и $\lambda_{дост} = 2$ за сутки.

Пусть D^i_{Bj} - j-е входные конфиденциальные данные i-го уровня, а D_{Vj} - j-е выходные данные. Ниже приведен перечень входных и выходных данных рассматриваемой АСОИУ: $D^0_{B1}, D^0_{B2}, \ldots, D^0_{B14}$; $D^1_{B1}, D^1_{B2}, \ldots, D^1_{B6}$; $D^2_{B1}, D^2_{B2}, D^2_{B3}$; D^3_{B1}; $D_{V1}, D_{V2}, \ldots, D_{V12}$. Пусть z_i-i-я задача, решаемая в АСОИУ. Тогда перечень задач для рассматриваемой АСОИУ имеет вид: $z_1, z_2 \ \ldots \ z_{12}$. Граф связи задач $G(Z)$ и структурная схема аппаратных средств АСОИУ представлены на рис. 2.3. и 2.4.

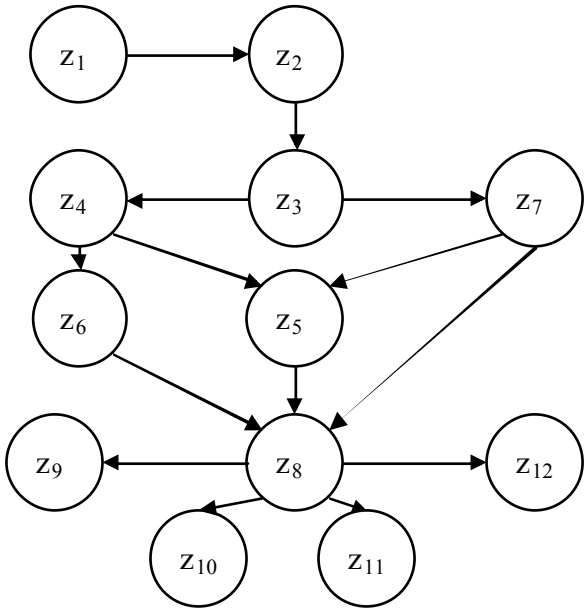

Рис. 2.3.

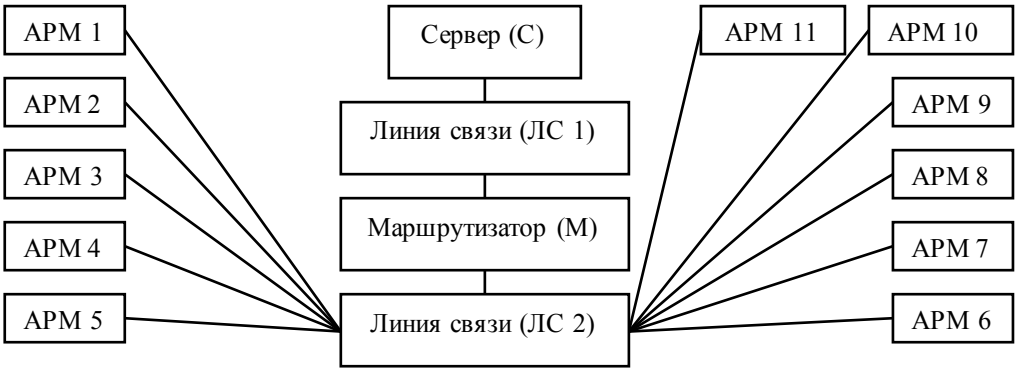

Рис. 2.4.

Запишем для рассматриваемой АСОИУ описанные выше булевские матрицы $B_1 = [b_{ij}^{(1)}]_{n\times m}$, $B_2 = [b_{jr}^{(2)}]_{m\times l}$, $B_3 = [b_{hj}^{(3)}]_{m\times m}$, $B_4 = [b_{jw}^{(4)}]_{m\times t}$ в виде таблиц 2–5 Приложения 1. В них пустым ячейкам соответствуют нули.

Определим средние интервалы между попытками нарушения ИБ компонент конфиденциальности, целостности и доступности с использованием ожидаемых интенсивностей нарушения ИБ этих компонент $\lambda_{конф} = 10$, $\lambda_{цел} = 5$ и $\lambda_{дост} = 2$ по формуле (2.19): $\tau_{конф} = \frac{1}{\lambda_{конф}} = 0.1$, $\tau_{цел} = \frac{1}{\lambda_{цел}} = 0.2$, $\tau_{дост} = \frac{1}{\lambda_{дост}} = 0.5$. Зная требуемый уровень ИБ разрабатываемой АСОИУ $Q_{ИБ}^{доп}$=0,9 и средние интервалы времени между попытками нарушения ИБ компонент конфиденциальности, целостности и доступности можно, используя формулу (2.20), найти вероятности обеспечения ИБ компонент конфиденциальности, целостности и доступности: $Q_{конф} = 0.9869$, $Q_{цел} = 0.974$, $Q_{дост} = 0.9363$.

Заказчиком спрогнозированы интенсивности попыток нарушения конфиденциальности входных данных первого, второго и третьего уровней конфиденциальности за сутки: $\lambda_1^{конф} = 2$, $\lambda_2^{конф} = 3$ и $\lambda_3^{конф} = 5$. Следовательно, можно определить ожидаемые средние интервалы времени между нарушениями входных данных первого, второго и третьего уровней конфиденциальности в виде: $\tau_1^{конф} = \frac{1}{\lambda_1^{конф}} = 0.5$, $\tau_2^{конф} = \frac{1}{\lambda_2^{конф}} = 0.333$, $\tau_3^{конф} = \frac{1}{\lambda_3^{конф}} = 0.2$. Далее используя вероятность обеспечения ИБ компоненты конфиденциальности $Q_{конф} = 0.9869$ и значения, определяющие средние интервалы времени между нарушениями конфиденциальности входных данных первого, второго и третьего уровней, определим вероятности обеспечения ИБ конфиденциаль-

ности входных данных первого, второго и третьего уровней: $Q_1^B = 0.9936$, $Q_2^B = 0.9958, Q_3^B = 0.9975$.

Заказчик оценил среднее количество попыток нарушения конфиденциальности отдельных узлов АСОИУ величиной в 3-7 раз в сутки, и задал, с учетом формулы (2.19), следующие оценки интервалов между попытками нарушения ИБ ТС (см. таблицу 6 Приложение 1). Найдем допустимые вероятности обеспечения ИБ конфиденциальности данных решаемых задач с использованием таблиц 2-4 Приложения 1 и вероятностей обеспечения ИБ конфиденциальности входных данных первого, второго и третьего уровней: $Q_1^B = 0.9936$, $Q_2^B = 0.9958$ и $Q_3^B = 0.9975$. Результат приведен в таблице 7 Приложения 1.

Найдем вероятности обеспечения конфиденциальности информации при прохождении ее через ТС АСОИУ на примере задачи z_2. Применим методику, описанную выше для определения вероятностей обеспечения конфиденциальности информации ТС АСОИУ. При решении задачи используются следующие ТС: АРМ2-АРМ7, АРМ10, АРМ11, С, ЛС1, М, ЛС1. Для этих ТС заказчик прогнозирует средние интервалы между попытками нарушения конфиденциальности представленные в таблице 6 Приложения 1.

Уровень ИБ по конфиденциальности для z_2 равен 0,9958. Тогда найдем вероятности обеспечения ИБ ТС используемых при решении задачи z_2. Результат приведён в таблице 8 Приложения 1.

Аналогично для других задач получим результаты, которые приведен в таблице 9 Приложения 1. В каждом ее столбце выбирается максимальное значение, оно принимается за допустимое с точки зрения ИБ. Таким образом, формируются требования по ИБ предъявляемые к каждому ТС используемому в проектируемой АСОИУ. Конечный результат приведён в таблице 10 Приложения 1, где во второй строке указаны допустимые значения вероятностей обеспечения ИБ ТС.

Из полученных результатов следует, что более жесткие требования по обеспечению конфиденциальности ИБ предъявляются к тем ТС, которые участвуют при решении задач, использующих данные наивысшего уровня конфиденциальности, а так же к наиболее загруженным ТС системы. Это видно на примере сервера и маршрутизатора (см. рис. 2.3), которые имеют вероятности обеспечения ИБ компоненты конфиденциальности равные 0,9998. Рассуждая аналогично, можно отметить, что АРМ1 имеет самые низкие требования, предъявляемые к обеспечению ИБ равные 0,9989.

Перейдем к формированию требований обеспечения целостности ИБ рассматриваемой АСОИУ. Заказчиком спрогнозированы интенсивности попыток нарушения целостности входных данных нулевого, первого, второго и третьего уровней конфиденциальности: $\lambda_0^{цел} = 1$, $\lambda_1^{цел} = 2$, $\lambda_2^{цел} = 3$ и $\lambda_3^{цел} = 5$. Используя вероятность обеспечения ИБ компоненты целостности $Q_{цел}^{доп} = 0.974$ и интенсивности попыток нарушения целостности входных данных, определим вероятности обеспечения ИБ целостности входных данных нулевого, первого, второго и третьего уровней: $Q_0^{ЦВ} = 0.9871$, $Q_1^{ЦВ} = 0.9935$, $Q_2^{ЦВ} = 0.9957$, $Q_3^{ЦВ} = 0.9974$. Заказчик оценил среднее количество попыток нарушения целостности отдельных задач АСОИУ величиной в 3-7 раз за сутки, и задал следующие интенсивности попыток нарушения ИБ задач (см. таблицу 11 Приложения 1).

Определим требования, предъявляемые к задачам, решаемым в АСОИУ, а именно найдем допустимые вероятности обеспечения ИБ целостности данных решаемых задач с использованием таблиц 2-4 Приложения 1 и вероятностей обеспечения ИБ целостности конфиденциальных входных данных нулевого, первого, второго и третьего уровней: $Q_0^{ЦВ} = 0.9871$, $Q_1^{ЦВ} = 0.9935$, $Q_2^{ЦВ} = 0.9957$, $Q_3^{ЦВ} = 0.9974$. Результат приведен в таблице 12 Приложения 1. Построим множество путей L:

$$l_1=\{z_1,z_2,z_3,z_4,z_6,z_8,z_9\} \quad l_5=\{z_1,z_2,z_3,z_4,z_5,z_8,z_9\}$$
$$l_2=\{z_1,z_2,z_3,z_4,z_6,z_8,z_{10}\} \quad l_6=\{z_1,z_2,z_3,z_4,z_5,z_8,z_{10}\}$$
$$l_3=\{z_1,z_2,z_3,z_4,z_6,z_8,z_{11}\}, \quad l_7=\{z_1,z_2,z_3,z_4,z_5,z_8,z_{11}\}$$
$$l_4=\{z_1,z_2,z_3,z_4,z_6,z_8,z_{12}\} \quad l_8=\{z_1,z_2,z_3,z_4,z_5,z_8,z_{12}\}$$
$$l_9=\{z_1,z_2,z_3,z_7,z_5,z_8,z_9\} \quad l_{13}=\{z_1,z_2,z_3,z_7,z_8,z_9\}$$
$$l_{10}=\{z_1,z_2,z_3,z_7,z_5,z_8,z_{10}\} \quad l_{14}=\{z_1,z_2,z_3,z_7,z_8,z_{10}\}$$
$$l_{11}=\{z_1,z_2,z_3,z_7,z_5,z_8,z_{11}\}, \quad l_{15}=\{z_1,z_2,z_3,z_7,z_8,z_{11}\}$$
$$l_{12}=\{z_1,z_2,z_3,z_7,z_5,z_8,z_{12}\} \quad l_{16}=\{z_1,z_2,z_3,z_7,z_8,z_{12}\}$$

Определим требования, предъявляемые к задачам, решаемым в АСОИУ с использованием интенсивностей попыток нарушения целостности задач (таблица 11 Приложения 1). Для каждого из множества путей $l_r \in L$, определим требования, предъявляемые к вероятностям обеспечения целостности задач включенных в этот путь. Результат приведен в таблице 13 Приложения 1. Выберем в каждом столбце таблицы 13 Приложения 1 максимальное значение (см. таблицу 14 Приложения 1). Построим таблицу 15 Приложения 1, в которой первая строка это перечень всех задач, вторая строка совпадает со вторым столбцом таблицы 11 Приложения 1, третья строка совпадает со второй строкой таблицы 14 Приложения 1, а четвертая строка состоит из максимальных элементов каждого ее столбца. Таким образом, в четвертой строке таблицы 15 Приложения 1 будут сформированы требования, предъявляемые к целостности задач решаемых в АСОИУ.

Определим требования, предъявляемые к ТС, исходя из уровней целостностей задач и интенсивностей нарушения целостности ТС (см. таблицу 16 Приложения 1). Результат приведен в таблице 17 Приложения 1. По аналогично с таблицами 9 и 10 Приложения 1 для компоненты конфиденциальности построим таблицы 17 и 18 Приложения 1, которые содержит требования к ТС с точки зрения компоненты целостности. Таким образом, более жесткие требования по обеспечению ИБ предъявляются к тем ТС, которые

используют данные наивысшего уровня целостности и к наиболее часто востребованным ТС.

Сформируем требования предъявляемые к компоненте доступности ИБ рассматриваемой АСОИУ. Допустимая вероятность обеспечения ИБ доступности $Q_{дост}^{доп} = 0.9363$. Заказчик оценил среднее количество попыток нарушения доступности отдельных задач АСОИУ величиной в 3-7 раз за сутки и задал следующие интенсивности попыток нарушения ИБ задач (см. таблицу 19 Приложения 1). Используя вероятность обеспечения ИБ компоненты доступности $Q_{дост}^{доп} = 0.9363$ и интенсивности попыток нарушения доступности входных данных, определим вероятности обеспечения ИБ доступности входных данных нулевого, первого, второго и третьего уровней: $Q_0^{ДВ} = 0.9681$, $Q_1^{ДВ} = 0.9839$, $Q_2^{ДВ} = 0.9893$, $Q_3^{ДВ} = 0.9935$. Найдем допустимые вероятности обеспечения ИБ доступности данных решаемых задач с использованием таблиц 2-4 Приложения 1 и вероятностей обеспечения ИБ доступности конфиденциальных входных данных нулевого, первого, второго и третьего уровней: $Q_0^{ДВ} = 0.9681$, $Q_1^{ДВ} = 0.9839$, $Q_2^{ДВ} = 0.9893$, $Q_3^{ДВ} = 0.9935$. Результат приведен в таблице 20 Приложения 1. Определим требования, предъявляемые к задачам, решаемым в АСОИУ с использованием интенсивностей попыток нарушения доступности задач (таблица 19 Приложения 1) и распределения задач по ТС (таблица 5 Приложения 1). Для каждого пути $l_r \in L$, определим требования, предъявляемые к вероятностям обеспечения доступности задач включенных в этот путь. Результат приведен в таблице 21 Приложения 1. Выберем в каждом столбце таблицы 21 Приложения 1 максимальное значение (см. таблицу 22 Приложения 1). Построим таблицу 20 Приложения 1, в которой первая строка это перечень всех задач, вторая строка совпадает со вторым столбцом таблицы 17 Приложения 1, третья строка совпадает со второй строкой таблицы 19 Приложения 1, а четвертая строка состоит из макси-

мальных элементов каждого столбца. Таким образом, в четвертой строке таблицы 23 Приложения 1 будут сформированы требования, предъявляемые к доступности задач решаемых в АСОИУ. Определим требования, предъявляемые к ТС, исходя из уровней доступности задач и интенсивностей нарушения доступности ТС (см. таблицу 24 Приложения 1). Результат приведен в таблице 25 Приложения 1. Окончательный результат определения уровней обеспечения доступности ТС приведён в таблице 26 Приложения 1.

Выводы по главе 2.

1. Предложена математическая модель и метод, позволяющий формировать компромиссное значение требуемой вероятности обеспечения ИБ АСОИУ с учетом совокупной стоимости применяемых СИБ и возможных при этом потерь от НСД к конфиденциальной информации.

2. Для формирования количественных вероятностных характеристик ИБ компонент АСОИУ предлагается использовать статистику попыток нарушения ИБ реальных АСОИУ или же спрогнозированные Заказчиком интенсивности попыток нарушения ИБ компонент АСОИУ.

3. Разработана методика формирования допустимых значений вероятностей обеспечения ИБ конфиденциальности, целостности и доступности информации циркулирующей в АСОИУ, а так же данных, задач и ТС системы.

4. Приведен пример вычисления допустимых вероятностных характеристик ИБ данных, задач и ТС АСОИУ. При решении использовались заданные Заказчиком интенсивности попыток нарушения ИБ конфиденциальности, целостности, доступности, а так же данных, задач и ТС системы. В системе фигурируют данные четырёх уровней конфиденциальности: совершенно секретно, секретно, ДСП, открытые данные, Заказчиком был задан допустимый уровень ИБ разрабатываемой АСОИУ $Q_{ИБ}^{доп}=0,9$.

Глава 3. Вероятностные модели и методы обеспечения информационной безопасности АСОИУ.

В данной главе предлагаются модели и методы решения задач, приведенных на третьем уровне дерева целей и задач, представленного на рисунке 1.1. Эти модели наряду с моделями и методами, представленными в главе 2, должны, на наш взгляд, составить основу ПТИБ, цели и задачи которой были определены в первой главе работы. При разработке предполагаемых моделей и методов были использованы такие принципы ПТИБ, как принцип комплексности применяемых СИБ, принцип экономичности СИБ, принцип максимальной ИБ критических компонентов АСОИУ, принцип прогнозирования угроз и применения средств нападения, принцип обеспечения максимальной неопределённости для противника применяемых стратегий по обеспечению ИБ, принцип применения экспертных и статистических оценок, а так же базовые модели теории (1.7),(1.15),(1.22),(1.25).

3.1. Математическая модель выделения критических элементов системы.

Рассмотрим задачу выявления критических компонент прикладных ИТ [105], описываемых моделью вида (1.15). Комплексная безопасность АСОИУ обеспечивается при полной реализации всех технологий, описываемых отношением (1.15). Реализация каждой ИТ, входящей в это множество связывается с определенным маршрутом в графе, представленном на рис. 1.2. При этом каждый маршрут должен начинаться в определенной вершине множества “ЛГР” и заканчиваться в соответствующей вершине множества “Решения”.

Обозначим граф прикладных ИТ как $J(X, Д)$, где $X = П_1 \cup A \cup B \cup P \cup П_2 \cup R$ - множество вершин, $Д$ – множество дуг графа. Будем считать, что нарушение нормальной работы любой вершины $x \in X$ этого графа за счет «взлома» или отказа соответствующего компонента

АСОИУ приводит к невозможности реализации соответствующей прикладной ИТ из их наличного множества. Обозначим, через L - полное множество маршрутов в графе $J(X, Д)$ и построим матрицу $\Omega = [\omega_{lk}]$ с элементами:

$$\omega_{lk} = \begin{cases} 1, & \textit{если вершина } x_k \in X \textit{ входит в маршрут } l_k \in L; \\ 0, & \textit{в противном случае.} \end{cases}$$

Выделим в графе J минимальное число вершин, через которые проходят все пути множества L. Данная задача может быть решена с использованием формализма «задача о минимальном покрытии» [68]. Введём вектор булевских переменных $\xi = (\xi_1, \xi_2, \ldots \xi_n)$, где $n = |X|$ - число вершин графа J. Любая переменная ξ_k - может принимать следующие значения:

$$\xi_k = \begin{cases} 1, & \textit{если вершина } x_k \in X \textit{ включена в минимальное покрытие}; \\ 0, & \textit{в противном случае.} \end{cases}$$

Это требование можно записать в виде следующих ограничений:

$$\xi_k \in \{0;1\}, \quad k = \overline{(1,n)} \tag{3.1}$$

Условия того, чтобы через каждую вершину, входящую в минимальное покрытие, проходил не менее чем один маршрут множества L записывается как

$$\sum_{k=1}^{n} \omega_{lk} \xi_k \geq 1, \quad l \in L \tag{3.2}$$

С учетом ограничений (3.1) требование минимальности числа вершин, входящих в искомое покрытие представляется целевой функцией вида:

$$N = \sum_{k=1}^{n} \xi_k \to \min_{\xi_k} \tag{3.3}$$

В работе [62] отмечается, что решение задачи линейного булевского программирования (3.3)–(3.2),(3.1) может быть не единственным. С точки зрения сформулированной задачи в совокупности рассматриваемых прикладных ИТ может присутствовать несколько подмножеств «критических»

компонент. Для ликвидации неоднозначности при их выявлении рассмотрим дополнительную целевую функцию вида:

$$P = \prod_{k=1}^{n} p_k^{\xi_k} \to \max_{\xi_k} \qquad (3.4)$$

Здесь p_k - вероятность успеха возможных атак на k – ю компоненту множества прикладных ИТ. Значение вероятностей $p_1, p_2, \ldots, p_n$ могут быть определены путем опроса соответствующих экспертов или путём обработки статистических данных. Как было показано в главе 2 величина P вследствие формулы (3.4) имеет смысл вероятности вывода из строя системы прикладных ИТ вида (1.25). Решение задачи нелинейного булевского программирования (3.4)–(3.1),(3.2) позволяет найти такое подмножество компонент ИТ, вывод которых из строя с максимальной вероятностью не позволяет успешно выполнить все прикладные ИТ рассматриваемой системы. Преобразуем путем логарифмирования критерий (3.4) к линейному виду:

$$\ln P = \sum_{k=1}^{n} \xi_k \ln p_k \ .$$

Вводя обозначения:

$$P^* = \ln P, \quad p_k^* = \ln p_k \qquad (3.5)$$

получим линейную целевую функцию вида:

$$P^* = \sum_{k=1}^{n} p_k^* \xi_k \to \max_{\xi_k} \qquad (3.6)$$

Решение задачи (3.3)–(3.1),(3.2) и (3.6)–(3.1),(3.2) возможно с использованием процедуры симплекс метода [68] с предварительной заменой ограничений (3.1) на неравенства вида:

$$0 \le \xi_k \le 1, \quad k \in (\overline{1,n}) \qquad (3.7)$$

Для более глубокого анализа критических «компонент» и в последующем требуемых экономических средств на обеспечение ИБ предлагается решать известными методами [62] двухкритериальную задачу линейного про-

граммирования вида (3.3),(3.6)–(3.2),(3.7). Полученное множество оптимальных по Парето минимальных покрытий анализируется администратором (проектировщиком) системы ИБ для выбора действительно «критических» компонент АСОИУ нуждающихся в более высоком уровне обеспечения ИБ. С помощью моделей, аналогичных модели (3.3),(3.6)–(3.2),(3.7) можно выявлять «критические» компоненты в составе анализируемой АСОИУ. В частности, используя ориентированные графы, которые описывают отношения Q_3, Q_4, Q_5, Q_6 и Q_7, определяемые выражениями (1.9),(1.11)–(1.14) «критические» компоненты могут быть выделены в следующих составных частях АСОИУ: структура взаимодействия аппаратных средств, структура системных и прикладных программ, распределенный блок данных, структура взаимодействия пользовательских АСОИУ, организационной структуры рассматриваемой организации.

3.2. Оптимальный выбор средств информационной безопасности системы.

Рассмотрим отношение W_1, определяемое выражением (1.26) в его матричном представлении с элементами:

$$w_{ij}^{(1)} = \begin{cases} 1, & \textit{если от } i-\textit{ой угрозы ИТ} - \textit{продукты системы защищает} \\ & j-\textit{ео средство}; \\ 0, & \textit{в противном случае.} \end{cases}$$

Пронумеруем элементы множества угроз и располагаемых СИБ концептуальной модели системы ИБ (1.25) как $U = \{1,2,3,\ldots,i,\ldots,n\}$, $M = \{1,2,3,\ldots,j,\ldots,m\}$. Введём в рассмотрение булевские переменные:

$$x_j \in \{0;1\}, \quad j = \overline{(1,m)} \tag{3.8}$$

такие, что

$$x_j = \begin{cases} 1, & \textit{если для защиты системы выбрано } j-\textit{ое средство}; \\ 0, & \textit{в противном случае.} \end{cases}$$

Потребуем, чтобы каждая угроза системы была бы парирована не менее чем одним СИБ. Это требование представим условием вида:

$$\sum_{j=1}^{m} w_{ij}^{(1)} x_j \geq 1, \quad i = \overline{(1,n)} \tag{3.9}$$

Стоимость СИБ используемых в АСОИУ определяется выражением вида:

$$C = \sum_{j=1}^{m} c_j x_j \to \min_{x_j} \tag{3.10}$$

где c_j - стоимость j- го СИБ. Обозначим через p_j - вероятность того, что противник сможет преодолеть j-е СИБ. Количественные значения вероятностей $p_1, p_2, \ldots, p_m$ могут быть определены путём специальных испытаний множества средств M на стойкость от воздействия множества угроз U. Естественно предположить, что выполняется условие, что чем больше величина стоимости c_j, тем меньше вероятность p_j, $j = \overline{(1,m)}$. Будем считать, что противник одновременно атакует все СИБ имеющиеся в составе АСОИУ. В этом случае стойкость системы ИБ может быть оценена как вероятность ее преодоления (взлома) противником. Эту вероятность можно представить как

$$\Theta = \prod_{j=1}^{m} p_j^{x_j} \to \min_{x_j} \tag{3.11}$$

Следует отметить, что если все $x_j \equiv 0$, $j = \overline{(1,m)}$, то есть СИБ в АСОИУ отсутствуют, то величина $\Theta = 1$. Таким образом, выбор оптимальных СИБ АСОИУ можно осуществить путём решения двухкритериальной задачи нелинейного булевского программирования (3.11),(3.10),(3.8),(3.9). При этом критерий (3.11) можно преобразовать к линейной форме путём его логарифмирования, как это было сделано в предыдущем разделе. Получаемое в результате паретооптимальное множество вариантов СИБ предъявляется администратору или проектировщику системы для выбора из него компромиссного решения с учётом его стойкости к нарушению ИБ и стоимости.

3.3. Теоретико-игровая модель размещения конфиденциальной информации на серверах системы.

Современные АСОИУ имеют, как правило, трехзвенную (или многозвенную) архитектуру типа «клиент-сервер» [69]. В них предусматриваются серверы приложений, серверы баз данных и рабочие места пользователей систем (клиенты), объединенные локальной или корпоративной вычислительной сетью.

Одним из важных аспектов реализации подобных систем является обеспечение безопасности хранения и передачи *конфиденциальных данных* (КД) [70]. В настоящее время существует ряд способов обеспечения безопасного размещения информации на серверах таких, как применение паролей условно-постоянного действия, шифрование информации на устройствах хранения, трансляция адресов и т.п. Желательно, чтобы средства обеспечения безопасности подобного рода обладали двумя свойствами: возможность изменения атрибутов доступа к информации либо по местоположению, либо по времени, что существенно осложняет задачу нарушения ее безопасности; обеспечение «прозрачности» местоположения данных относительно приложений пользователя [69]. Данные свойства, как известно, могут обеспечиваться указанными выше системными программными средствами. Другим перспективным средством обеспечения конфиденциальности и целостности данных является их маскировка. В работе [71] в качестве средств маскировки предлагается использовать криптографические методы обеспечения ИБ для шифрования данных. В более широком смысле под маскировкой будем понимать создание для нарушителя «ложных» целей как объектов для его атак. В качестве таких целей могут выступать файлы со случайными, но близкими к реальным данными, либо «пустые» файлы. Для решения задачи размещения КД на серверах АСОИУ целесообразно использовать теоретико-игровые модели [72,100,101,106], где одним из игроков выступает администратор системы ИБ АСОИУ (обозначим его как игрок А), а другим потенциальный

противник (обозначим - игрок В).

Рассмотрим ситуацию с точки зрения администратора системы ИБ АСОИУ. В распоряжении игрока A находится n стратегий $A_1, A_2, ..., A_n$, где A_i - стратегия игрока A, состоящая в том, что КД нужно расположить на i-м сервере. В распоряжении нарушителя также находится n- стратегий $B_1, B_2, ..., B_n$, где B_j - стратегия игрока B, состоящая в том, что КД нужно искать на j-м сервере. Построим платежную матрицу Γ для игрока A:

$$\Gamma = [\gamma_{ij}] = \begin{bmatrix} P + c_1 & c_1 & \dots & c_1 \\ c_2 & P + c_2 & \dots & c_2 \\ \dots & \dots & \dots & \dots \\ c_n & c_n & \dots & P + c_n \end{bmatrix}, \qquad (3.12)$$

где γ_{ij} - потери игрока A, если атаке подвергается j-й сервер, а КД находятся на i-м сервере (то есть игрок A выбрал стратегию A_i). Здесь $P > 0$ это материальный (в финансовом смысле) ущерб, наносимый системе при нарушении конфиденциальности ее данных, а c_i - стоимость хранения КД на i-м сервере. Обозначим через $p = (p_1, p_2, ..., p_n)$ смешанную стратегию игрока A [73,74], в которой стратегии $A_1, A_2, ..., A_n$ принимаются с вероятностями $p_1, p_2, ..., p_n$. При этом $p_i \geq 0$, $i = \overline{1,n}$, $p_1 + p_2 + ... + p_n = 1$. Обозначим множество смешанных стратегий игрока А через S_A. Как известно, любая чистая стратегия A_i, $i = \overline{1,n}$, принадлежит множеству смешанных стратегий S_A. Смешанные стратегии, которыми руководствуется администратор СИБ, определяют механизм размещения КД на серверах АСОИУ. При использовании этих стратегий КД будут случайно размещаться на одном из серверов АСОИУ, а на других серверах в это время будут присутствовать «ложные» файлы. В таком случае пользователь, запрашивающий данные, будет знать адрес только соответствующего сервера приложений, а точное их местоположение в текущий момент будет определяться системными программными

средствами данного сервера с одновременным обеспечением свойства прозрачности доступа. Следуя принципу гарантированного результата, определим в качестве наилучшего поведения для игрока A применение гарантирующей смешанной стратегии [75]. Гарантирующая смешанная стратегия игрока A находится как решение следующей задачи линейного программирования [76,77]:

$$v \to \min \tag{3.13}$$

при выполнении условий

$$\sum_{i=1}^{n} p_i \gamma_{ij} - v \le 0, \quad j = \overline{1,n}, \tag{3.14}$$

$$\sum_{i=1}^{n} p_i = 1, \; p_i \ge 0, \quad i = \overline{1,n}, \tag{3.15}$$

В работе [78] предлагается рассматривать дополнительные критерии оптимальности искомых стратегий. Будем считать заданными величины k_i - какие-либо затраты на реализацию i-той стратегии. Например, величина k_i - может характеризовать стоимость c_i или время t_i необходимое для реализации i-той стратегии. Тогда математическое ожидание затрат на реализацию выбранных стратегий определяется следующим образом[67]:

$$K = \sum_{i=1}^{n} k_i p_i .$$

Например, если вместо k_i подразумевать стоимость выполнения стратегии c_i, то это выражение будет иметь смысл средней стоимости реализации использования смешанных стратегий. В рассматриваемой задаче в качестве дополнительного критерия будем использовать именно среднюю стоимость C размещения КД на серверах системы:

$$C = \sum_{i=1}^{n} c_i p_i \to \min . \tag{3.16}$$

Отметим, что предложенные в работе [72] теоретико-игровые модели

не учитывают дополнительные критерии оптимальности искомых стратегий. Построим множество оптимальных по Парето решений [62] с использованием линейной свертки критериев (3.13),(3.16) вида:

$$L(\alpha, p_1,..,p_i,..,p_n,v) = \alpha v + (1-\alpha)\sum_{i=1}^{n} c_i p_i \to \min . \qquad (3.17)$$

Варьируя параметр свертки $\alpha \in [0;1]$ в указанном интервале, получим множество решений $\{(p_1, p_2,...,p_n)\}$, оптимальных по Парето. Это множество предоставляется игроку A, который, исходя из сопоставления значений v и C, выбирает конкретный вариант значений $p_1^0, p_2^0,...,p_n^0$.

Рассмотрим вопрос реализации случайного механизма размещения КД. Пусть p_i^0, $i = \overline{1,n}$, полученные из выбранного администратором варианта вероятности размещения КД на серверах сети. Построим с их использованием интервалы $[0, p_1^0)$, $[p_1^0, p_1^0 + p_2^0),\ldots,[\sum_{i=1}^{k-1} p_i^0, \sum_{i=1}^{k} p_i^0),\ldots,[\sum_{i=1}^{n-1} p_i^0, 1)$ [6]. В начале каждого рабочего дня или в течение каждого часа будем генерировать равномерно распределённое число $\xi \in [0,1]$. Если это число попадает в некоторый k-й интервал, где $k = \overline{1,n}$, то в этот день или час КД располагаются на k-м сервере.

3.4. Примеры обеспечения информационной безопасности АСОИУ.

Пример выявления «критических» аппаратных средств АСОИУ. Рассмотрим портал Академии наук Республики Татарстан [95], включающий в себя множество объектов, описанное выражением (1.23): a_1 - главный сервер сети , a_2 - главный маршрутизатор, a_3- коммутатор 3-го этажа, a_4 - коммутатор 2-го этажа, a_5- контроллер домена группы поддержки интернет служб, a_6- сетевой принтер 1, a_7- сетевой принтер 2, a_8- сканер, a_9- АРМ администратора, a_{10}- АРМ вебмастера, a_{11}- АРМ пользователя, a_{12}- АРМ *book*, a_{13}- АРМ *summer*. Структура портала представлена на рис. 3.3.

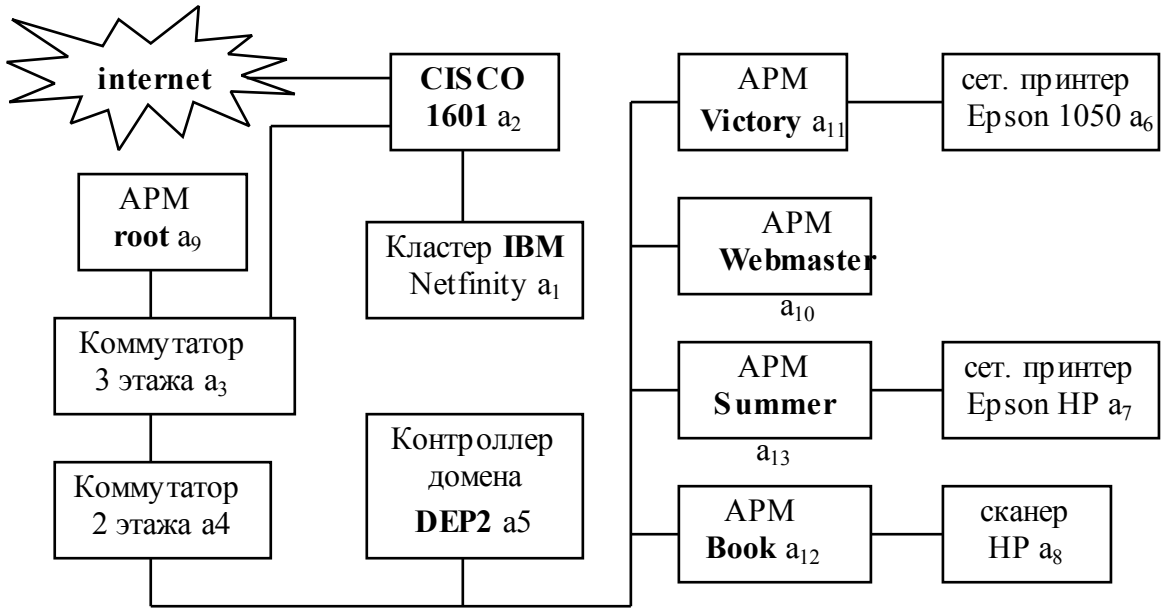

Рис. 3.3.

Рассмотрим следующие пути передачи информации в системе, составляющие множество L: $l_1=\{a_9, a_3, a_2, a_1\}$, $l_2=\{a_{11}, a_5, a_4, a_3, a_2, a_1\}$, $l_3=\{a_{10}, a_5, a_4, a_3, a_2, a_1\}$, $l_4=\{a_9, a_3, a_4, a_5, a_{13}, a_7\}$, $l_5=\{a_9, a_3, a_4, a_5, a_{12}, a_8\}$, $l_6=\{a_{11}, a_5, a_4, a_3, a_2\}$, $l_7=\{a_{10}, a_5, a_4, a_3, a_2\}$. Построим матрицу B, которая имеет вид:

$$B=\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Зададимся вероятностями нарушения безопасности каждого элемента: p_1= 0,9; p_2= 0,8; p_3= 0,7; p_4= 0,5; p_5= 0,4; p_6= 0,25; p_7= 0,25; p_8= 0,55; p_9= 0,7; p_{10}= 0,65; p_{11}= 0,6; p_{12}= 0,65; p_{13}= 0,55. Решая задачу линейного булевского программирования (3.4)–(3.1),(3.2) [96,97], находим решение вида: ξ^o=(0,0,1,0,0,0,0,0,0,0,0,0,0). Отсюда следует, что наиболее «критичным» устройством, влияющим на безопасность системы в целом, является коммутатор 3-го этажа.

Пример оптимального выбора средств информационной безопасности АСОИУ. Пусть множество угроз, входящих в концептуальную модель системы ИБ (1.25), имеет вид: $U = \{u_1, u_2, u_3\}$, где u_1–сканер портов, u_2– вирусная атака, u_3–подслушивающее устройство. Проектировщик системы ИБ располагает множеством СИБ $M = \{m_1, m_2, m_3, m_4\}$, где m_1–система локализации подслушивающих устройств, m_2– система обнаружения вторжений, m_3–МЭ, m_4– антивирус. Отметим, что множество угроз и СИБ входит в модель (1.25). Элементы этого множества описываются следующими условными характеристиками: $c_1 = 5$, $c_2 = 10$, $c_3 = 1$, $c_4 = 6$, $p_1 = 0{,}3$, $p_2 = 0{,}1$, $p_3 = 0{,}8$, $p_4 = 0{,}2$. Отношение (1.26) W_1 представим матрицей вида:

$$W_1 = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \end{array} \begin{array}{c} \begin{array}{cccc} m_1 & m_2 & m_3 & m_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Ограничения (3.8) конкретизируются как

$$x_1 \in \{0;1\};\ x_2 \in \{0;1\};\ x_3 \in \{0;1\};\ x_4 \in \{0;1\} \tag{3.18}$$

Система условий (3.9) примет в данном случае вид

$$\begin{aligned} & x_2 + x_3 + x_4 \geq 1 \\ & x_2 + x_4 \geq 1 \\ & x_1 \geq 1 \end{aligned} \tag{3.19}$$

Критерии оптимальности задачи записываются как

$$\begin{aligned} & C = 5x_1 + 10x_2 + 1x_3 + 6x_4 \to \min_{x_j} \\ & \Theta = 0{,}3^{x_1} \cdot 0{,}1^{x_2} \cdot 0{,}8^{x_3} \cdot 0{,}2^{x_4} \to \min_{x_j} \end{aligned} \tag{3.20}$$

Множество допустимых решений задачи, определяемое условиями (3.18) и (3.19) включает в себя две точки с координатами: 1) $x_1 = 1;\ x_2 = 1;\ x_3 = x_4 = 0$; 2) $x_1 = 1;\ x_2 = x_3 = 0;\ x_4 = 1$. Значения целевых функций (3.20) в этих точках соответственно будут равны:

$C_1 = 15,\ \ \Theta_1 = 0{,}03;\ \ C_2 = 11,\ \ \Theta_2 = 0{,}06.$ Построим эти точки на графике в пространстве критериев (см. рис. 3.4).

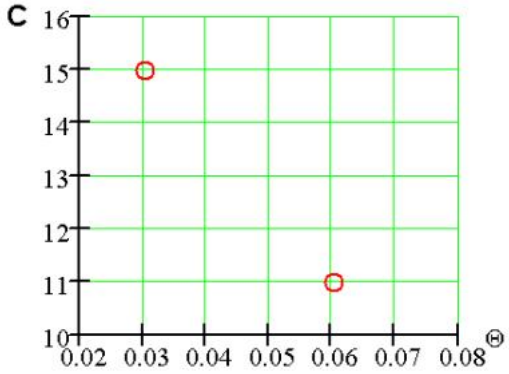

Рис. 3.4.

Таким образом, имеется два варианта применения имеющихся СИБ: а) система локализации подслушивающих устройств, система обнаружения вторжений б) система локализации подслушивающих устройств, антивирус. Матрица W_1 показывает, что выбранные СИБ полностью перекрывают все виды угроз. Администратор или проектировщик системы ИБ выбирает конкретный вариант, исходя из располагаемых финансовых возможностей и допустимого значения уровня ИБ.

Оптимальное размещение конфиденциальной информации на серверах АСОИУ. Рассмотрим АСОИУ банка, в которой в группу серверов для хранения КД включено четыре сервера, стоимость которых $c_s^1 = 1350$ тыс.руб., $c_s^2 = 1170$ тыс.руб., $c_s^3 = 900$ тыс.руб. и $c_s^4 = 1500$ тыс.руб.

По оценкам специалистов на поддержание работоспособности сервера требуется в год от 20% до 100% от стоимости его аппаратной и программной составляющих, в зависимости от уровня конфиденциальности хранимых на них данных. Учитывая вышесказанное, зададимся значениями стоимостей обеспечения КД c_i при хранении на серверах АСОИУ, за которые примем 20% стоимости самих серверов c_s^i, где i – номер сервера. Таким образом, $c_1 = 270$ тыс.руб., $c_2 = 234$ тыс.руб., $c_3 = 180$ тыс.руб. и $c_4 = 300$ тыс.руб. Бу-

дем считать, что потери игрока A при раскрытии КД составляют величину $P = 3000$ тыс. руб. С учетом используемых исходных данных матрица игры (3.12) примет вид:

$$\Gamma = \begin{bmatrix} 3270 & 270 & 270 & 270 \\ 234 & 3234 & 234 & 234 \\ 180 & 180 & 3180 & 180 \\ 300 & 300 & 300 & 3300 \end{bmatrix}.$$

Средняя стоимость использования рассматриваемых серверов (3.16) конкретизируется как: $C = 270p_1 + 234p_2 + 180p_3 + 300p_4$. Ограничения (3.14),(3.15) принимают вид:

$$\begin{array}{l} 3270p_1 + 270p_2 + 270p_3 + 270p_4 - v \le 0 \\ 234p_1 + 3234p_2 + 234p_3 + 234p_4 - v \le 0 \\ 180p_1 + 180p_2 + 3180p_3 + 180p_4 - v \le 0 \\ 300p_1 + 300p_2 + 300p_3 + 3300p_4 - v \le 0 \end{array}, \qquad (3.21)$$

$$p_i \ge 0, \quad i = \overline{1,4}, \; p_1 + p_2 + p_3 + p_4 = 1. \qquad (3.22)$$

Линейная свертка критериев L вида (3.17) записывается как:

$$\begin{array}{l} L(\alpha, p_1, p_2, p_3, p_4, v) = \\ = \alpha v + (1-\alpha)(270p_1 + 234p_2 + 180p_3 + 300p_4) \to \min \end{array}. \qquad (3.23)$$

Решая задачу линейного программирования (3.23),(3.21),(3.22) при различных значениях α, получим результаты, которые представлены в таблице 3.1.

Табл. 3.1.

№, варианта / α / результат	№1	№2	№3	№4
	0-0.01	0.02-0.04	0.05-0.06	0.07-1
p_1	0	0	0.3193	0.242
p_2	0	0.491	0.3313	0.254
p_3	1	0.509	0.3493	0.272
p_4	0	0	0	0.232
v	3180	1707	1228	996
C	180	206.5	226.6	243.3

Таким образом, мы получили четыре компромиссных решения, которые предоставляются администратору СИБ для выбора варианта размещения КД. Будем считать, что администратор СИБ АСОИУ выбрал вариант №3 и построил отмеченные выше интервалы для этого случая: $[0;0.3193)$, $[0.3193;0.6506)$, $[0.6506;1)$, $[1;1)$. Пусть сгенерировано случайное число $\xi = 0{,}35$. Это число попадает во второй интервал, следовательно, КД нужно разместить на втором сервере. Если в следующий раз будет сгенерировано равномерно распределённое число $\xi = 0.1$, то КД нужно будет разместить на первом сервере.

Рассмотрим один из вариантов реализации механизма случайного размещения информации при использовании в АСОИУ серверов баз данных класса MS SQL Server. Если случайному размещению подлежат отдельные информационные объекты, для их перемещения могут быть использованы следующие подходы:

1) Использование хранимых процедур с распределенными запросами. Механизм распределенных запросов MS SQL Server позволяет обращаться в пределах одного запроса к другим серверам MS SQL Server. Таким образом, для реализации рассматриваемого подхода требуется создать SQL-процедуру, которая производит копирование данных с внешнего сервера на текущий и удаление данных на внешнем сервере.

2) Использование средств встроенного в MS SQL Server механизма преобразования данных DTS (Data Transformation Services - служба преобразования данных). Данные средства позволяют осуществлять копирование/перемещение данных как между серверами MS SQL Server, так и с внешними механизмами хранения с помощью технологии универсального доступа OLE DB. Среда MS SQL Server предоставляет возможности автоматического запуска как хранимых процедур, так и пакетов DTS по расписанию с помощью службы SQL Agent.

Оба представленных варианта предполагают хранение информации о текущем местоположении КД на одном из серверов группы. Данная информация модифицируется соответствующим образом в ходе выполнения каждой операции перемещения. Таким образом, можно обеспечить ежедневный (ежечасный) запуск процедуры случайного выбора сервера и перемещения КД по серверам АСОИУ в соответствии с методикой описанной выше.

Выводы по главе 3.

1. Разработана математическая модель выделения критических элементов АСОИУ с использованием граф прикладной информационной технологии системы, вероятностей преодоления их противником и заданным отношении взаимосвязи угроз и СИБ.

2. Приведено решение задачи оптимального выбора СИБ АСОИУ из заданного множества с учетом стоимости выбранных СИБ и вероятности преодоления противником хотя бы одного из них.

3. Решена двухкритериальная задача размещения КД в серверной части АСОИУ на основе теоретико-игровой модели «администратор системы ИБ – противник». Предложен метод, реализующий случайный механизм размещения КД в серверной части системы.

4. Приведен ряд примеров, иллюстрирующих предложенные выше методы и модели обеспечения ИБ АСОИУ, которые показали, что с их помощью можно повысить уровень ИБ АСОИУ.

Глава 4. Автоматизация испытаний средств информационной безопасности АСОИУ.

Рассмотренные в предыдущих главах задачи анализа и синтеза СИБ требуют экспериментальной оценки степени ИБ используемых и выбираемых средств и методов обеспечения ИБ. Отметим, что в главе 2 описаны способы формирования требований по ИБ к элементам АСОИУ и системе в целом. Поэтому возникает необходимость проверить, на сколько эти требования могут быть обеспечены выбранными СИБ элементов АСОИУ. В доступной литературе [4-7,43,44] говорится о необходимости испытаний СИБ, но не указываются пути реализации этого важного этапа в создании и эксплуатации АСОИУ. В работе [42] говорится о необходимости получения информации о ИБ АСОИУ из протоколов испытаний фирм ее производителей, но не описаны соответствующие подходы и методики, позволяющие сделать это.

4.1. Цели и задачи автоматизированных испытаний средств информационной безопасности.

Приведем ряд определений, которые в последующем будут использованы при разработке структуры и функций АСИ СИБ. В нашем случае объектом испытания (ОИ) являются СИБ некоторого информационного ресурса АСОИУ, которые подвергаются испытаниям на ИБ. Следуя работе [87], под автоматизированной системой испытаний (АСИ) будем понимать человеко-машинный организационно-технический комплекс, предназначенный для обеспечения максимально возможного в данных условиях уровня автоматизации испытательных работ по оценке ИБ.

Рассмотрим цели и задачи, которые необходимо решить при автоматизации процесса испытания СИБ. Выделим две цели, которые должны быть достигнуты при решении задач АСИ СИБ: 1) Уменьшение трудоемкости проведения испытаний СИБ АСОИУ; 2) Повышение достоверности оценки ИБ АСОИУ.

Достижение этих целей, как и в любых других областях техники возможно только путем автоматизации этих процессов в частности применение специальных автоматизированных систем испытаний (АСИ) [87].

Отметим, что для достижения сформулированных целей необходимо решить ряд задач, в состав которых входят:

1) сокращение времени проведения испытаний, которого можно добиться с использованием применения специального программного обеспечения производящего выбор методов и средств испытания СИБ АСИ, обрабатывающего результаты работы АСИ и формирующего все необходимые отчеты для принятия решения о достижении целей испытаний;

2) сокращение времени проведения испытаний за счет применение быстродействующих серверов и каналов связи, а так же рабочих станций для обработки результатов испытаний.

Как уже говорилось выше цель любого испытания – получение достоверных результатов. Достижение этой цели возможно при использовании: 1) аппарата теории вероятностей и математической статистики, а именно ее раздела обработки результатов испытаний [67]; 2) количественных оценок, которые будут выступать в качестве критерия достоверности испытаний. В качестве такого количественного критерия может выступать оценка вероятности нарушения ИБ ОИ.

Отметим, что количественная оценка достоверности проведения испытаний, позволяет судить о достижении целей испытания, при условии, что заданы или рассчитаны допустимые значения вероятностей нарушения ИБ ОИ методы определения, которых представлены в главе 2. Использование подхода учитывающего количественные оценки позволяет конкретизировать и упростить методику принятия решения о соответствии ОИ требованиям, предъявляемым к нему с точки зрения ИБ. Стоит отметить, что достоверность испытаний будет тем выше, чем больше количество опытов проведено в его ходе, с целью проверки ИБ рассматриваемо СИБ [67].

4.2. Структура и функции автоматизированной системы испытаний средств информационной безопасности.

Следуя работе [87], в составе АСИ СИБ можно выделить следующие основные компоненты:

Техническое обеспечение – комплекс технических средств, обеспечивающих функционирование системы и выполнение возложенных на нее функций.

Математическое обеспечение – совокупность математических моделей и методов, лежащих в основе логических и вычислительных процессов, сопровождающих выполнение испытательных работ.

Программное обеспечение (ПО) – совокупность программ, обеспечивающих целевое использование АСИ СИБ. Программное обеспечение состоит из общего (ОПО) и специального (СПО). ОПО предназначено для разработки, отладки и организации функционирования СПО АСИ СИБ. Оно состоит из операционной системы, системы программирования, обрабатывающих программ, технологических комплексов и инструментальных систем. СПО это совокупность программ, которые реализуют алгоритмы АСИ СИБ. Оно состоит из двух взаимосвязанных программных комплексов: системы настройки и системы управления испытанием.

Информационное обеспечение (ИО) – совокупность данных испытаний вместе с программно аппаратными средствами их управления.

Лингвистическое обеспечение (ЛО) – совокупность действующих формальных языков описания информации и алгоритмов ее обработки в процессе автоматизированных испытаний.

Важной компонентой АСИ СИБ является персонал системы, который включает в себя администратора системы и испытателей СИБ. Структурная схема АСИ СИБ представлена на рис. 4.1.

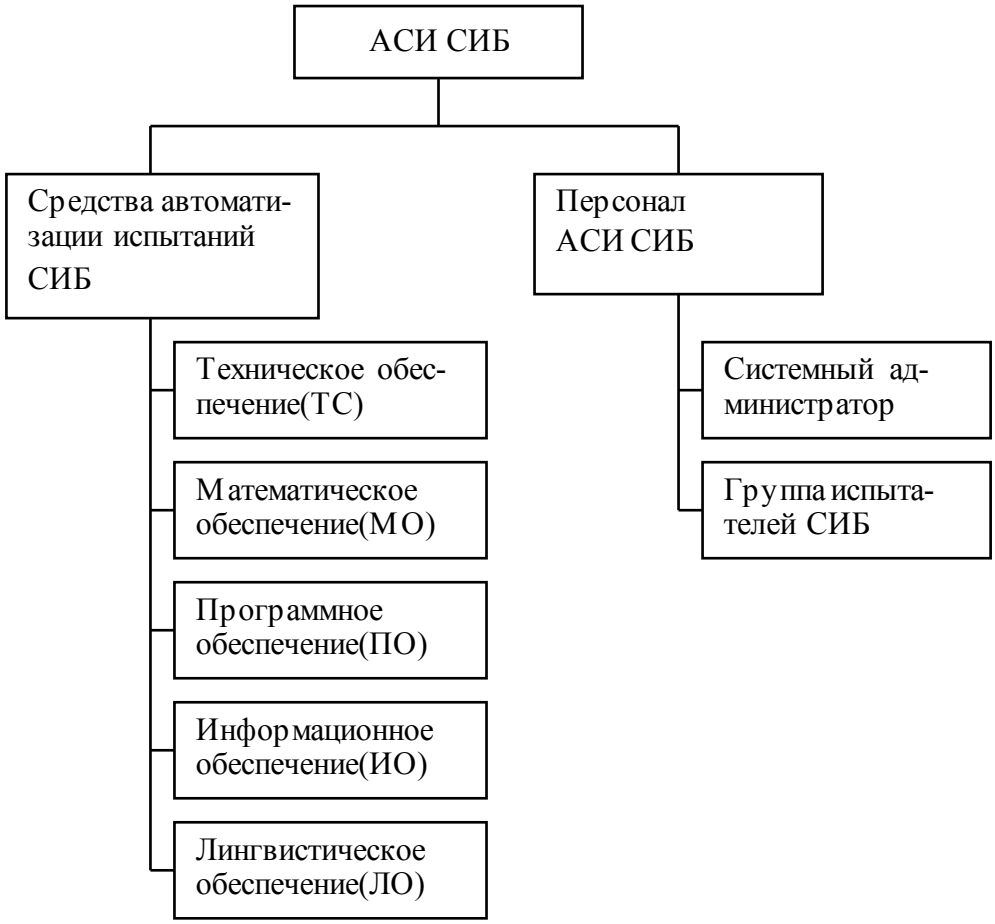

Рис. 4.1. Структурная схема АСИ СИБ.

Опишем компоненты АСИ СИБ, представленные на рис. 4.1.

Техническое обеспечение системы АСИ СИБ включает в себя компьютерные стенды, в составе которых используются технические средства формирования и реализации средств нападения на ОИ, а так же обработки результатов испытаний. Структура технических средств представлена на рис. 4.2.

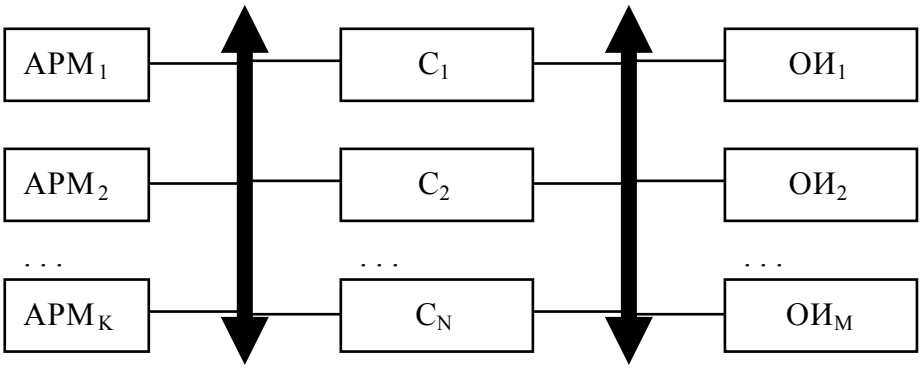

Рис. 4.2. Структура технических средств АСИ СИБ.

На этом рисунке приняты следующие условные обозначения:

1) APM_1, $APM_2,\ldots,APM_k$ …, APM_K – автоматизированные рабочие места K испытателей СИБ.

2) C_1, $C_2,\ldots,C_n$ …,C_N - сервера АСИ СИБ.

3) $ОИ_1$, $ОИ_2,\ldots,ОИ_m$ …, $ОИ_M$ – объекты испытаний. Отметим, что в общем случае каждый АРМ может взаимодействовать с любым сервером ТС АСИ СИБ.

Математическое обеспечение АСИ СИБ включает в себя математические методы и алгоритмы обработки результатов испытаний СИБ. Рассмотрим один из вариантов таких методов и алгоритмов. Будем считать, что АСИ СИБ работает по схеме независимых испытаний [67]. Пусть событие A - это факт выявления уязвимости тестируемого СИБ при реализации некоторого *модуля формирования атак* (МФА).

Пусть n - это количество МФА реализованных в составе АСИ СИБ для испытания ИБ i - го СИБ рассматриваемой АСОИУ. Допустим в n опытах событие A произошло m раз не трудно заметить, что число появлений события A распределено по биномиальному закону [67] и вероятность того, что событие A появится ровно m раз в серии из n опытов имеет вид:

$$P_{m,n} = C_n^m p^m q^{n-m}, \qquad (4.1)$$

где p - вероятность реализации события A, а $q = 1 - p$.

После испытания на ИБ i-го СИБ АСОИУ можно вычислить частоту появления события A, которая равна $p^* = \frac{m}{n}$. Так как вероятности появления события A является величиной не известной и нам известна только ее оценка $p^* = \frac{m}{n}$, построим доверительный интервал $I_\beta = (p_1, p_2)$, в который частота события A p^* попадает с доверительной вероятностью β. Для этого нужно решить систему уравнений [67]:

$$\sum_{m=k}^{n} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \tag{4.2}$$

$$\sum_{m=0}^{k} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \tag{4.3}$$

где $\alpha = 1-\beta$ и $k = np^*$ – число появлений события A. Решая уравнения (4.2) и (4.3) относительно p, можно найти границы доверительного интервала p_1 и p_2. Отметим, что методы нахождения решения уравнений (4.2),(4.3) был подробно описан в работах [67,88–90].

Рассмотрим случай, когда $m = 0$, то есть в n опытах событие A зафиксировано не было. В этом случае [67], p_1=0, а p_2 имеет вид:

$$p_2 = 1 - \sqrt[n]{1-\beta}, \tag{4.4}$$

В работах [67,88] приведены формулы для расчета значений границ доверительного интервала для точечной оценки вероятности p^*. Если число испытаний сравнительно велико $n > 1000$ или $9 < npq < 100$ и $n < 1000$, тогда частота события p^* есть случайная величина, распределение которой близко к нормальному [9,88–90]. Формулы (4.5), позволяют найти, границы доверительного интервала для нее.

$$\begin{aligned} p_1 &= \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} - t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1+\frac{t_\beta^2}{n}}; \\ p_2 &= \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} + t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1+\frac{t_\beta^2}{n}}. \end{aligned} \tag{4.5}$$

Доверительный интервал для вероятности p будет иметь вид:

$$I_\beta = (p_1, p_2). \tag{4.6}$$

Этот интервал будет содержать искомую вероятность p с вероятностью β. Поставим задачу определения минимального значения левой границы доверительного интервала p_2. для заданного значения доверительной вероятности β. То есть, какова точность оценки вероятности p при максимально возможном числе опытов n, чтобы верхняя доверительная граница для вероятности события A была равна заданному значению, при отсутствии успешных реализаций события A. Решение этой задачи имеет вид [67]:

$$p_2 = 1 - \sqrt[n]{1-\beta}, \qquad (4.7)$$

Построим решающие правила для оценки результатов испытаний. Пусть (p_{1i}, p_{2i}) - доверительный интервал для статистической вероятности $p_i^* = \frac{m_i}{n_i}$ нарушения ИБ i-го СИБ АСОИУ, $i = \overline{(1, N)}$. Взаимное расположение расчетного допустимого значения вероятности P_i и доверительного интервала (p_{1i}, p_{2i}) предоставлено на рис. 4.3.

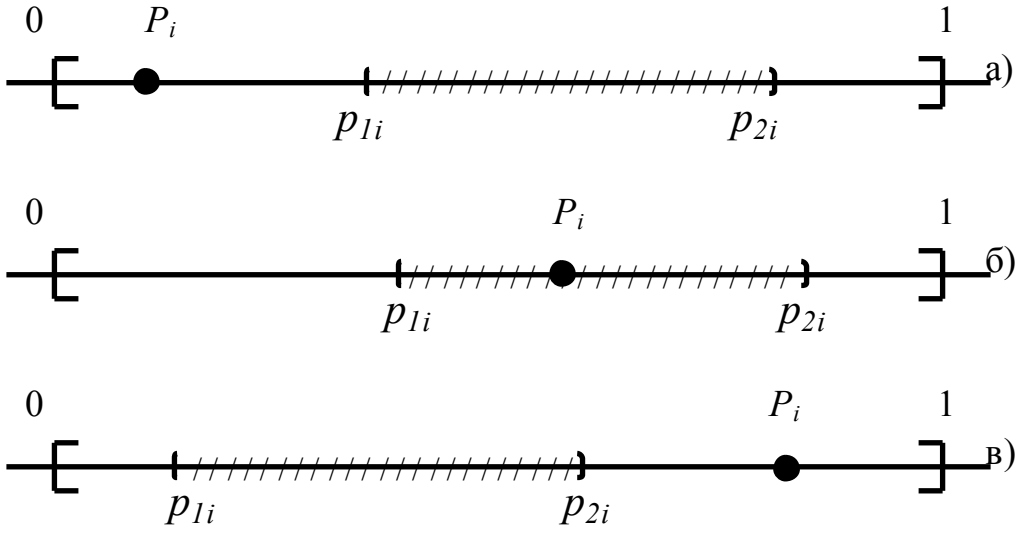

Рис. 4.3.

Случай а) соответствует ситуации, когда значение вероятности нарушения ИБ, которое располагается в интервале (p_{1i}, p_{2i}) больше допустимого значения этой вероятности P_i. Здесь можно сделать вывод о том, что имеющиеся СИБ не выполняют требования по ИБ для итого элемента.

В случае б) однозначного ввода о стойкости, имеющихся СИБ, сделать нельзя, так как значение вероятности нарушения ИБ, которое располагается в интервале (p_{1i}, p_{2i}) может быть, как больше, так и меньше допустимого значения этой вероятности P_i.

Случай в) соответствует ситуации, при которой заданное требование по обеспечению ИБ выполняется. При этом, чем больше P_i отличается от величины p_{2i}, тем выше стойкость СИБ к имеющимся средствам нападения.

Таким образом, имеем следующее решающее правило для оценки тестируемых СИБ *i*-го СИБ АСОИУ:

«Если выполняется одно из неравенств: $P_i < p_{1i}$ или $p_{1i} \le P_i \le p_{2i}$, то требования по ИБ *i*-го СИБ АСОИУ не выполняются. При выполнении условия: $P_i > p_{2i}$ существующие СИБ обеспечивают ИБ *i*-го элемента АСОИУ с доверительной вероятностью равной β.» Построим аналогичные решающие правила (см. рис. 4.4.) для случая отсутствия успешных реализация нарушения ИБ АСОИУ, то есть когда $(p_{1i}, p_{2i}) = (0, p_{2i})$.

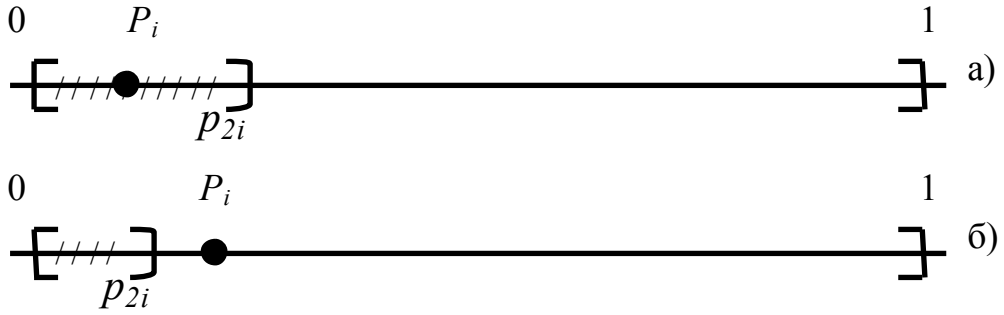

Рис. 4.4.

В случае а) однозначного ввода о стойкости имеющихся СИБ сделать нельзя, так как значение вероятности нарушения ИБ, которое располагается в интервале $(0, p_{2i})$ может быть, и больше, и меньше допустимого значения этой вероятности P_i. Случай б) соответствует ситуации, при которой заданное требование по обеспечению ИБ выполняется. Отметим, что если предложенные решающие правила дали отрицательные или не однозначные выводы

по выполнению требований ИБ, то производится пересмотр состава применяемых СИБ и испытания повторяются до удовлетворения имеющихся требований по ИБ рассматриваемого СИБ АСОИУ.

Рассмотрим математические методы и алгоритмы обработки результатов работы АСИ СИБ. Допустим при испытании некоторого СИБ АСОИУ S, найдено множество U_S уязвимостей. Рассмотрим множество F видов компонент информации обрабатываемой в АСОИУ: конфиденциальность, целостность и доступность. Опишем отношение взаимосвязи множеств F и U_S в виде:

$$R_S \subseteq U_S \times F, \tag{4.8}$$

где $F = \{К, Ц, Д\}$, а К – конфиденциальность, Ц – целостность и Д – доступность информации обрабатываемой в АСОИУ. Отношение (4.8) определяет какая уязвимость тестируемого СИБ АСОИУ влияет на конкретную компоненту информации множества F. Отношение (4.8) представляет собой бинарное отношение и может быть описано булевской матрицей вида:

$$C = [c_{ij}]_{|U(S)| \times |F|}. \tag{4.9}$$

Величины $M_S = |U_S|$ и $|F|$ определяют мощности множеств U_S и F соответственно, и первая из них является переменной, вторая же равна трём, это следует из определения множества F. Матрицу (4.9) заполним, используя результаты работы сканера безопасности Nessus. В его разделах описания содержится информация, определяющая фактор риска (Risk Factor), используя которую испытатель может, выделить из них те, которые влияют на компоненты конфиденциальности, целостности и доступности тестируемого СИБ АСОИУ (см. Приложение 2). Примем следующие условные обозначения: U_S^K - множество уязвимостей влияющих на конфиденциальность тестируемого СИБ АСОИУ, $U_S^Ц$ - множество уязвимостей влияющих на целостность тестируемого СИБ АСОИУ, $U_S^Д$ - множество уязвимостей влияющих

на доступность тестируемого СИБ АСОИУ. Следовательно, теперь с использованием матрицы (4.9) можно определить мощности каждого из множеств U_S^K, $U_S^Ц$, $U_S^Д$:

$$M_S^K = \sum_{i=1}^{M_S} c_{i1}, M_S^Ц = \sum_{i=1}^{M_S} c_{i2}, M_S^Д = \sum_{i=1}^{M_S} c_{i3}. \quad (4.10)$$

Далее определим точечные оценки вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности:

$$p^*_{S|K} = \frac{M_S^K}{n},\ p^*_{S|Ц} = \frac{M_S^Ц}{n},\ p^*_{S|Д} = \frac{M_S^Д}{n}. \quad (4.11)$$

Аналогично, определим точечную оценку вероятности нарушения ИБ тестируемого СИБ АСОИУ:

$$p^*_S = \frac{M_S}{n} \quad (4.12)$$

Далее для каждой из найденных по формулам (4.11),(4.12) вероятностей построим доверительные интервалы с использованием формул (4.2)(4.3) или (4.5) в зависимости от значения параметра npq и количества испытаний n. Определим интегральные характеристики ИБ компонент конфиденциальности, целостности и доступности рассматриваемой АСОИУ и всей системы в целом. Так как нарушение ИБ хоть одного из СИБ АСОИУ ведет к нарушению ИБ АСОИУ, можно сформировать интегральные оценки вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности АСОИУ:

$$p^*_{инт|K} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|K}\right),\ p^*_{инт|Ц} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|Ц}\right),$$
$$p^*_{инт|Д} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|Д}\right) \quad (4.13)$$

где $p^*_{i|K}$, $p^*_{i|Ц}$, $p^*_{i|Д}$ - оценки вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности i - го СИБ АСОИУ. Определим

оценку вероятности нарушения ИБ АСОИУ по аналогии с формулой (4.13) в виде:

$$p^*_{инт|\,АСОИУ\,СН} = 1 - \left(1 - p^*_{инт|К}\right)\left(1 - p^*_{инт|Ц}\right)\left(1 - p^*_{инт|Д}\right). \qquad (4.14)$$

По аналогии с нахождением доверительных интервалов для компонент конфиденциальности, целостности и доступности СИБ АСОИУ, построим для каждой из найденных по формулам (4.13),(4.14) вероятностей доверительные интервалы. Используя методику, описанную выше и сформированные на этапе проектирования АСОИУ требования [91], предъявляемые как к отдельным СИБ так и к тестируемой АСОИУ можно сделать вывод о достаточной либо не достаточной степени ИБ рассматриваемой системы.

Структурная схема **программного обеспечения** АСИ СИБ представлена на рис. 4.5.

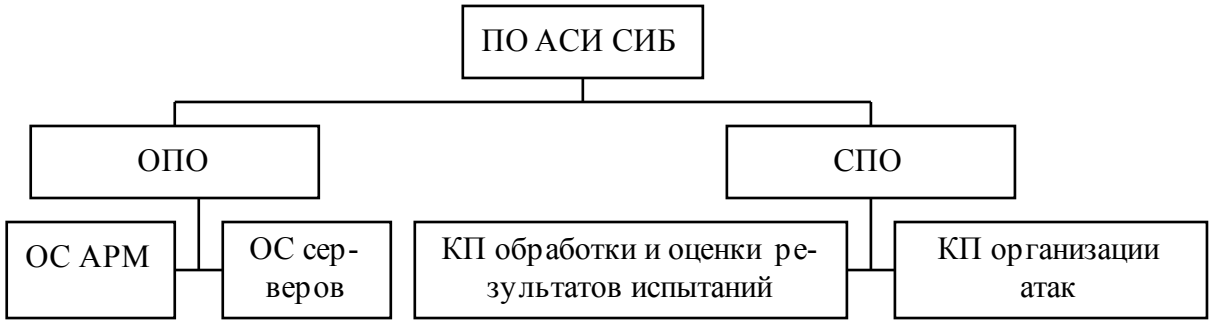

Рис. 4.5.

Рассмотрим компоненты представленные на рис. 4.5. Комплекс программ организации атак служит для ввода служебной информации и входных данных испытания, определения требуемого числа испытаний и выбора по определённому правилу или с помощью случайного механизма из банка существующих средств нападения на тестируемый элемент АСОИУ МФА. Комплекс программ обработки и оценки результатов испытаний реализует следующие функции: фиксация фактов нарушения или не нарушения ИБ для каждой атаки (теста), нахождение доверительного интервала для оценки вероятности нарушения ИБ объект испытания по результатам проведенных испытаний, с использованием формул (4.2),(4.3) или (4.5),(4.6), применение

решающего правила для оценки стойкости тестируемого элемента АСОИУ, формирование и выдача протокола испытаний.

Отметим, что комплекс программ формирования атак можно организовать с использованием современных сканеров уязвимостей их применение требует предварительной инвентаризации [92] сети АСОИУ, т.е. определения: 1) состава и конфигурации сети (рабочих станции, устройств, ОС, стека протоколов); 2) сетевых ресурсов, в первую очередь открытых для совместного пользования; 3) пользователей и групп; 4) приложений и идентификационных маркеров; 5) общих параметров политик безопасности и т.д.

На этом этапе проводится анализ уязвимости сети с целью фиксации обновлений и настроек ОС и приложений ОИ. Современные сканеры уязвимостей [92] анализируют рабочие станции, сервера, межсетевые экраны, сетевое оборудование, сервисы и приложения, составляют список уязвимостей, классифицируя их по степени опасности, и предлагают рекомендации по устранению уязвимостей. Это позволяет их эффективно использовать при идентификации и последующем контроле ОИ, анализе угроз администрирования, конфигурирования и политики безопасности. В настоящее время достаточно много сканеров уязвимостей. Выделим ряд критериев для выбора таких средств: количество реально обнаруживаемых ими уязвимостей (в том числе в сервисах, установленных на нестандартных портах), количество ложных срабатываний, удобство пользования сканером. Для выявления актуальных угроз очень важным является поддержка регулярных обновлений баз уязвимостей и интеграция по ним с IDS-продуктами. Из общеизвестных сканеров можно выделить следующие продукты:

Сетевой сканер Nessus [93,94] – единственный сканер, сертифицированная версия которого распространяется Гостехкомиссией РФ бесплатно. Серверная часть сканера работает в среде Unix. Nessus предоставляет широкие возможности по поиску уязвимостей сетей и исследованию структуры

сетевых сервисов, постоянно обновляется и является одним из самых эффективных сетевых сканеров.

Семейство сканеров ISS (Internet Scanner, System Scanner) как полнофункциональные системы анализа ИБ, поддерживающие базу уязвимостей XForce, современные технологии сканирования, технологию клиент-сервер и так далее [40]. Одна из версий Internet Scanner имела сертификат Гостехкомиссии РФ. К ее недостаткам относят высокую стоимость и медленность сканирования.

Отметим отечественный сетевой сканер - XSpider (Positive Tech.), к сожалению, не сертифицированном. В печати отмечается его эффективность, однако при лаконичности отчетной информации.

В качестве системных сканеров следует выделить средства, поставляемые разработчиками операционных сред, а именно: MSBA для Windows 2000/XP, ASET для Solaris. Сканеры проверяют типовые уязвимости, правильность конфигурации, контролируют целостность файлов, своевременность установки сервисных пакетов операционных сред.

В системах, основанных на промышленных базах данных, могут быть использованы сканеры уязвимости СУБД, например Database Scanner (ISS). Для сокращения трудоемкости разработки АСИ СИБ предлагается использовать существующее программное обеспечение. В частности для компоненты ОПО можно использовать любую UNIX подобную ОС с набором всевозможных утилит и программ для разработки, доработки и настройки программных компоненты СПО, а для компоненты СПО может быть применен упомянутый выше сканер безопасности Nessus [93,94,107]. На сегодняшний день Nessus является одним из самых мощных сетевых сканеров безопасности. Ниже приведены его основные возможности и характеристики:

1) Модульная архитектура, в которой каждый отдельный МФА выполнен в виде подключаемого модуля. Таким образом, возможно, добавить свой собственный МФА, не меняя кода самого сканнера.

2) Клиент серверная архитектура позволяющая организовать работу системы в среде КТС представленную на рис. 4.2.

3) Гибкость, которая определяется возможностью испытывать одновременно неограниченное количество объектов. Nessus позволят работать с различными портами в том числе и не стандартными. То есть, если какой-либо сетевой сервис использует не заданный по умолчанию порт, то Nessus определит это, и выполнит испытания корректно.

4) Адаптивность проводимых тестов. Все тесты, проводимые Nessus координируются между собой, это позволяет ускорить процесс испытания за счет исключения тестов, которые приведут к заведомо отрицательному результату с точки зрения возможных уязвимостей в ИБ. Например, если сервер не принимает анонимную авторизацию, тогда не будут проводиться все тесты, связанные с проверкой работы сервера в режиме анонимного доступа.

5) Многорежимность функционирования включает в себя специальные режимы:

а) безопасный – режим, который не может нанести вред объекту испытания,

б) не безопасный – режим, который может нанести вред объекту испытания, вызвав отказ в обслуживании сетевых сервисов, потерю и изменение жизненно важной для тестируемого объекта информации.

6) Возможность испытания объектов оснащенных средствами шифрования передаваемой информации с поддержкой протоколов SSL,HTTPS, SMTPS, IMAPS и других.

7) Возможность сохранения результатов работы в различных форматах: ASCII, LaTeX, HTML, HTML с графиками.

В качестве недостатков системы Nessus можно указать на тот факт, что она осуществляет только качественную оценку безопасности с использованием бальной оценки. Это вызывает необходимость разработки комплекса программ обработки результатов работы Nessus.

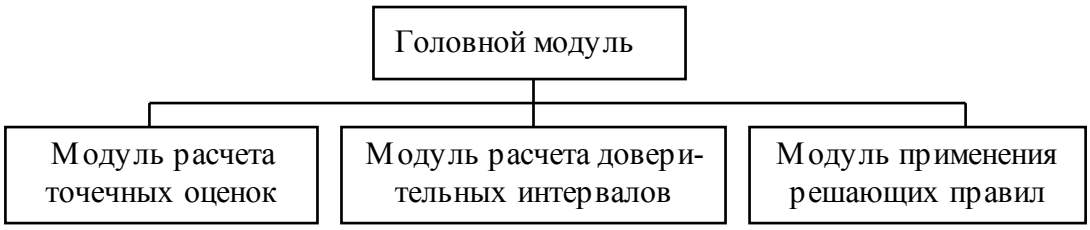

Рис. 4.6.

Структура комплекс программ оценки и обработки результатов работы СПО представлена на рис. 4.6. Рассмотрим более подробно модули представленные на рис. 4.6. Головной модуль предназначен для передачи результатов работы от одного модуля к другому, в порядке их нумерации на рис. 4.6.

Модуль расчета точечных оценок производит вычисление значений точечных оценок вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности тестируемого ОИ с использованием формул (4.11), а так же вычисление значения точечной оценки вероятности нарушения ИБ тестируемого ОИ с применение формулы (4.12). Модуль расчета доверительных интервалов строит доверительные интервалы для вероятностей полученных в ходе работы модуля №1 с применением формул (4.2),(4.3), (4.4) или (4.5),(4.6) в зависимости от исходных данных. Модуль применения решающих правил служит для формирования заключения о соответствии либо не соответствии СИБ ОИ предъявляемым к нему требованиям с точки зрения ИБ с использованием решающих правил приведенных выше.

Любой процесс испытания [87] использует некоторую совокупность входных данных, которые представляют собой **информационное обеспечение.** Перечислим данные, которые входят в состав ИО АСИ СИБ: дата проведения испытания; ФИО испытателя; характеристика объекта испытания, которая включат в себя тип ОС, назначение ОИ и т.д. Подобная информация используется для выбора МФА рассчитанных на данный ОИ, что ведет к уменьшению количества применяемых МФА; расчетные (заданные) значения вероятностей обеспечения ИБ компонент АСОИУ и всей системы в целом;

значения доверительных вероятностей β; версия БСН, который представляет собой множество МФА на ОИ.

Для повышения достоверности проводимых испытаний количество МФА представленных в БСН должно непрерывно увеличиваться, не трудно заметить, что общее количество МФА является ограничивающим фактором при задании допустимого уровня ИБ тестируемого ОИ. Это наглядно демонстрируется формулой (4.7), которая позволяет найти наименьшую верхнюю границу доверительного интервала для вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности либо всего ОИ в целом. Из этой формулы следует, что чем больше объем БСН, тем меньше может быть значение верхней границы доверительного интервала p_2 и следовательно выше достоверность испытаний. Необходимость пополнения БСН так же связана с тем, что постоянно появляются новые СИБ и как следствие новые уязвимости в составе АСОИУ. Структура ИО АСИ СИБ представлена на рис. 4.7.

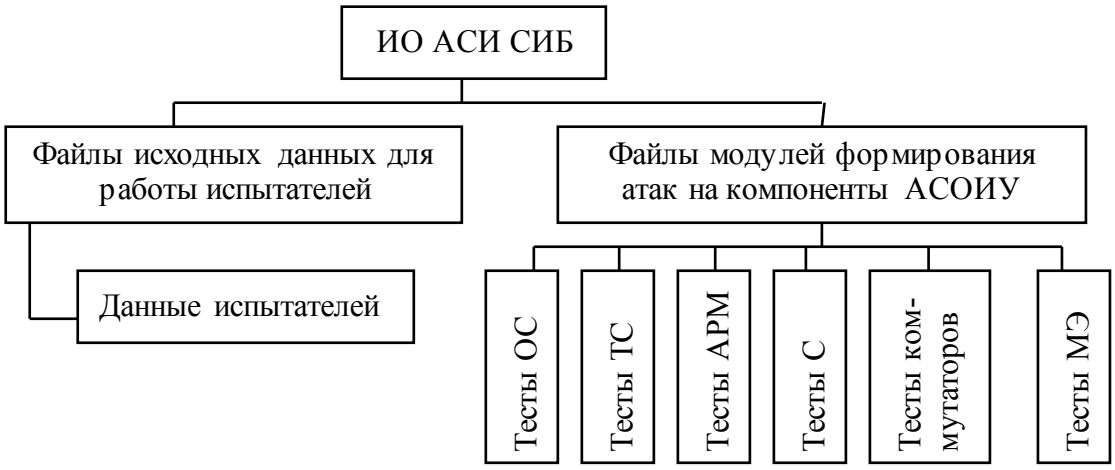

Рис. 4.7.

Тесты, которые используются при проверке безопасности можно представить с использованием классификации (см. таблицу 1 Приложения 1.и рис. 4.8.)

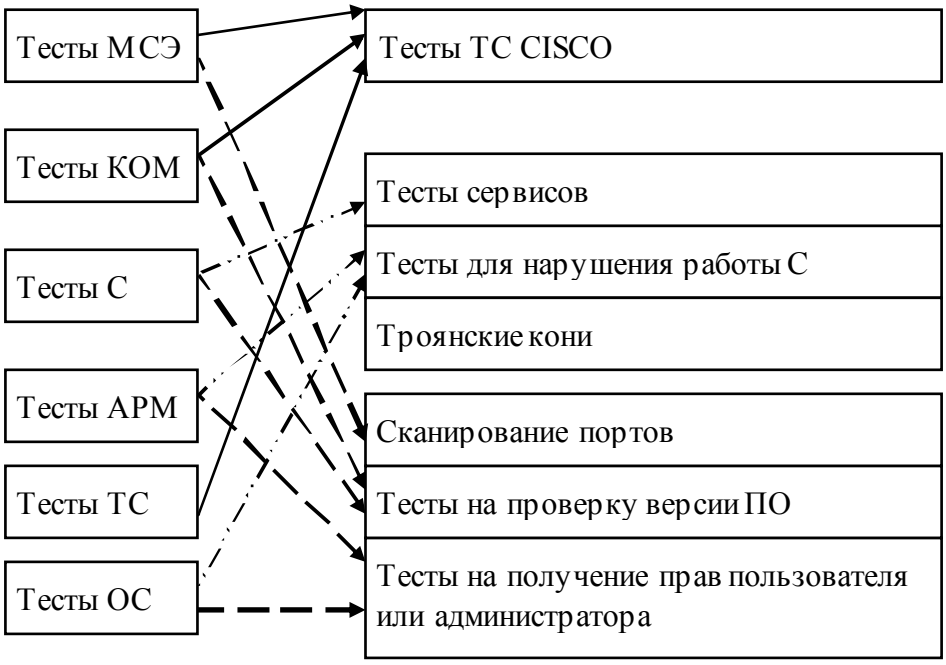

Рис. 4.8.

Тесты имеют уровень опасности, выявляемых ими уязвимостей, список которых приведен ниже: None – уязвимости нет, Low – низкий уровень уязвимости, Medium – средний уровень уязвимости, High – высокий уровень уязвимости, Critical – критический уровень уязвимости. После сканирования ОИ Nessus выдает результат, который можно сохранить в удобном для пользователя формате.

Рассмотрим инструменты, которые позволяют разрабатывать МФА, а именно **лингвистическое обеспечение**. Это вид обеспечения включает в себя специальный язык разработки МФА, а так же язык программирования используемый при создании комплекса программ обработки и оценки результатов испытаний. В качестве примера такого языка предлагается использовать NASL (Nessus Attack Scripting Language). Как уже говорилось выше, Nessus использует для организации атак отдельные модули, которые написаны на языке NASL [94]. NASL не является широко профильным языком написания сценариев. Его целью является создание тестов на проверку безопасности. В связи с этим NASL не требует большого объема оперативной памяти для выполнения сценариев, он оптимизирован для сканера безопасности Nessus

упомянутого выше. Написание тестов для Nessus на этом языке занимает мало времени. Из недостатков NASL стоит выделить следующие: в нем не поддерживается тип данных «Структура» и у него нет корректного отладчика, хотя и существует автономный интерпретатор. Стоит отметить, что NASL одновременно является как средством проверки безопасности АСОИУ, так и средством, позволяющим потенциальному нарушителю ИБ определить слабые места некоторой АСОИУ и в дальнейшем использовать их для получения доступа к ней. Тесты написанные на NASL приведены в Приложении 2.

Рассмотрим состав **персонала АСИ СИБ.** В персонал системы входит системный администратор и испытатели. В обязанности системного администратора АСИ СИБ входит: регистрация и удаление учетных записей испытателей в АСИ СИБ, назначение и изменение прав доступа испытателей к серверам АСИ СИБ, выдача имен и паролей для доступ к серверам АСИ СИБ, подержание серверов АСИ СИБ в рабочем состоянии, обновление БСН. В обязанности каждого из испытателей входит получение программы испытания, установка связи с сервером АСИ СИБ, на котором работает программа организации атак, вход в АСИ СИБ, ввод программы испытания проведение испытания, обработка результатов и формирование решения о соответствии тестируемого ОИ заданным требованиям по ИБ. Опишем методику, по которой должен работать испытатель в АСИ СИБ.

4.3. Алгоритмы и методика проведения автоматизированных испытаний средств информационной безопасности.

Предложенная выше АСИ СИБ нуждается в определении технологии ее применения при испытании конкретных элементов АСОИУ. Ответственность за результаты проводимых испытаний несет такая категория работников АСИ СИБ как испытатели. Методика их работы при проведении каждого цикла испытаний включает в себя следующие этапы:

1) Получение задания на проведение испытания, в котором указывается ОИ, цели испытания, сроки, характеристики ОИ. 2) Формирование програм-

мы испытаний, которая включают в себя виды оцениваемых уязвимостей, используемых тестов и ожидаемых результатов испытаний, вида оформления испытаний. 3) Формирование требуемого комплекса технических средств испытаний. 4) Испытания технических и программных средств АСИ СИБ. 5) Ввод имени и пароля при входе в АСИ СИБ. При разрешении входа в систему испытатель вводит свои реквизиты (ФИО, ИНН, дату, год рождения и другие данные). Эта информация необходима для облегчения классификации результатов работы испытателей, а так же облегчения поиска в больших объемах информации. 6) Выбор из БСН групп тестов указанных в программе испытаний. 7) Выбор ОИ согласно программы испытаний. 8) Запуск выбранных тестов. 9) Анализ текущей информации о ходе испытания. 10) По завершению цикла испытаний запуск комплекса программ по обработке и оценке результатов. 11) Формирование отчета о проведенных испытаниях. 12) Формирование решения о достижении целей испытаний.

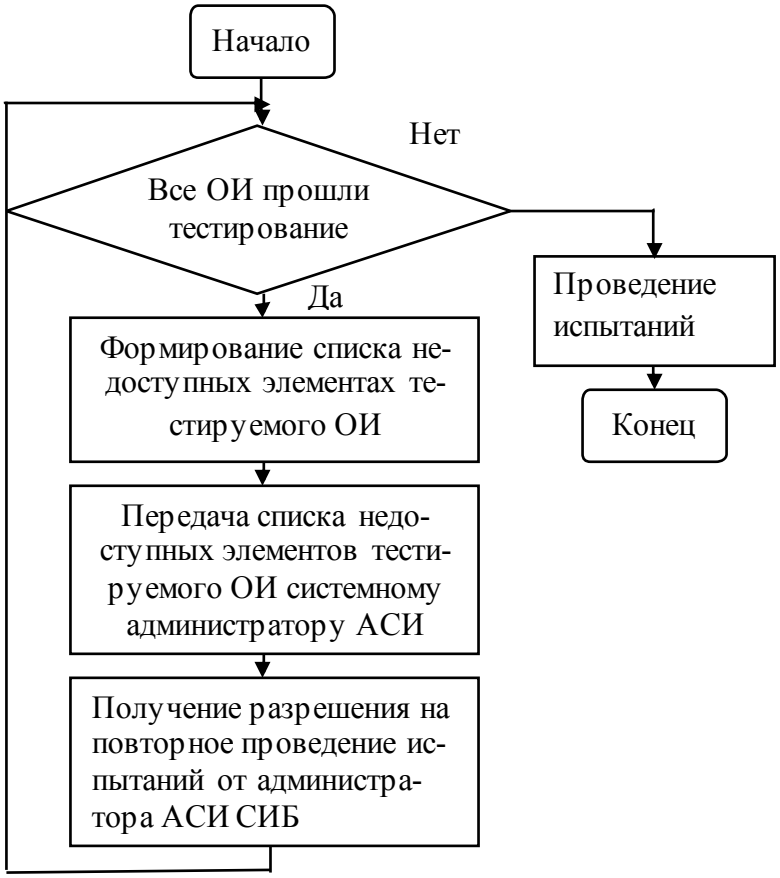

Рис. 4.9.

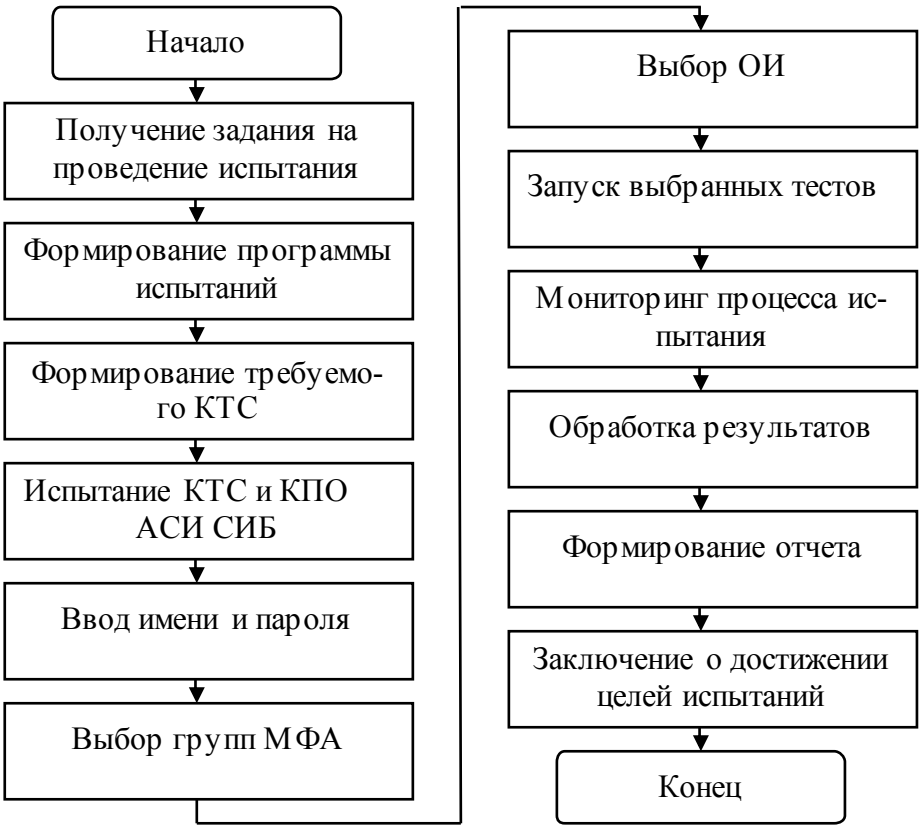

Рис. 4.10.

На рис. 4.9 приведен алгоритм работы испытателя в случае выявления элементов тестируемого ОИ не прошедших испытание по тем или иным причинам.

Если цели испытаний достигнуты, то испытания заканчиваются, в противном случае осуществляется переход к пункту 6 и осуществляется повтор пунктов 6-12. Обобщенная блок схема методики проведения автоматизированных испытаний СИБ приведена на рис. 4.10.

Отметим, что если испытания не выявили ни одной уязвимости ОИ, то с использованием NASL могут быть написаны МФА специально для проверки наличия предполагаемых уязвимостей тестируемого ОИ.

4.4. Методика применения расчетных и экспериментальных методов оценки ИБ АСОИУ.

Предложенные выше математические модели и методы для их практического применения должны подменятся определенной методикой обеспече-

ния ИБ существующих и разрабатываемых АСОИУ. Такая методика должна включать следующие этапы:

1. Задание допустимого значения вероятности не нарушения ИБ АСОИУ или определение компромиссного значения требуемой вероятности обеспечения ИБ АСОИУ при решении задачи (2.1)–(2.3).

2. Формирование допустимых значений вероятностей обеспечения конфиденциальности, целостности и доступности данных, обрабатываемых в АСОИУ, задач, решаемых в системе и ТС, используемых в системе, с помощью выражений (2.17)–(2.49).

3. Проведение автоматизированных испытаний СИБ АСОИУ, если разработана новая система или же она находится на стадии доработки или модернизации.

4. Если в результате проведения испытаний найдены СИБ не удовлетворяющие требования по ИБ сформированным при выполнении этапов 1,2, то выполняется этап 5, в противном случае система считается, удовлетворяющей заданным и сформированным требованиям на этапах 1,2 и готовой к эксплуатации.

5. Для обеспечения уровня ИБ СИБ, не прошедших испытания на этапе 3, применяются следующие модели и методы обеспечения ИБ, список которых приведен ниже:

5.1. В системе с учетом вероятностей, полученных при испытаниях на этапе 3, выделяются критические элементы путем решения задачи (3.3),(3.6)–(3.2),(3.7).

5.2. Для критических элементов выявленных на этапе 5.1. осуществляется выбор СИБ путем решения задачи оптимального выбор СИБ АСОИУ (3.11),(3.10),(3.8),(3.9).

5.3. Для того, что бы повысить уровень ИБ секретных данных обрабатываемых и хранимых в АСОИУ применяется теоретико-игровая модель размещения конфиденциальной информации на серверах АСОИУ (3.13)–

(3.16). Так же для этих целей может быть применен метод маскировки секретных данных (3.18),(3.24),(3.25),(3.26),(3.27).

Далее осуществляется переход к этапу 3 до выполнения требований по ИБ. Отметим, что на этапе 5 могут применяться и другие модели и методы обеспечения ИБ [60,108].

4.5. Пример обработки результатов испытаний программных средств информационной безопасности.

Рассмотрим макетный образец АСИ СИБ, который основан на использовании сканера безопасности Nessus и ПО обработки результатов.

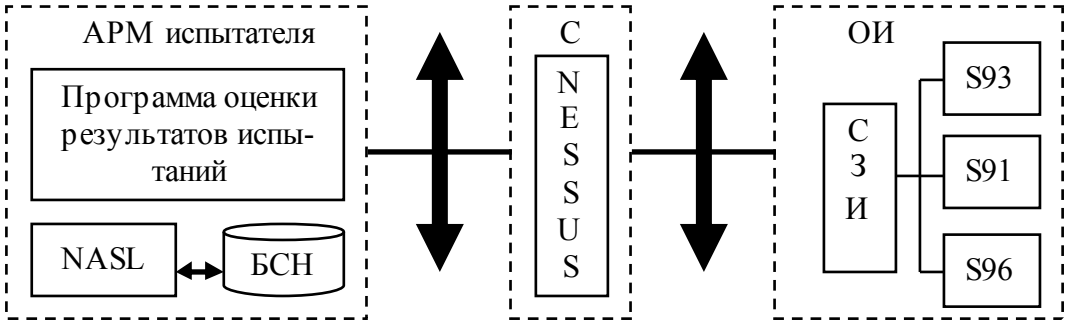

Рис. 4.11.

Его структурная схема представлен на рис. 4.11. Рассмотрим в качестве ОИ СИБ группу серверов $S91$, $S93$, $S96$ работающих под управлением ОС Windows, которые выступают в качестве ОИ на рис. 4.11. Эти сервера входят в серверную часть системы электронного документооборота ВУЗА описанную в разделе 2.3. Требования по ИБ для ее элементов были сформированы ранее в той же главе. Рассмотрим программу испытаний этой группы серверов. Она включает в себя следующие данные. 1) Личные данные испытателя и дата проведения испытаний. 2) Тип операционной системы, под управлением которой работают сервера – Windows. С учетом этого для испытаний на ИБ было выбрано 1627 тестов. 3) Доверительная вероятность $\beta = 0{,}95$. 4) Вероятности обеспечения ИБ компонент АСОИУ. Заказчиком были сформированы допустимые вероятности нарушения ИБ серверов АСОИУ (см. табл. 4.1).

Табл. 4.1

$p_{инт\|АСОИУСН}$	0,1		
$p_{инт\|К}$	0,05		
$p_{инт\|Ц}$	0,05		
$p_{инт\|Д}$	0,05		
Сервер	S96	S91	S93
$p_К$	0,005	0,01	0,01
$p_Ц$	0.005	0.01	0.01
$p_Д$	0.005	0.01	0.01

По окончанию работы Nessus выдал отчет, изучив который испытатель сформировал таблицу, содержащую количество найденных уязвимостей для каждого из серверов, и разбил их по угрозе нарушения конфиденциальности, целостности и доступности информации (таблица 4.2).

Табл. 4.2

Сервер	S91	S93	S96
Всего	1	0	1
К	1	0	1
Ц	1	0	1
Д	0	0	0

С использованием методики описанной выше были найдены точечные оценки, и доверительные интервалы для исходных данных таблицы 4.2 результат представлен в таблице 4.3.

Табл. 4.3

Сервер	S91	S93	S96
$p^*_К$	0.0006146281	0	0.0006146281
$I^К_\beta$	(0.0006136303; 0.0006156276)	(0;0.0018396)	(0.0006136303; 0.0006156276)
$p^*_Ц$	0.0006146281	0	0.0006146281
$I^Ц_\beta$	(0.0006136303; 0.0006156276)	(0;0.0018396)	(0.0006136303; 0.0006156276)
$p^*_Д$	0	0	
$I^Д_\beta$	(0;0.0018396)	(0;0.0018396)	(0;0.0018396)

Определим интегральные точечные оценки конфиденциальности, целостности, доступности и всей системы в целом с применением формул (4.13), (4.14). Результат приведен в таблице 4.4.

Табл. 4.4

$p^{*}_{инт\|АСОИУ\ СН}$	0.0024563
$I^{АСОИУ\ СН}_{инт\|\beta}$	(0.0024508146; 0.0024617976)
$p^{*}_{инт\|К}$	0.0012289
$I^{К}_{инт\|\beta}$	(0.0012265939; 0.0012312104)
$p^{*}_{инт\|Ц}$	0.0012289
$I^{Ц}_{инт\|\beta}$	(0.0012265939; 0.0012312104)
$p^{*}_{инт\|Д}$	0
$I^{Д}_{инт\|\beta}$	(0;0.0018396)

Сравнив требования по ИБ представленные в таблице 4.1 и доверительные интервалы, полученные в таблицах 4.3 и 4.4 с использованием решающих правил описанных выше можно сделать заключение о том удовлетворяет ли СИБ тестируемых серверов и система в целом требованиям заказчика.

Результат, говорящий о соответствии ТС заданным требования по обеспечению ИБ, приведен в таблице 4.5.

Табл. 4.5

ОИ	АСОИУ	S96	S91	S93
Соответствие	Да	Да	Да	Да

В результате испытаний получено подтверждение требуемого уровня ИБ СИБ серверов рассматриваемой системы.

Выводы по главе 4.

1. Введен ряд определений необходимых для разработки структуры и функций АСИ СИБ. Описаны цели и задачи, которые необходимо решить при автоматизации процесса испытания СИБ.

2. Для получения достоверных результатов испытания на ИБ предлагается использовать аппарат теории вероятностей и математической статистики, а именно раздел обработки результатов испытаний.

3. Разработана структура и функции АСИ СИБ. Изложена методика и алгоритмы проведения автоматизированных испытаний СИБ. Приведена классификация возможных тестов для проверки ИБ.

4. Предложена методика разработки информационно безопасных АСОИУ.

5. Предложен макетный образец АСИ СИБ, который основан на использовании сканера безопасности Nessus и программы обработки результатов, разработанной для него.

Заключение

1. Приведен обзор работ, посвященных вопросам обеспечения ИБ, а так же обзор и анализ основных СИБ. Обоснована необходимость создания прикладной теории ИБ предметом, которой является разработка методик эффективного применения существующих и перспективных СИБ в процессе разработки и эксплуатации АСОИУ.

2. Приведено, используемое в работе, определение понятия ИБ. Сформулированы основные принципы прикладной теории ИБ: принцип комплексности применяемых СИБ, принцип экономичности СИБ, принцип обеспечения максимальной ИБ критических компонентов АСОИУ, принцип прогнозирования угроз и применения средств нападения, принцип обеспечения максимальной неопределённости для противника применяемых стратегий ИБ.

3. Предложены следующие базовые модели прикладной теории ИБ: абстрактная математическая модель, концептуальная модель информационной системы, модель прикладной информационной технологии, концептуальная модель системы ИБ ИТ – продуктов.

4. Для формирования количественных вероятностных характеристик ИБ компонент АСОИУ предложено использовать статистику попыток нарушения ИБ реальных АСОИУ или же спрогнозированные заказчиком интенсивности попыток нарушения ИБ компонент АСОИУ. На основе этого разработан подход, позволяющий формировать компромиссное значение требуемой вероятности обеспечения ИБ АСОИУ с учетом стоимости СИБ, применяемых для ее обеспечения, и допустимых потерь от нарушения ИБ системы.

5. Разработана методика формирования допустимых значений вероятностей обеспечения конфиденциальности, целостности и доступности информации, циркулирующей в проектируемой или существующей АСОИУ. На ее основе разработана методика формирования допустимых значений ве-

роятностей обеспечения ИБ данных, циркулирующих в АСОИУ, задач решаемых в АСОИУ и ТС используемых в ней.

6. Приведен пример вычисления допустимых вероятностных характеристик ИБ данных, задач и ТС АСОИУ. При решении использовались заданные Заказчиком интенсивности попыток нарушения ИБ конфиденциальности, целостности, доступности, а так же данных, задач и ТС системы. В системе фигурируют данные четырёх уровней конфиденциальности: «совершенно секретно», «секретно», «ДСП», «открытые данные», Заказчиком был задан допустимый уровень ИБ разрабатываемой АСОИУ $Q_{ИБ}^{доп}=0,9$.

7. Разработана математическая модель выделения критических элементов АСОИУ, позволяющая существенным образом повысить ИБ рассматриваемой АСОИУ за счет своевременного выделения среди ее элементов наиболее уязвимых с точки зрения ИБ.

8. Приведено решение двухкритериальной задачи оптимального выбора СИБ АСОИУ из заданного множества с учетом стоимости выбранных СИБ и вероятности преодоления противником хотя бы одного из них.

9. Для решения задачи размещения конфиденциальных данных в серверной части АСОИУ предложено использовать теоретико-игровые модели, где одним из игроков выступает администратор СИБ АСОИУ, а другим потенциальный противник. Рассмотрен вопрос реализации случайного механизма размещения конфиденциальных данных.

10. Предложена методика создания «ложных целей» для информационных атак на хранимые в АСОИУ конфиденциальные данные, в качестве которых выступают файлы, замаскированные под реальную информацию.

11. Описаны цели и задачи, которые необходимо решить при автоматизации процесса испытания СИБ. Разработана структура и функции АСИ СИБ. Изложена методика и алгоритмы проведения автоматизированных испытаний СИБ. Приведена классификация возможных тестов для проверки ИБ. Предложена методика разработки информационно безопасных АСОИУ.

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999, 328 с.
2. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ–Петербург, 2003.–368 с.
3. Казарин О.В. Безопасность программного обеспечения компьютерных систем. М.: МГУЛ, 2003, 212 с.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных.- М.: Энергоатомиздат, 1994. Кн.1.-401с.
5. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему. Ч.1. – СПб.: Мир и семья-95, 1997. -312с.
6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. -М.: 1992.
7. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. -М.: 1992.
8. Савкин С.В. Взаимосвязь информационной безопасности, цены и качества // XXXI Гагаринские чтения. Тезисы докладов международной молодежной конференции. Москва, 5-9 апреля 2005 г. М.: МАТИ 2005. Т.4, 30-31 с.
9. Васильев В.И., Иванова Т.А. Алгоритм проектирования оптимальной структуры комплексной системы защиты информации на основе анализа риска. Материалы VII Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2005. – 270-274 с.
10. Васютин С.В., Корнеев В.В., Райх В.В., Синица И.Н. Принятие обобщенных решений в системах обнаружения вторжений, использующих

несколько методов анализа данных мониторинга. Материалы VII Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2005. – 318-325 с.

11. Климов С.М. Структура методики оценки эффективности средств защиты информации от программно-математических воздействий. Материалы V Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2003. – 36-40 с.
12. Тищенко Е.Н. Некоторые подходы к определению экономической эффективности методов защиты информации в среде распределенной информационной системы. Материалы V Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2003. – 245-247 с.
13. Чибиров М. О. Об использовании конечных игровых моделей при синтезе систем защиты информации. Материалы VI Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2004. – 69-70 с.
14. Мосолов А.С., Новиков Ю.В. Обобщенный критерий оценки эффективности подсистемы обнаружения СКБ и оценка вероятности обнаружения нарушителя. Материалы VI Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2004. – 116-118 с.
15. Лепешкин О.М., Кульчицкий К.А. Экономико-математическая модель информационной безопасности предприятия. Материалы VI Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2004. –126-127 с.
16. Росенко. А.П. Научно-теоретические основы исследования влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированных информационных системах. Известия ТРТУ. Тематический выпуск. Материалы VII Международ-

ной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 19-30с.

17. Росенко А.П., Евстафиади С.П., Феник Е.В. Применение методики функциональной декомпозиции к локальной автоматизированной информационной системе. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 30-35с.
18. Калмыков И.А. Метод пересчета коэффициентов обобщенной с полиадической системы для спецпроцессоров с деградируемой структурой. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 35-42с.
19. Сундеев П.В. Модульно-кластерный анализ: аспекты информационной безопасности. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 53-60с.
20. Климов С.М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 74-82с.
21. Жук А.П., Савелов Р. Ю. Архитектура межсетевого экрана для корпоративных сетей. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 143-147с.
22. Мирошников В.В. Методический подход к оценке эффективности способов защиты информации в среде распространения сигналов локаль-

ной вычислительной сети. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. № 4 - 156-163с.

23. Илларионов Ю.А., Монахов М.Ю. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах. - Владимир: ВГУ, 2004.
24. Ермошин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. Как Cisco Systems и ведущие компании мира используют Интернет Решения для Бизнеса. - М.: Изд-во Московского гуманитарного университета, 2003.
25. Абашеев А.А., Жуков И.Ю., Иванов М.А. и др. Ассемблер в задачах защиты информации. - М.: КУДИЦ-ОБРАЗ, 2004.
26. Мак-Клар С., Шах С., Шах Ш. Хакинг в Web: атаки и защита. - М., СПб., Киев: Вильямс, 2003.
27. Морозов Н.П., Чернокнижный С.Б. Защита деловой информации для всех: компьютерные программы, работа офиса, законодательство. - СПб.: ИД "Весь", 2003.
28. Уфимцев Ю.С, Буянов В.П., Ерофеев Е.А. и др. Методика информационной безопасности. - М.: Экзамен, 2004.
29. Защита информации в сети - анализ технологий и синтез решений. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. - М.: ДМК Пресс, 2004.
30. Уэнстром М. Организация защиты сетей Cisco. - М., СПб., Киев: Вильямс, 2003.
31. Березин С.В., Шапошников И.В. Ваш выход в интернет. Секреты эффективной и безопасной работы. - СПб.: БХВ-Петербург, 2004.
32. Разработка экспертных систем. Среда CLIPS. Частиков А.П., Гаврилова Т.А., Белов Д.Л. - СПб.: БХВ-Петербург, 2003.

33. Лодон Дж., Лодон К. Управление информационными системами. - 7-е изд.. - СПб.: Питер, 2005.
34. Киселев В.Д., Есиков О.В., Кислицин А.С. Защита информации в современных системах ее передачи и обработки.
35. Лопатин С.Е. Проблемы информационной безопасности и информационный терроризм. // XXXI Гагаринские чтения. Тезисы докладов международной молодежной конференции. Москва, 5-9 апреля 2005 г. М.: МАТИ 2005. Т.4, 18-19 с.
36. Наумов Д. А. Программный комплекс локализации сетевых атак // XXXI Гагаринские чтения. Тезисы докладов международной молодежной конференции. Москва, 5-9 апреля 2005 г. М.: МАТИ 2005. Т.4, 21-22 с.
37. Сердюк В. А. Роль персональных сетевых экранов в защите автоматизированных систем от информационных атак // XXXI Гагаринские чтения. Тезисы докладов международной молодежной конференции. Москва, 5-9 апреля 2005 г. М.: МАТИ 2005. Т.4, 31-32 с.
38. Толпегин П.В. Агентно–ориентированный подход к построению корпоративных систем безопасности с применением методов классификации и распознавания // XXXI Гагаринские чтения. Тезисы докладов международной молодежной конференции. Москва, 5-9 апреля 2005 г. М.: МАТИ 2005. Т.4, 38-39 с.
39. Жуков А.А., Третьяк Н.В. Технология аудита банковских информационных систем. // IT-бизнес. Электронный банк. М. 2006. №1 с. 18–25с.
40. Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А.А. Разработка систем информационно-компьютерной безопасности // – СПб: ВКА им. А.Ф.Можайского, 2003. – 327 с.
41. Марков А.С., Миронов С.В., Цирлов В.Л. Разработка политики безопасности организации в свете новейшей нормативной базы // Защита информации. Конфидент, 2004. - №2. – С. 20-28.

42. Мельников Ю.Н., Готовский М.Ю. Выбор комплекса мер защиты информации на основе критерия «эффективность–стоимость». // Приборы и системы управления. №11. 1998. – 11-13с.
43. Воробьев А.А. Проблемные вопросы анализа защищенности автоматизированных систем. // «Актуальные проблемы информационного противоборства», сборник статей. – М. МАКПБ, 1999.
44. Воробьев А.А. Методика испытаний АС ВН на соответствие требованиям по защищенности от несанкционированного доступа. Отчет о научно-исследовательской работе. Разработка временных технических условий и методик сертификационных испытаний технических, программных средств и автоматизированных систем по требованиям безопасности информации (промежуточный). Шифр – "Билетер-СП". М.: 1998г.
45. Астахов А. Аттестация автоматизированных систем // Jet Info, 2000 - № 11. - 20 с.
46. Марков А.С., Цибин В.В. К вопросу о сертификации программных ресурсов автоматизированных систем по требованиям безопасности информации // Документальная электросвязь, 2004. - № 13.
47. Марков А.С., Щербина С.А. Испытания и контроль программных ресурсов // InformationSecurity, 2003. – № 6 – С. 25.
48. Положение об аттестации объектов информатизации по требованиям безопасности информации. Гостехкомиссия России, 1994.
49. Просянников Р. Проблемы аттестации автоматизированных систем // Netweek. 2002, - № 9.
50. Цибин В.В. Теория и практика аттестации объектов информатизации по требованиям безопасности информации – ЗАО «НПП «БИТ», 2000.
51. Воробьев А. А. Теоретико-игровые модели исследования защищенности автоматизированных систем. //Тезисы докладов межвидового се-

минара МО РФ "Эффективность технической эксплуатации и ремонта ВВТ". - Люберцы: МО РФ, 2003. - с. 62-68.

52. Воробьев А. А., Хромов А.В. и др. РВ 50.1.023–2000. Рекомендации по стандартизации «Положение по организации разработки математического, программного, информационного и лингвистического обеспечения АС ВН, отвечающего требованиям информационной безопасности». – М.: Издательство стандартов, 2000 г. (Приняты Постановлением Госстандарта России № 164–СТ от 21.06.2000).
53. Воробьев А. А., Хромов А.В. и др. РВ 50.1.024–2000. Рекомендации по стандартизации «Положение по классификации и кодированию программного и информационного обеспечения АС ВН по требованиям информационной безопасности». – М.: Издательство стандартов, 2000г. (Приняты Постановлением Госстандарта России № 164–СТ от 21.06.2000).
54. Воробьев А. А., Хромов А. В., Климов С. М. Рекомендации по стандартизации «Положение по сопровождению программного обеспечения АС ВН по требованиям безопасности информации» (Утверждены Начальником вооружения ВС РФ 30.11.2000 в качестве рекомендаций по стандартизации Минобороны России).
55. Кук Д., Бейз Г. Компьютерная математика.–М.: Наука, 1990. – 383с.
56. Компьютер и задачи выбора. / Автор предисловия. Ю.И. Журавлев. М.: Наука, 1989. –208 с.
57. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. – М.: Наука, 1968, 496с.
58. Моисеев В.С. Анализ функционирования СУ предприятием на базе е информационной модели. // ИВУЗ «Авиационная техника», №2 1973 с. 15-22.
59. Берж К. Теория графов и ее применения. М.: Иностранная литература, 1962, 319 с.

60. Гинатуллин И.А., Зиновьев П.А., Моисеев В.С., Иванов К.В., Тутубалин П.И. Обзор методов и средств защиты информации. – ШИФР ПМ-12-СМ-6. – Института проблем информатики АН РТ. – Казань. – 2005г.
61. Моисеев В.С., Дятчин В.В., Тутубалин П.И. Оценка требуемых вероятностей обеспечения информационной безопасности. // Вестник КГТУ. №4. – с. 36–39.
62. Моисеев Н.Н. Математические задачи системного анализа. М.: Наука, 1981, 488 с.
63. Кудрявцев Л.Д. Курс математического анализа: Учебник для студентов университетов и вузов. В 3-х т. 2-е изд. М.: Высш. шк., 1989.
64. Галатенко В.А. Основы информационной безопасности. Учеб.: Для вузов. 3-е изд. – М. - ИНТУИТ.РУ, 2006 – 208 с.
65. Курило А.П., Мамыкин В.Н. Обеспечение информационной безопасности бизнеса. М. изд. - БДЦ-ПРЕСС, 200 – 512 с.
66. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004. – 384 с.
67. Вентцель Е.С. Теория вероятностей. М.: Высш. шк., 2002, 575 с.
68. Кристофидес Н. Теория графов. Алгоритмический подход М.: Мир, 1978. 432 с.
69. Таненбаум Э., Ван Стен М. Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003.
70. Мирошников Б. Проблема 21 века // Системы и средства защиты информации. IT Security. – М: 2004. – №1. – С. 10-30.
71. Герасименко В.А., Размахнин М.К. Организация работ по защите информации в системах электронной обработки данных // Зарубежная радиоэлектроника. – 1989. – №12. – С. 110-120.
72. Нестеров С.А. Об использовании конечных игровых моделей для оценки экономической эффективности систем защиты информации // Тр.

научно-техн. конф. «Безопасность информационных технологий». – 2001. – Т.1. – С. 31-33.

73. Воробьев Н.Н. Основы теории игр. Бескоалиционные игры. – М.: Наука, 1984.
74. Вентцель Е.С. Исследование операций. – М.: Советское радио, 1972.
75. Льюс Р.Д., Райфа Х. Игры и решения. М.: Иностранная литература. 1961.
76. Оуэн Г. Теория игр. – М.: Наука, 1971.
77. Дюбин Г.Н., Суздаль В.Г. Введение в прикладную теорию игр. – М.: Наука, 1981.
78. Моисеев В.С., Козар В.В., Тутубалин П.И., Бормотов К.В. Двухкритериальная теоретико-игровая модель с заданным упорядочиванием смешанных стратегий // Вестник КГТУ. – 2005. – №1. – С. 40–45.
79. Мамиконов А.Г., Кульба В.В. , Шелков А.Б. Достоверность, защита и резервирование информации в АСУ. М.: Энергатомиздат. 1988 г, 302 с.
80. Хайруллин Р.Р. Методы сокрытия шифротекста в шифроттексте // Международный молодёжный научн. конф. «Туполевские чтения», т.3, Казань, 2005, с.111-113.
81. Димаки А.В. Получение последовательностей случайных чисел с заданным законом распределения // Доклады Международной научно-практической конференции, ч.2, Томск 2005, 296 с.
82. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М., Наука, 1984, 831с.
83. Уайлд Д.Д. Методы поиска экстремума. М., Наука, 1967, 268с.
84. Подиновский В.В., Ногин В.Д. Паретооптимальные решения многокритериальных задач - М. «Наука», 1982. – 256 с.
85. Дятчин В.В., Тутубалин П.И., Бормотов К.В. Применение теоретико-игровой модели для размещения конфиденциальной информации на

серверах корпоративной информационной системы. // Исследования по информатике. Выпуск №11. – Изд.: Отечество. Казань, 2007. – с.89–94.

86. Новоселов А.С., Болнокин В.Е., Чинаев П.И., Юрьев А.Н. Системы адаптивного управления летательными аппаратами, М., Машиностроение, 1987, 280с.

87. Адгамов Р.И., Берхеев М.М., Заляев И.А. и д.р. Автоматизированные испытания в авиастроении. – М.: Машиностроение, 1989. – 232 с.

88. Дунин-Барковский И.В., Смирнов Н.В. Теория вероятностей и математическая статистика в технике. М. Изд. технико-теорет.лит. 1955.

89. Манита А.Д. Теория вероятностей и математическая статистика.М.: Издательский отдел УНЦ ДО Московского университета., 2001.

90. Феллер В. Введение в теорию вероятностей и её Приложения. Т.1. М.: Мир, 1964. 513с.

91. Моисеев В.С., Дятчин В.В., Тутубалин П.И. Расчет вероятностных характеристик информационной безопасности разрабатываемых автоматизированных систем. Тезисы докладов 3-й международной научно-практической конференции. Казань, 2005г. с.113-114.

92. Марков А., Ермолаев С., Инструментальные средства аттестации программных ресурсов объектов информатизации. // InformationSecurity №4, 2004г.

93. http://www.nessus.org

94. http://www.dn-systems.org/boss/doc/nasl_guide-20050103.pdf

95. Ботарев И.В., Зиновьев П.А., Насыров И.З, Фирсов А.А. О целях, задачах и перспективах развития корпоративного домена «www.antat.ru» // Исследования по информатике. Вып.3. – Казань. Отечество. 2001. с. 31-40.

96. Корбут А.А., Финкельштейн Ю.Ю. Дискретное программирование (Серия: «Экономико-математическая библиотека») М.: Наука, 1969 г. - 368 с.

97. Финкельштейн Ю.Ю. Приближенные методы и прикладные задачи дискретного программирования. М.: Наука, 1976. – 263 с.

98. Моисеев В.С., Козар А.Н., Дятчин В.В. Информационная безопасность автоматизированных систем управления специального назначения. Изд. Отечество. Казань. 2006 г.

99. Дятчин В.В., Моисеев В.С., Огородников Р.В., Тутубалин П.И. Основные задачи прикладной теории безопасности информационных систем. // Тезисы докладов 2–й ежегодной международной научно-практической конференции. «Инфокоммуникационные технологии глобального информационного общества». Казань, 2004. с. 33.

100. Козар А.Н., Тутубалин П.И., Бормотов К.В. Двухкритериальная теоретико–игровая модель с заданным упорядочиванием смешанных стратегий // Компьютерное моделирование 2004. Труды 5–й Международной научно–технической конференции. Часть 1, СПб. Изд. Нестор. 2004. с.80–82.

101. Бормотов К.В., Тутубалин П.И. Теоретико–игровая модель упорядочивания смешанных стратегий. // XXII Туполевские чтения. Материалы Международной молодежной научной конференции. Казань. 2004. с.6–8.

102. Тутубалин П.И., Дятчин В.В. Теоретико–множественная модель информационной системы для построения статистических оценок обеспечения конфиденциальности, целостности и доступности данных. // Сборник статей XVI Международной научно–технической конференции. Пенза, 2005. с.188–191.

103. Тутубалин П.И. Определение допустимых значений вероятностей не нарушения ИБ компонент конфиденциальности, целостности и доступности информации ИС. // VIII Королевские чтения. Всероссийская молодежная научная конференция. Самара. Тезисы докладов. 2005. с. 339.

104. Тутубалин П.И. Методика формирования допустимых вероятностей нарушения информационной безопасности аппаратно–программных средств АСУ. // Туполевские чтения. Материалы Международной молодежной научной конференции, посвященной 1000–летию города Казани. Казань. 2005. Т.3. с.20–22.

105. Тутубалин П.И. Задача определения критических компонент прикладных информационных технологий. // Электронные средства и системы управления. Доклады международной научно–практической конференции. Томск. 2005.Ч.2.–с. 166–169.

106. Тутубалин П.И. Рандомизировнная стратегия размещения конфиденциальных данных в узлах сети КИС. // Микроэлектроника и информатика–2005. 12–я Всероссийская межвузовская научно–техническая конференция студентов и аспирантов. Тезисы докладов. –М.: МИЭТ, 2005. с.194.

107. Тутубалин П.И. Вероятностные модели и методы обеспечения информационной безопасности АСУ. // XIV Туполевские чтения. Материалы Международной молодежной научной конференции. Казань. 2006. Т.4. с.96–98.

108. Кузнецов Н.А., Кульба В.В., Микрин Е.А. и др. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. Ин-т проблем передачи информации. РАН. – М. Наука, 2006.

109. http://www.do.rksi.ru/library/courses/infbez/ch01s03.dbk

Приложение 1. Таблицы результатов расчетов

Табл. П.1. 1.

№ Варианта	λ	$q(\lambda)$	$Z_{\phi}(q)$ руб. в год	$Z_{C}(q)$ руб. в год
1	0,9801111	0,9507702	1762	950770
2	0,9802847	0,9515472	1746	951547
…	…	…	…	…
30	0,9851458	0,97656789	1309	976567
…	…	…	…	…
40	0,9868822	0,98751665	1154	987516
…	…	…	…	…
46	0,9879236	0,99479480	1061	994794
47	0,9880972	0,99606783	1046	996067
48	0,9882708	0,99735933	1030	997359
49	0,9884445	0,99866986	1015	998669

Табл. П.1. 2.

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
D^0_{B1}										1		
D^0_{B2}						1						1
D^0_{B3}		1	1			1						1
D^0_{B4}												
D^0_{B5}	1											
D^0_{B6}	1									1		
D^0_{B7}									1			
D^0_{B8}	1				1		1		1		1	1
D^0_{B9}	1				1		1		1		1	1
D^0_{B10}	1						1				1	
D^0_{B11}				1		1						
D^0_{B12}			1		1	1	1					
D^0_{B13}												
D^0_{B14}												
D^1_{B1}	1	1	1	1					1	1		
D^1_{B2}												
D^1_{B3}				1								
D^1_{B4}		1	1		1	1	1				1	1
D^1_{B5}						1		1				1
D^1_{B6}								1				1
D^2_{B1}												
D^2_{B2}		1							1			
D^2_{B3}												
D^3_{B1}							1					

Табл. П.1. 3.

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
D_{V1}	1											
D_{V2}		1										
D_{V3}			1									
D_{V4}				1								
D_{V5}					1							
D_{V6}						1						
D_{V7}							1					
D_{V8}								1				
D_{V9}									1			
D_{V10}										1		
D_{V11}											1	
D_{V12}												1

Табл. П.1. 4.

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
z_1		1										
z_2			1									
z_3				1			1					
z_4					1	1						
z_5								1				
z_6								1				
z_7					1			1				
z_8									1	1	1	1
z_9												
z_{10}												
z_{11}												
z_{12}												

Табл. П.1. 5.

	C	M	ЛС1	ЛС2	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11
z_1	1	1	1	1	1									1	1
z_2	1	1	1	1		1	1	1	1	1	1			1	1
z_3	1	1	1	1		1	1							1	1
z_4	1	1	1	1		1	1					1		1	1
z_5	1	1	1	1										1	1
z_6	1	1	1	1										1	1
z_7	1	1	1	1								1	1	1	1
z_8	1	1	1	1								1	1	1	1
z_9	1	1	1	1										1	1
z_{10}	1	1	1	1										1	1
z_{11}	1	1	1	1									1	1	1
z_{12}	1	1	1	1									1	1	1

Табл. П.1. 6.

Наименование ТС	Интервал между попытками нарушения ИБ ТС (в сутки)
АРМ 1 - АРМ 11	1/3=0.333
Сервер	1/7=0.142
Маршрутизатор	2/(7+3)=0.2
ЛС1 и ЛС2	1/3=0.333

Табл. П.1. 7.

Задача	Требования по ИБ (конфиденциальность)
z_1	0.9936
z_2	0.9958
z_3	0.9958
z_4	0.9958
z_5	0.9975
z_6	0.9958
z_7	0.9975
z_8	0.9975
z_9	0.9975
z_{10}	0.9975
z_{11}	0.9975
z_{12}	0.9975

Табл. П.1. 8.

Наименование ТС	Допустимые вероятность нарушения ИБ
АРМ 2 - АРМ 7	0.9996
АРМ 10 – АРМ 11	0.9996
Сервер	0.9998
Маршрутизатор	0.9997
ЛС1 и ЛС2	0.9996

Табл. П.1. 9.

	С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
z_1	0.9995	0.9994	0.9989	0.9989	0.9989									0.9989	0.9989
z_2	0.9998	0.9997	0.9996	0.9996		0.9996	0.9996	0.9996	0.9996	0.9996	0.9996			0.9996	0.9996
z_3	0.9997	0.9996	0.9994	0.9994		0.9994	0.9994							0.9994	0.9994
z_4	0.9998	0.9997	0.9995	0.9995		0.9995	0.9995					0.9995		0.9995	0.9995
z_5	0.9998	0.9997	0.9995	0.9995										0.9995	0.9995
z_6	0.9996	0.9995	0.9992	0.9992										0.9992	0.9992

Продолжение Табл. П.1. 9.

	С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
z_7	0.9998	0.9998	0.9996	0.9996								0.9996	0.9996	0.9996	0.9996
z_8	0.9998	0.9998	0.9996	0.9996								0.9996	0.9996	0.9996	0.9996
z_9	0.9998	0.9997	0.9995	0.9995										0.9995	0.9995
z_{10}	0.9998	0.9997	0.9995	0.9995										0.9995	0.9995
z_{11}	0.9998	0.9998	0.9996	0.9996									0.9996	0.9996	0.9996
z_{12}	0.9998	0.9998	0.9996	0.9996									0.9996	0.9996	0.9996

Табл. П.1. 10.

С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
0.9998	0.9998	0.9996	0.9996	0.9989	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996

Табл. П.1. 11

Номер задачи	Интенсивности попыток нарушения целостности ИБ задач
1-3	6
4-7	7
8	5
9-12	3

Табл. П.1. 12.

Задача	Требования по ИБ (целостность)
z_1	0.9935
z_2	0.9958
z_3	0.9958
z_4	0.9958
z_5	0.9974
z_6	0.9958
z_7	0.9974
z_8	0.9974
z_9	0.9974
z_{10}	0.9974
z_{11}	0.9974
z_{12}	0.9974

Табл. П.1. 13.

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
l_1	0.9967	0.9967	0.9967	0.9972		0.9972		0.996	0.9934			
l_2	0.9967	0.9967	0.9967	0.9972		0.9972		0.996		0.9934		
l_3	0.9967	0.9967	0.9967	0.9972		0.9972		0.996			0.9934	
l_4	0.9967	0.9967	0.9967	0.9972		0.9972		0.996				0.9934
l_5	0.9967	0.9967	0.9967	0.9972	0.9972			0.996	0.9934			
l_6	0.9967	0.9967	0.9967	0.9972	0.9972			0.996		0.9934		
l_7	0.9967	0.9967	0.9967	0.9972	0.9972			0.996			0.9934	
l_8	0.9967	0.9967	0.9967	0.9972	0.9972			0.996				0.9934
l_9	0.9967	0.9967	0.9967		0.9972		0.9972	0.996	0.9934			
l_{10}	0.9967	0.9967	0.9967		0.9972		0.9972	0.996		0.9934		
l_{11}	0.9967	0.9967	0.9967		0.9972		0.9972	0.996			0.9934	
l_{12}	0.9967	0.9967	0.9967		0.9972		0.9972	0.996				0.9934
l_{13}	0.9963	0.9963	0.9963				0.9968	0.9955	0.9926			
l_{14}	0.9963	0.9963	0.9963				0.9968	0.9955		0.9926		
l_{15}	0.9963	0.9963	0.9963				0.9968	0.9955			0.9926	
l_{16}	0.9963	0.9963	0.9963				0.9968	0.9955				0.9926

Табл. П.1. 14.

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
0.9967	0.9967	0.9967	0.9972	0.9972	0.9972	0.9972	0.996	0.9934	0.9934	0.9934	0.9934

Табл. П.1. 15.

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
0.9935	0.9958	0.9958	0.9958	0.9974	0.9958	0.9974	0.9974	0.9974	0.9974	0.9974	0.9974
0.9967	0.9967	0.9967	0.9972	0.9972	0.9972	0.9972	0.9960	0.9934	0.9934	0.9934	0.9934
0.9967	0.9967	0.9967	0.9972	0.9974	0.9972	0.9974	0.9974	0.9974	0.9974	0.9974	0.9974

Табл. П. 1. 16.

Наименование ТС	Интенсивность атак нарушения целостноти ТС
АРМ 2 - АРМ 7	2
АРМ 10 – АРМ 11	2
Сервер	5
Маршрутизатор	5
ЛС1 и ЛС2	5

Табл. П.1. 17.

	С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
z_1	0.9997	0.9994	0.9989	0.9989	0.9989									0.9989	0.9989
z_2	0.9998	0.9997	0.9996	0.9995		0.9996	0.9996	0.9996	0.9996	0.9996	0.9996			0.9996	0.9996
z_3	0.9997	0.9996	0.9994	0.9994		0.9994	0.9994							0.9994	0.9994

Продолжение Табл. П.1. 17.

	С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
z_4	0.9998	0.9997	0.9995	0.9995		0.9995	0.9995					0.9995		0.9995	0.9995
z_5	0.9998	0.9997	0.9995	0.9995										0.9995	0.9995
z_6	0.9996	0.9995	0.9992	0.9991										0.9992	0.9992
z_7	0.9998	0.9998	0.9996	0.9996								0.9996	0.9995	0.9996	0.9996
z_8	0.9998	0.9998	0.9996	0.9996								0.9996	0.9996	0.9995	0.9996
z_9	0.9998	0.9997	0.9995	0.9995										0.9995	0.9995
z_{10}	0.9998	0.9997	0.9995	0.9997										0.9995	0.9995
z_{11}	0.9998	0.9998	0.9996	0.9996									0.9996	0.9996	0.9996
z_{12}	0.9998	0.9998	0.9996	0.9997									0.9996	0.9996	0.9995

Табл. П.1. 18.

С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
0.9998	0.9998	0.9996	0.9996	0.9997	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996

Табл. П. 1. 19.

Номер задачи	Интенсивности попыток нарушения доступности ИБ задач
1-3	6
4-7	7
8	5
9-12	3

Табл. П.1. 20.

Задача	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
Требования по ИБ	0.9839	0.9893	0.9893	0.9893	0.9935	0.9893	0.9935	0.9935	0.9935	0.9935	0.9935	0.9935

Табл. П.1. 21.

	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
l_1	0.9917	0.9917	0.9917	0.9929		0.9929		0.9901	0.9835			
l_2	0.9917	0.9917	0.9917	0.9929		0.9929		0.9901		0.9835		
l_3	0.9917	0.9917	0.9917	0.9929		0.9929		0.9901			0.9835	
l_4	0.9917	0.9917	0.9917	0.9929		0.9929		0.9901				0.9835
l_5	0.9917	0.9917	0.9917	0.9929	0.9929			0.9901	0.9835			
l_6	0.9917	0.9917	0.9917	0.9929	0.9929			0.9901		0.9835		
l_7	0.9917	0.9917	0.9917	0.9929	0.9929			0.9901			0.9835	
l_8	0.9917	0.9917	0.9917	0.9929	0.9929			0.9901				0.9835
l_9	0.9917	0.9917	0.9917		0.9929		0.9929	0.9901	0.9835			
l_{10}	0.9917	0.9917	0.9917		0.9929		0.9929	0.9901		0.9835		
l_{11}	0.9917	0.9917	0.9917		0.9929		0.9929	0.9901			0.9835	
l_{12}	0.9917	0.9917	0.9917		0.9929		0.9929	0.9901				0.9835
l_{13}	0.9907	0.9907	0.9907				0.992	0.9889	0.9815			
l_{14}	0.9907	0.9907	0.9907				0.992	0.9889		0.9815		
l_{15}	0.9907	0.9907	0.9907				0.992	0.9889			0.9815	
l_{16}	0.9907	0.9907	0.9907				0.992	0.9889				0.9815

Табл. П. 1. 22.

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
0.9917	0.9917	0.9917	0.9929	0.9929	0.9929	0.9929	0.9901	0.9835	0.9835	0.9835	0.9835

Табл. П.1. 23.

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}
0.9839	0.9893	0.9893	0.9893	0.9935	0.9893	0.9935	0.9935	0.9935	0.9935	0.9935	0.9935
0.9917	0.9917	0.9917	0.9929	0.9929	0.9929	0.9929	0.9901	0.9835	0.9835	0.9835	0.9835
0.9917	0.9917	0.9917	0.9929	0.9935	0.9929	0.9935	0.9935	0.9935	0.9935	0.9935	0.9935

Табл. П.1. 24.

Наименование ТС	Интенсивность атак нарушения доступности ТС
АРМ 2 - АРМ 7	2
АРМ 10 – АРМ 11	2
Сервер	7
Маршрутизатор	7
ЛС1 и ЛС2	2

Табл. П.1. 25.

	С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
z_1	0.9996	0.9996	0.9985	0.9985	0.9985									0.9985	0.9985
z_2	0.9998	0.9998	0.9992	0.9992		0.9992	0.9992	0.9992	0.9992	0.9992	0.9992			0.9992	0.9992
z_3	0.9996	0.9996	0.9987	0.9987		0.9987	0.9987							0.9987	0.9987
z_4	0.9997	0.9997	0.9991	0.9991		0.9991	0.9991					0.9991		0.9991	0.9991
z_5	0.9996	0.9996	0.9986	0.9986										0.9986	0.9986
z_6	0.9996	0.9996	0.9984	0.9984										0.9984	0.9984
z_7	0.9997	0.9997	0.999	0.999								0.999	0.999	0.999	0.999
z_8	0.9997	0.9997	0.999	0.999								0.999	0.999	0.999	0.999
z_9	0.9996	0.9996	0.9986	0.9986										0.9986	0.9986
z_{10}	0.9996	0.9996	0.9986	0.9986										0.9986	0.9986
z_{11}	0.9997	0.9997	0.9988	0.9988									0.9988	0.9988	0.9988
z_{12}	0.9997	0.9997	0.9988	0.9988									0.9988	0.9988	0.9988

Табл. П.1. 26.

С	М	ЛС1	ЛС2	А1	А2	А3	А4	А5	А6	А7	А8	А9	А10	А11
0.9998	0.9998	0.9992	0.9992	0.9985	0.9992	0.9992	0.9992	0.9992	0.9992	0.9992	0.9991	0.999	0.9992	0.9992

Приложение 2. Результаты испытания программных средств информационной безопасности.

Результаты работы сканера безопасности Nessus.

Этот отчет описывает ОИ, которые были испытаны на ИБ.

Детали испытаний

Количество испытаных хостов	3
Количество информационных сообщений	2
Количество предупреждения	3

Список хостов

10.114.9.1	Есть предупреждения
10.114.9.3	Информация
10.114.96.4	Есть предупреждения

Анализ хоста 10.114.9.1

	Порт/Сервис	Тип уязвимости
10.114.9.1	lotusnote (1352/tcp)	Информация
10.114.9.1	ms-wbt-server (3389/tcp)	Предупреждение
10.114.9.1	ms-wbt-server (3389/tcp)	Информация
10.114.9.1	general/tcp	Информация
10.114.9.1	general/icmp	Информация

Подробное описание хоста 10.114.9.1

Тип	Порт	Описание
I	lotusnote (1352/tcp)	Домино сервер (CN=IKARBRP/O=KSTU-KAI) слушает на этом порту
W	ms-wbt-server (3389/tcp)	Диагноз: Возможен доступ на хост. Описние: Версия ПО сервиса Terminal Service позволяет провести атаку типа MITM. Взломщик может использовать эту уязвимость с целью кражы конфиденциальной информации (пароль,

		…). Смотрите так же: http://www.oxid.it/downloads/rdp-gbu.pdf Фактор риска: Средний / CVSS Base Score : 6 (AV:R/AC:H/Au:NR/C:P/A:P/I:P/B:N) CVE : CVE-2005-1794 BID : 13818, Nessus ID : 18405
I	ms-wbt-server (3389/tcp)	Диагноз: Терминальный сервис запущен на хосте. Описание: Терминальный сервер может быть использован для входа в систему. Рекомендации: Остановите его, если в нем нет явной необходимости. Фактор риска: None / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) BID : 3099, 7258 Nessus ID : 10940
I	general/tcp	Nessus не смог точно определит тип ОС. Возможно она принадлежит одному из этих типов: Microsoft Windows 2000 Professional Microsoft Windows 2000 Professional Service Pack 3 Microsoft Windows 2000 Professional Service Pack 4 Microsoft Windows 2000 Server Microsoft Windows 2000 Server Service Pack 2 Microsoft Windows CE Microsoft Windows Mobile 2003 Second Edition Microsoft Windows XP Home Edition Microsoft Windows XP Professional Microsoft XP Professional SP 2, Nessus ID : 11936

I	general/icmp	Диагноз: Возможно определить текущее время на хосте. Описание: Хост отвечает на ICMP запрос времени. Это может позволить взломщику узнать текущее время на хосте. Это может помочь ему прочить все протоколы авторизации. Рекомендации: Фильтруйте входящие и исходящие ICMP пакеты. Фактор риска: Нет / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) CVE : CVE-1999-0524, Nessus ID : 10114

Анализ хоста 10.114.9.3

	Порт/Сервис	Тип уязвимости
10.114.9.3	netbios-ssn (139/tcp)	Нет информации
10.114.9.3	ntp (123/udp)	Информация

Подробное описание хоста 10.114.9.3

Тип	Порт	Описание
I	ntp (123/udp)	NTP (Network Time Protocol) сервис слушает на этом порту. Фактор риска: Низкий, Nessus ID : 10884

Анализ хоста 10.114.96.4

	Порт/Сервис	Тип уязвимости
10.114.96.4	lotusnote (1352/tcp)	Информация
10.114.96.4	ms-wbt-server (3389/tcp)	Предупреждение

Security Issues and Fixes: 10.114.96.4

Type	Port	Issue and Fix
I	lotusnote (1352/tcp)	Domino сервер (CN=IKAR1/O=KSTU-KAI) слушает на этом порту, Nessus ID : 11410

W	ms-wbt-server (3389/tcp)	Диагноз: Возможен доступ на хост. Описние: Версия ПО сервиса Terminal Service позволяет провести атаку типа MITM. Взломщик может использовать эту уязвимость с целью кражы конфиденциальной информации (пароль, …). Смотрите так же: http://www.oxid.it/downloads/rdp-gbu.pdf Фактор риска: Средний / CVSS Base Score : 6 (AV:R/AC:H/Au:NR/C:P/A:P/I:P/B:N) CVE : CVE-2005-1794 BID: 13818 Nessus ID : 18405
I	ms-wbt-server (3389/tcp)	Диагноз: Терминальный сервис запущен на хосте. Описание: Терминальный сервер может быть использован для входа в систему. Рекомендации: Остановите его, если в нем нет явной необходимости. Фактор риска: None / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) BID : 3099, 7258 Nessus ID : 10940

Классификация тестов Nessus.

1. Тесты проверки безопасности операционной системы AIX.

2. Наличие программных закладок, через которые можно беспрепятственно войти в систему (backdoor).

3. Уязвимости в CGI (Common Gateway Interface) скриптах web-серверов.

4. Уязвимости в CGI: XSS (Common Gateway Interface) скриптах web-серверов.

5. Уязвимость аппаратно-программных средств CISCO.

6. Тесты проверки безопасности операционной системы Debian.

7. Проверка имен пользователей задаваемых по умолчанию в операционной системы UNIX.

8. Вывод из стоя служб сервера.

9. Тесты проверки безопасности операционной системы Fedora.

10. Уязвимости в сервисах восстановления информации пользователей.

11. Уязвимости в фаерволах.

12. Тесты проверки безопасности операционной системы FreeBSD.

13. Уязвимости в FTP сервере.

14. Тесты на получение пользовательских полномочий на удаленном сервере.

15. Тесты на получение прав администратора на удаленном сервере.

16. Тесы общие для всех платформ.

17. Тесты проверки безопасности операционной системы Gentoo.

18. Тесты проверки безопасности операционной системы HP-UX.

19. Тесты проверки безопасности операционной системы MacOS.

20. Тесты проверки безопасности операционной системы Mandrake.

21. Проверка версии программного обеспечения.

22. Тесты проверки безопасности операционной системы NetWare.

23. Проверка работоспособности NIS (Сетевой информационный ресурс).

24. Проверка работоспособности ЛВС с распределёнными одноранговыми объектами.

25. Сканирование портов.

26. Тесты проверки безопасности операционной системы Red Hat.

27. Удаленный доступ к файлам.

28. Проверка вызова удаленных процедур (RPC).
29. Определение сервисов удаленного хоста.
30. Рекомендации по настройкам сканера Nessus.
31. Тесты проверки безопасности операционной системы SlackWare.
32. Уязвимости протокола SMTP.
33. Уязвимости протокола SNMP.
34. Тесты проверки безопасности операционной системы Solaris.
35. Тесты проверки безопасности операционной системы SuSE.
36. Тесты проверки безопасности операционной системы Ubuntu.
37. Выявление не используемых процессов.
38. Испытание Web сервера.
39. Тесты проверки безопасности операционной системы Windows.
40. Уязвимости Windows.
41. Уязвимости менеджера пользователей Windows.

Табл. П.2. 1.

№	Вид тестов	К	Ц	Д
1	Тесты проверки настроек безопасности операционных систем: AIX, Debian, Fedora, FreeBSD, Gentoo, HP-UX, MacOS, Mandrake, NetWare, Red Hat, SlackWare, Solaris, SuSE, Ubuntu, Windows.	+	+	+
2	Тесты проверки межсетевых экранов.	+	+	+
3	Тесты проверки аппаратно-программных средств CISCO.	+	+	+
4	Тесты для вывод из стоя служб сервера.		+	+
5	Тесты проверки уязвимостей в CGI скриптах web-серверов (CGI является стандартом интерфейса внешней прикладной программы с Web сервер)	+	+	+
6	Тесты наличия программных закладок	+	+	+

7	Тесты проверки уязвимостей FTP серверов, NIS сервисов (Сетевой информационный сервис), Web – сервера, File – сервера.	+	+	+

Продолжение Табл. П.2. 1.

8	Тесты проверки уязвимостей в сервисах восстановления информации о пользователе.	+		
9	Тесты проверки имен пользователей задаваемых по умолчанию в операционных системах UNIX, Windows.	+	+	+
10	Тесты на получение пользовательских полномочий на удаленном сервере.	+		
11	Тесты на получение прав администратора на удаленном сервере.	+	+	+
12	Тесты проверки работоспособности ЛВС с распределёнными одноранговыми объектами.	+	+	+
13	Тесты проверки службы вызова удаленных процедур (RPC – это механизм, который позволяет программе, работающей на одном компьютере, выполнять программный код на удаленном компьютере).	+	+	+
14	Тесты определения полного списка служб хоста.	+		
15	Тесты определение полного списка не используемых служб хоста.	+		
16	Тесты проверки уязвимостей протоколов SMTP, SNMP.	+	+	+
17	Сканирование портов.	+		
18	Тесты проверки версии программного обеспечения объекта испытания.	+	+	+

В таблице приняты следующие условные обозначения: «К» – конфиденциальность, «Ц» – целостность, «Д» – доступность, «+» – значит, что данная группа тестов может нарушить конфиденциальность или целостность или

доступность данных ОИ, возможен вариант, когда тесты рассматриваемой группы нарушат более одной компоненты ИБ. В этом случае в строке напротив названия группы тестов будет стоять несколько плюсов.

Примеры тестов написанных на NASL.

Пример 1. Ниже приведен теста, который проверит, на всех ли узлах запущен сервис SSH и сообщит пользователю, на каком хосте он не запущен. SSH (Secure Shell) - сетевой протокол, позволяющий производить удалённое управление компьютером и передачу файлов. Он сходен по функциональности с протоколом TELNET и RLOGIN, однако использует алгоритмы шифрования передаваемой информации.

```
if(description)
{ script_name(Russian:"Проверка запуска SSH на удаленном хосте");
script_description(Russian:" Проверка запуска SSH");
script_summary(Russian:"Соединение на удаленный TCP порт 22");
script_category(ACT_GATHER_INFO);
script_family(Russian:"Инструментарий администратора");
script_copyright(Russian:"Этот тест написан Тутубалиным П.И.");
script_dependencies("find_service.nes");
exit(0);}
```

Проверка запуска SSH на другом порту.Поэтому мы обращаемся к дополнительному программному модулю “find_service”

```
port = get_kb_item("Services/ssh");
if(!port)port = 22;
ok = 0; # объявляем, что SSH еще не установлен
if(get_port_state(port))
{soc = open_sock_tcp(port);
if(soc)
{# Проверяем, что SSH сконфигурирован без TCP-Wrapper
#и что это действительно SSH
```

```
data = recv(socket:soc, length:200);
if("SSH" >< data)ok = 1;
}
close(soc);}
# Только предупреждаем пользователя, что SSH НЕ установлен
if(!ok) {
report = "SSH не работает на этом хосте!";
security_warning(port:22, data:report);}
```

Пример 2. Проверка возможности вывода из строя Proxy-сервера (WinProxy), работающего под управление Windows. Proxy-сервер – это система, находящаяся между исполняемыми приложениями (такими, как Internet Explorer) и Internet соединением (Server). Она перехватывает запросы к server-у, рассматривая возможность выполнить их самостоятельно. Что увеличивает быстродействие за счет отсечения повторных запросов одной и той же информации из Internet.

```
if (description) {script_id(20393);
script_version("$Revision: 1.1 $");
script_cve_id("CVE-2005-3187", "CVE-2005-3654", "CVE-2005-4085");
script_bugtraq_id(16147, 16148, 16149);
script_name(Russian:"WinProxy <Множественные уязвимости
(проверка реестра)");
script_summary(Russian: " Проверка с целью выявления уязвимостей
в реестре Windows)");
desc ="Раздел описания проблемы: На удаленном хосте выявлены уязвимости. Раздел подробного описания проблемы: На удаленном сервере под управлением ОС Windows запущен сервис WinProxy. В реестре сервера содержится информация позволяющая провести DoS-атаку и инициировать в сервисе WinProxy ошибку переполнения буфера обмена, что позволит нару-
```

шителю ИБ выполнить произвольный код на сервера. Более подробную информацию можно получить здесь:
http://www.idefense.com/intelligence/vulnerabilities/display.php?id=363
Рекомендации по устранению уязвимости ПО ОИ: Обновит ПО WinProxy до версии 6.1a или выше. Фактор рика: Critical / CVSS Base Score : 10
(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N)";
script_description(Russian:desc);
script_category(ACT_GATHER_INFO);
script_family(Russian:"Уязвимость в процедуре
удаленного администрирования");
script_copyright(Russian:"Все права по использованию данного теста
принадлежат компании Tenable Network Security");
script_dependencies("smb_hotfixes.nasl");
script_require_keys("SMB/Registry/Enumerated");
script_require_ports(139, 445);
exit(0);}
if (!get_kb_item("SMB/Registry/Enumerated")) exit(0);
# Поиск в реестре сведений о службе WinProxy.
name=get_kb_item("SMB/Registry/HKLM/SOFTWARE/Microsoft/
Windows/CurrentVersion/Uninstall/WinProxy 6/DisplayName");
if (name && name =~ "^WinProxy \(Version ([0-5]\.|6\.0)")
{# если версия WinProxy ниже 6.1, то есть обнаружена
security_hole(0); exit(0);}

Список сокращений

АСОИУ – автоматизированная система обработки информации и управления

ИБ – информационная безопасность

СИБ – средство информационной безопасности

НСД – несанкционированный доступ

СОВ– средство обнаружения вторжений

ЭС – экспертная система

ПТИБ – прикладная теория информационной безопасности

ТС – технические средства

АРМ – аппаратное средство

ИТ – информационная технология

ЛГР – лица, готовящие решения

ЛПР – лица, принимающие решения

ЛРР – лица, реализующие решения

КД – конфиденциальные данные

ОИ – объект испытания

АСИ – автоматизированная система испытаний

ПО – программное обеспечение

ОПО – общее программное обеспечение

СПО – специальное программное обеспечение

ИО – информационное обеспечение

ЛО – лингвистическое обеспечение

МФА – модуль формирования атак

СОДЕРЖАНИЕ

Послесловие

Группа компаний FUJITSU

Данная монография издана благодаря спонсорской поддержке предприятия ОАО «ICL-КПО ВС».

ОАО «ICL-КПО ВС» – одно из крупнейших предприятий России, занимающихся системной интеграцией и предоставлением комплексных решений в области компьютерных технологий, обеспечивая консалтинг, проектирование, внедрение, гарантийное и сервисное обслуживание компьютерных систем любого масштаба.

Богатый опыт взаимодействия с отечественными предприятиями, передовые западные методики и лучшая российская практика воплотились в разработках компании, каждая из которых – гибкий и современный инструмент для решения текущих и стратегических управленческих задач организации.

Среди основных направлений деятельности ОАО можно отметить следующие:

- системная интеграция;
- разработка и реализация прикладного программного обеспечения;
- внедрение и сопровождение современных информационных систем;
- производство серверов и персональных компьютеров;
- сервисное обслуживание;
- обучение.

На сайте компании **http://www.icl.ru** вы узнаете о разнообразной научно-производственной деятельности и кадровой работе предприятия, о сотрудничестве с отечественными и зарубежными предприятиями в области новейших информационных технологий.

Поблагодарив ОАО «ICL-КПО ВС» за спонсорскую поддержку в издании данной монографии, пожелаем ему успехов в дальнейшей деятельности.

Адрес: 420029, Казань, Сибирский тракт, д. 34.

Телефон: 8 (843) 273-24-43, Факс: 8 (843) 273-55-35, 272-39-52.