Общее описание процедуры аттестации автоматизированных систем по требованиям информационной безопасности

Александр Астахов

Введение

В современных условиях наиболее перспективным способом проверки достигнутого качества функционирования и уровня защищенности автоматизированных систем (АС) является процедура аттестации. В то время как для многих коммерческих АС аттестация носит добровольный характер, существует достаточно многочисленная категория АС, для которых аттестация, согласно действующему законодательству, является обязательным условием для начала или продолжения их эксплуатации. В их число входят АС, предназначенные для обработки информации, составляющей государственную тайну, для управления экологически опасными объектами и для ведения секретных переговоров.

В России аттестация по существу только начинает внедряться в практику создания и применения АС. В связи с этим существует целый комплекс нерешенных проблем, в числе которых проблемы стандартизации и совершенствования нормативной документации, состоящие в разработке, выборе и адаптации документов, применяемых при аттестации и описывающих процедуру, критерии и методику ее проведения. Целесообразным является использование для решения этих проблем опыта, накопленного мировым сообществом.

В США набор руководящих документов в области аттестации был сформирован еще в начале 80-х годов. Изучение и адаптация этих документов к российским условиям может существенно ускорить процесс создания отечественной нормативной базы. Для федеральных органов США основополагающим документом в области аттестации является Руководство по Проведению Аттестации и Аккредитации безопасности АС (FIPS PUB 102).

Данная работа является попыткой использования отечественного опыта и американской нормативной базы для создания общего руководства по проведению аттестации АС по требованиям безопасности информации.

Используемая терминология

Система аттестации АС является составной частью Единой системы сертификации средств защиты информации (СЗИ) и аттестации объектов информатизации по требованиям безопасности информации, организация функционирования которой осуществляется Гостехкомиссией при Президенте РФ. В соответствии с принятой в нашей стране концепцией защиты информации от несанкционированного доступа (НСД), существует два относительно самостоятельных направления решения этой проблемы: направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с АС. Отличие между этими направлениями заключается в том, что при рассмотрении вопросов защиты СВТ огрганичиваются только программно-техническими аспектами функционирования системы, в то время как защита АС предполагает рассмотрение организационных мер защиты, вопросов физического доступа, защиты информации от утечки по техническим каналам и т. п. СВТ представляют собой программно-технические средства, разрабатываемые и поставляемые на рынок как элементы, из которых строятся АС. Помимо набора СВТ, АС включает в себя обслуживающий персонал и систему организационных мероприятий, обеспечивающих ее функционирование, а также помещения, пользовательскую информацию, бумажную документацию и т. д. Существование двух условно различающихся направлений в защите информации является причиной отличия используемой в нашей стране терминологии от принятой в других странах. Понятие «сертификация по требованиям безопасности» в России применяется по отношению к СВТ, в то время как тот же самый процесс по отношению к АС называется аттестацией. В США в обоих случаях используется понятие «сертификация».

Согласно американским руководящим документам, сертификация по требованиям безопасности — это проводимый независимыми экспертами комплекс организационно-технических меропри-

тий по проверке соответствия реализованных в АС или СВТ механизмов безопасности определенному набору требований. Требования безопасности используются в качестве критерия для оценки уровня защищенности АС или СВТ. Они могут быть сформулированы в руководящих документах органов государственного управления, внутриведомственных и межведомственных приказах, национальных и международных стандартах, стандартизированных профилях защиты или заданиях по безопасности, а также в виде требований конкретной организации или пользователей АС.

Примечание: Для определенности, в остальной части настоящей статьи по отношению к АС будет использоваться принятый в нашей стране термин — аттестация.

В случае положительного результата аттестационных испытаний создается специальный документ — «Аттестат соответствия», в котором подтверждается, что объект испытаний соответствует требованиям стандартов или иных нормативно-технических документов по информационной безопасности. Таким образом, основным продуктом аттестации является аттестат соответствия. Но не менее важным является то, что к проведению обследования и аттестационных испытаний активно привлекается обслуживающий персонал АС, ее разработчики и пользователи, в результате чего повышается их осведомленность в вопросах обеспечения безопасности и общий уровень защищенности АС.

Аттестация АС по требованиям безопасности информации является лишь одним из аспектов общей процедуры аттестации, выполняемой с целью получения гарантий того, что АС удовлетворяет предъявляемым к ней требованиям по функциональности, производительности, безопасности, качеству и надежности функционирования. Поэтому ее лучше всего осуществлять как часть общей процедуры аттестации, охватывающей все требования к эффективности функционирования АС и зачастую использующей те же методы проведения обследования и испытаний.

В американской нормативной документации термин «сертификация» применяется по отношению к программному обеспечению, аппаратным компонентам, приложениям, системам, терминалам, сетям и другим объектам. Природа сертифицируемого объекта оказывает минимальное влияние на общий процесс проведения аттестации, хотя она оказывает существенное влияние на детали выполнения отдельных работ.

В США термином «аккредитация безопасности АС» обозначается основывающаяся на результатах аттестации санкция руководства предприятия, позволяющая использовать АС для обработки жизненно-важной и/или конфиденциальной информации в данной среде функционирования.

Таким образом, аккредитация является официальным разрешением руководства использовать данную АС в данной среде функционирования. Хотя в этом определении фигурируют только «жизненно-важные и/или конфиденциальные данные», предполагается его более широкая трактовка, охватывающая также критичные АС, которые могут и не содержать жизненно-важных и/или конфиденциальных данных. Такие АС считаются критичными скорее из-за того вреда, который может быть нанесен организации в случае отказа в обслуживании этой АС, чем от несанкционированного раскрытия или использования данных.

Критичные АС — это АС, для которых необходима определенная степень защищенности, потому что они обрабатывают критичные данные или существует риск причинения вреда в результате их неправильного функционирования или злоумышленного манипулирования ими.

Все АС имеют определенную степень критичности. Важным вопросом является наличие соглашения о том, для каких АС требуется проводить аттестацию. Желательно иметь упорядоченный по приоритетам список таких АС.

Описание процедуры аттестации

Процедуру аттестации АС можно условно разделить на несколько последовательных этапов: планирование, сбор информации, базовый анализ, детальный анализ, подготовка отчетных документов и аккредитация. Далее рассматривается содержание каждого из этих этапов.

Планирование

План подготовки и проведения аттестации должен определять проблемные области, потребности в специальных знаниях, потребности в инструментарии для поддержки процедуры оценивания и другие вопросы, ответы на которые невозможно дать без проведения соответствующего анализа, характерного для этапа базового оценивания и специфичного для каждой конкретной ситуации. Можно выделить четыре стадии планирования:

- Инициирование.
- Анализ.
- Планирование ресурсов.
- Документирование плана проведения аттестации.

Инициирование

На этапе инициирования осуществляется определение общей схемы проведения аттестации и ее согласование с заказчиком работ. Схема определяет общий порядок выполнения работ и необходимые затраты ресурсов. Рассматриваются следующие вопросы:

1. Назначение, выполняемые функции и структура объекта информатизации; критичность АС и обрабатываемой в ней информации; границы проведения обследования; узкие места и проблемные области; состав и структура комплекса средств защиты; привлечение для проведения работ специалистов различных технических профилей.
2. Оценка временных затрат и затрат ресурсов на проведение работ; наличие результатов ранее проведенного анализа рисков и аудита безопасности, которые можно было бы использовать для определения трудоемкости и объема работ по аттестации.
3. Состав экспертной группы; распределение обязанностей между специалистами.
4. Факторы, оказывающие влияние на качество и глубину аттестационных испытаний.
5. Наличие специфических для данного объекта требований, которые должны использоваться в качестве критерия для проведения аттестации, помимо имеющейся нормативной документации.
6. Наличие и полнота документации, документированность используемых механизмов безопасности.
7. Наличие и документированность политики безопасности организации.

Принятая схема проведения аттестации оформляется в виде Технического задания и Плана-графика работ.

Анализ

Анализ составляет основную часть процесса планирования. В процессе анализа рассматриваются следующие вопросы:

1. Требования безопасности
2. Исходные данные
3. Границы проведения аттестации и распределение работ
4. Области повышенного внимания
5. Требуемый уровень детализации

Анализ требований безопасности

Целью аттестации является проверка соответствия исследуемой АС предъявляемым к ней требованиям безопасности. Поэтому анализ начинается с рассмотрения требований безопасности. Основным критерием для аттестации служат требования, сформулированные в виде руководящих документов Гостехкомиссии РФ, законов РФ, внутриведомственных, межведомственных, национальных и международных стандартов. Для каждой АС рассматривается также набор внутренних требований, которые формулируются по результатам анализа рисков и учитывают специфику и особенности среды функционирования исследуемой АС. Некоторые внутренние требования могут быть очень специфичными для данной АС и касаться критичности данных, ограничений на раскрытие некоторых видов информации и других вопросов безопасности.

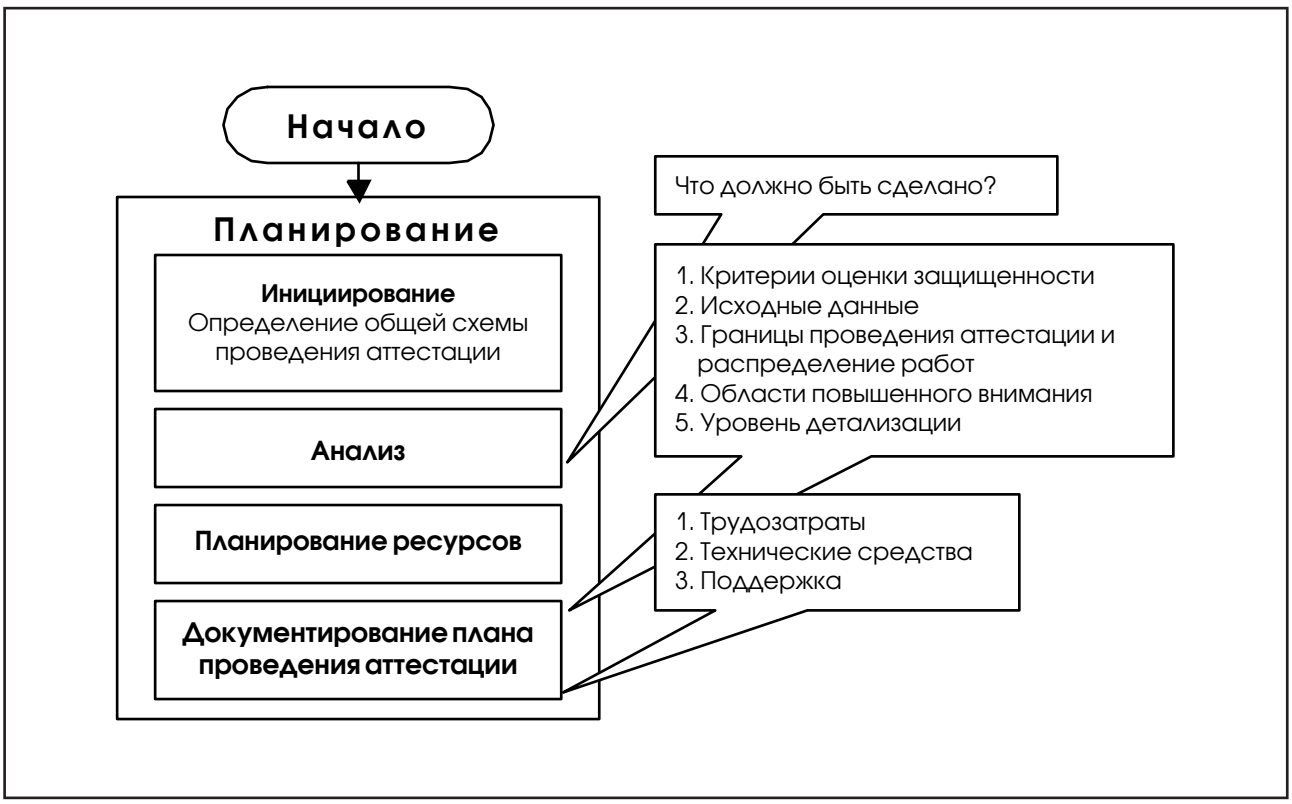

Рис. 1. Планирование процедуры аттестации.

Анализ состава исходных данных

Для разработки программы и методики аттестационных испытаний помимо стандартного перечня исходных данных, содержащегося в РД Гостехкомиссии «Положение по аттестации объектов информатизации по требованиям безопасности информации», необходимо предоставить также дополнительные данные, состав которых уточняется в каждой конкретной ситуации. Например, сообщения об известных слабостях АС, попытках НСД к информации или отчеты о возникших проблемах, полученные в ходе предшествующего периода ее эксплуатации, приводят к необходимости сбора дополнительных сведений из более узких областей.

Руководство организации, владеющей либо эксплуатирующей АС, может иметь собственное мнение по поводу информации, которая может быть предоставлена в качестве исходных данных для аттестации. При планировании эти мнения необходимо учитывать. Например, для обеспечения сохранности коммерческой тайны между заказчиком и исполнителем работ может быть заключено соглашение о конфиденциальности.

Определение границ проведения аттестации и распределение работ

При определении границ проведения аттестации необходимо в равной степени учитывать организационный, физический и программно-технический уровни обеспечения безопасности. В противном случае результаты аттестации не будут отражать реальный уровень защищенности АС. Например, надежные технические методы защиты окажутся бесполезными, если неправильно определен состав административных мероприятий или меры обеспечения физической безопасности являются неадекватными.

После определения границ проведения аттестации необходимо задокументировать предположения относительно среды функционирования. Например, если операционная система не попадает в границы объекта исследования, то нужно задокументировать предположение о том, что ОС обеспечивает достаточный базовый уровень защищенности в таких областях, как изоляция процессов, аутентификация, авторизация, мониторинг, контроль целостности, регистрация и учет событий и т. п. Предположения относительно среды и условий функционирования АС указываются в «Аттестате соответствия» и являются необходимым условием для разрешения обработки в АС критичной либо конфиденциальной информации.

Когда границы проведения аттестации определены, осуществляется распределение ответственности между специалистами экспертной группы. В большинстве случаев в подготовке и проведении аттестационных испытаний требуется участие специалистов различных технических профилей.

При определении состава экспертной группы и распределении работ учитывается ряд характеристик АС. Основные характеристики, на которые обращается внимание, включают количество и сложность программно-технических компонентов АС и их документированность.

Количество и сложность программно-технических компонентов АС определяют объем трудозатрат, необходимый для проведения аттестации. Кроме того, следует учитывать такие характеристики АС, как физическая, логическая или функциональная распределенность ее компонентов.

Документированность АС является важным фактором при планировании процедуры аттестации. Необходимо учитывать наличие описания подсистемы информационной безопасности АС, включая описание механизмов безопасности, комплекса средств защиты и системы организационных мероприятий; делается ли в документации разделение между механизмами безопасности и другими механизмами; документированы ли функциональные требования, имеются ли спецификации системы, тестовая документация, справочные руководства и т. п. Учитывается также полнота представленной документации, ее соответствие текущему состоянию дел, требованиям нормативной и методической документации.

Области повышенного внимания

При проведении аттестационных испытаний основное внимание должно уделяться компонентам и подсистемам, осуществляющим передачу, обработку и хранение критичной информации. Критичность информации определяется величиной возможного ущерба, который может быть нанесен организации в случае нарушения безопасности этой информации.

Помимо критичности информации на определение областей повышенного внимания могут также влиять и другие факторы. Например, меньше внимания может уделяться тем компонентам АС, все уязвимости которых уже хорошо изучены. Однако, существование этих уязвимостей должно найти отражение в документах.

Для определения областей повышенного внимания и концентрации усилий при аттестации могут использоваться различные методы экспертных оценок. Например, широко распространенный метод Дельфи. В качестве исходных данных для принятия решения могут служить результаты проведения аудита безопасности, либо комплексного аудита АС, результаты анализа рисков и данные об имевших место нарушениях безопасности. Уязвимые места, требующие особого внимания, могут быть выявлены по результатам опросов пользователей и обслуживающего персонала.

Требуемый уровень детализации

В большинстве случаев для получения адекватных результатов достаточно провести базовый анализ механизмов безопасности АС, позволяющий

определить общий уровень ее защищенности и степень соответствия требованиям безопасности. Базовый анализ ограничивается уровнем функциональных спецификаций и заключается в проверке наличия в составе системы компонентов, реализующих необходимый набор требований безопасности.

В некоторых ситуациях, по причине высокой критичности обрабатываемой информации или когда механизмы безопасности расположены на нижних уровнях абстракции и невидимы на верхних уровнях, оправдано проведение детального анализа. При детальном анализе не ограничиваются констатацией факта наличия необходимых функций безопасности, но оценивают также эффективность их реализации.

Существует большое количество критериев для определения уровня детализации, используемого при аттестации. В большинстве случаев основными критериями являются: критичность АС, состав исходных данных (например, доступность исходных текстов программ) и размещение механизмов безопасности (используются встроенные или наложенные средства защиты). Другими критериями могут служить: степень детализации, необходимая заказчику, размер и сложность АС, опыт экспертов. Решения, принятые на основании перечисленных выше критериев, могут относиться как ко всей АС, так и к ее отдельным компонентам и подсистемам.

Планирование ресурсов

На основе проведенного анализа осуществляется выделение ресурсов (временных, людских, технических средств и т. п.), необходимых для выполнения намеченных задач. Оценка времени включает не только время, необходимое для решения поставленных задач, но также, и время связанное с решением организационных вопросов при выделении соответствующих ресурсов. Выделение ресурсов производится с учетом возможных незапланированных ситуаций, способных оказать влияние на доступность людских и других ресурсов.

Документирование плана проведения аттестации

На основе проведенного анализа осуществляется подготовка и согласование плана проведения аттестации, который в общем случае включает в себя следующие разделы:

1. Резюме. Включает все необходимые сведения о порядке проведения работ.
2. Введение. Описывает структуру АС и границы проведения обследования, уровень критичности обрабатываемой информации и других ресурсов, группы задач, решаемых системой, и ограничения, накладываемые политикой безопасности, общий график работ, а также критерии для оценки уровня защищенности АС, включая требования нормативных документов и требования, специфичные для данной АС.
3. Распределение ответственности. Определяется организационная структура и обязанности экспертной группы и других участников процедуры аттестации. Определяются обязанности обслуживающего персонала по поддержке процедуры аттестации.
4. Требования безопасности. Определяется набор требований безопасности, используемых в качестве критерия при аттестации. Помимо существующей нормативной базы обычно имеются дополнительные требования, предъявляемые пользователями и политикой безопасности организации и специфичные для исследуемой АС. Универсальным методом для определения требований безопасности, адекватных существующим угрозам, является анализ рисков.
5. Подход к оцениванию. В этом разделе перечисляются задачи, выполняемые при проведении базового анализа и, в случае необходимости, детального анализа. Осуществляется распределение работ между участниками процедуры аттестации. Состав задач сильно зависит от того, находится ли АС на стадии разработки или на стадии эксплуатации. Затрагиваются следующие вопросы: области повышенного внимания, уровни детализации, конкретные задачи и используемые методы проведения испытаний, источники информации.
6. План-график работ. Определяет сроки подготовки промежуточных отчетных документов и исходных данных, сроки проведения совещаний и сроки окончания этапов выполнения работ. Сроки подготовки промежуточных отчетов определяются на основании оценки времени, сделанной на этапе планирования ресурсов.
7. Поддержка. Перечисляются требования к видам административной и технической поддержки процедуры аттестации со стороны обслуживающего персонала и руководства организации.
8. Отчетные документы. Основными отчетными документами являются отчет по результатам предварительного обследования объекта информатизации, программа и методика проведения аттестационных испытаний, протокол испытаний и заключение по результатам испытаний.
9. Приложения. В приложениях приводится структура отчета по результатам аттестационных испытаний, а также информация по методам и средствам, которые использовались при проведении испытаний и анализа или даются ссылки на источники такой информации.

Различия между процедурами аттестации, выполняемыми на стадии разработки АС и на стадии ее эксплуатации, проявляются при рассмотрении деталей выполнения отдельных задач. Например, при тестировании механизмов безопасности, аттестация, проводящаяся на стадии разработки,

располагает только данными тестирования, в то время как на стадии эксплуатации доступны также данные аудита и мониторинга безопасности.

Сбор информации

Большая часть работы, выполняемой при аттестации (включая фазу планирования), заключается в сборе информации. Рассмотрим три основных метода сбора информации:

1. Получение информации от обслуживающего персонала и разработчиков АС.
2. Изучение документации.
3. Проведение опросов.

При проведении аттестации наибольшее количество времени тратится на изучение характеристик АС. При изучении АС рассматриваются два основных вопроса: (1) назначение и принципы функционирования АС, (2) уровень защищенности АС (угрозы безопасности, ресурсы, механизмы защиты, уязвимости). Оба эти вопроса могут быть разрешены при изучении документации и в ходе опросов пользователей и разработчиков АС. Однако, эти способы сбора информации требуют больших временных затрат.

В идеале лучшим источником информации об объекте информатизации является проектная, рабочая и эксплуатационная документация. К сожалению, качество документации часто бывает низким, а иногда она просто отсутствует. С другой стороны, там, где она существует, ее объем может исчисляться сотнями и тысячами страниц печатного текста. Документация также может содержать устаревшие сведения. Механизмы безопасности в документации часто не отделяются от других механизмов или вообще не описываются. Поэтому существующая документация зачастую трудна для изучения и не содержит достаточного количества исходных данных для аттестации.

Метод проведения опросов также не лишен недостатков. Одним из основных недостатков этого метода является то, что для получения необходимой информации требуются значительные затраты времени. Типичный опрос требует, по крайней мере, один человеко-день работы, включая время его подготовки и документирования, и отнимает время и у проводящих опрос, и у опрашиваемых.

Наиболее эффективным методом сбора информации об АС является метод, при котором руководство организации, разрабатывающей либо эксплуатирующей АС, ставит перед ее разработчиками или обслуживающим персоналом задачу подготовить эту информацию и представить ее в экспертную группу.

Для проведения аттестационных испытаний должны быть подготовлены следующие документы:

1. Документы, содержащие требования безопасности.
2. Отчет по результатам анализа рисков.
3. Диаграммы информационных потоков приложений.

Документы, содержащие требования безопасности

Требования безопасности являются критерием для проведения аттестации. Если требования безопасности не были должным образом сформулированы, то это делается в ходе аттестации. Формулировка требований является результатом совместной работы специалистов, осуществляющих поддержку АС, и экспертов, проводящих ее аттестацию. Участие экспертов, проводящих аттестацию, необходимо по той причине, что у специалистов по поддержке АС недостаточно знаний в области информационной безопасности, особенно в отношении нормативной и правовой базы. Участие специалистов по поддержке АС необходимо по причине недостаточного понимания экспертами, проводящими аттестацию, особенностей функционирования АС, а также требований пользователей.

Типичный набор руководящих документов, используемых при аттестации АС в нашей стране, включает в себя, но не исчерпывается, следующими документами:

- Закон РФ от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации»;
- Закон РФ от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене»;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

Рис. 2. Сбор информации для аттестации.

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации», Гостехкомиссия России, 1997;
- «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1992.

Из перечисленных нормативных документов последние два имеют особое значение для аттестации.

Руководящий документ (РД) Гостехкомиссии РФ «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий первый. Классы подразделяются на четыре группы, отличающиеся уровнем защищенности:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию АС, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. Определяющими признаками, по которым производится группировка АС в различные классы, являются:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС — коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

Кроме этого, в зависимости от характера АС, могут использоваться другие руководящие документы Гостехкомиссии РФ, содержащие требования, предъявляемые к конкретным классам СВТ, входящим в состав АС.

Отчет по результатам анализа рисков

Анализ рисков на объекте информатизации проводится с целью обоснования требований безопасности, предъявляемых к АС, уточнения состава этих требований и выработки системы контрмер, необходимых для успешного противодействия существующим в данной среде угрозам безопасности. Отчет по результатам анализа рисков содержит описание ресурсов АС, оценку их критичности, описание существующих угроз и уязвимостей, оценку ущерба, связанного с осуществлением угроз, и оценку рисков. Оценка рисков определяется вероятностью осуществления угрозы, величиной уязвимости и величиной возможного ущерба, причиняемого организации в случае успешного осуществления угрозы. Проведение анализа рисков требует деятельного участия специалистов, отвечающих за эксплуатацию АС.

Диаграммы информационных потоков приложений

Диаграммы информационных потоков приложений описывают входные, выходные и внутренние информационные потоки приложений, выполняющихся в рамках АС. Диаграммы информационных потоков необходимы для понимания принципов функционирования АС. Этот документ готовится при участии специалистов, отвечающих за поддержку АС.

Описание механизмов безопасности АС

К механизмам безопасности относится любая реализация защитных мер, включая организационный, физический и программно-технический уровни, а также любые действия и процедуры, уменьшающие вероятность нарушения безопасности АС.

Документы, содержащие описание механизмов безопасности АС, полученные от разработчиков или обслуживающего персонала АС, должны подкрепляться изучением документации и проведением опросов.

Базовый анализ

Аттестация может проводиться на двух уровнях детализации: базовый анализ и детальный анализ. Основное отличие между базовым и детальным анализом заключается в том, что базовый анализ концентрируется главным образом на общих функциональных возможностях обеспечения безопасности АС, а не на особенностях отдельных защитных меха-

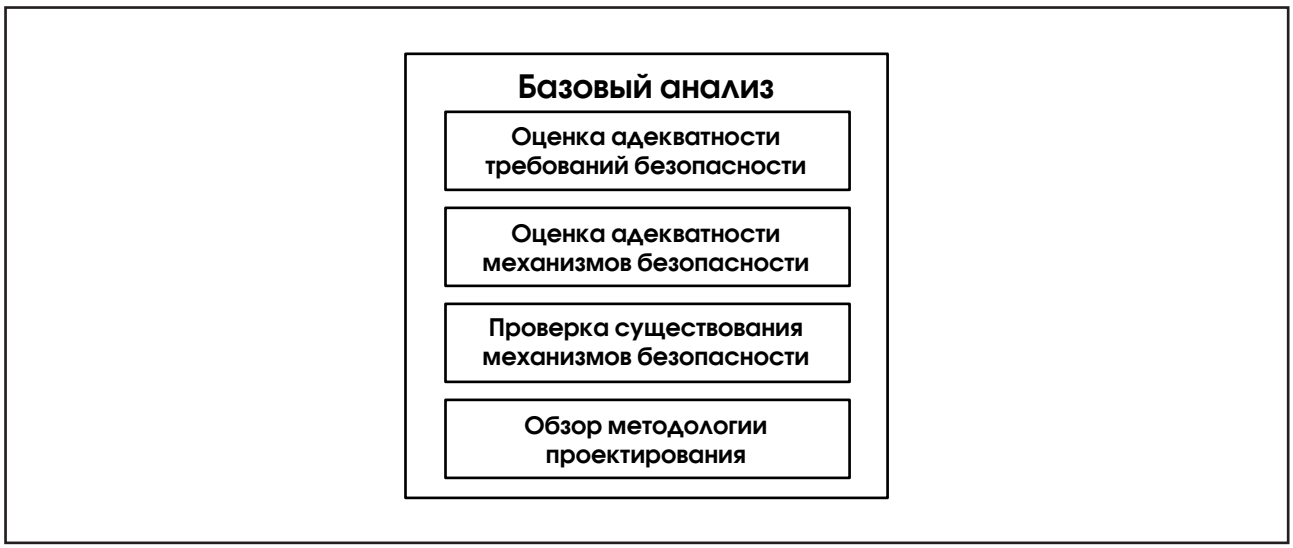

Рис. 3. Этапы базового анализа АС

низмов. Например, при базовом анализе определяется, является ли достаточным контроль доступа на уровне файлов или на уровне отдельных записей; достаточно ли осуществлять аутентификацию на уровне хостов или на уровне пользователей. При базовом анализе также проверяется существование механизмов безопасности. При детальном анализе проверяется правильность функционирования механизмов безопасности, удовлетворяют ли они критерию производительности, являются ли они достаточно надежными и их устойчивость к попыткам взлома.

В ходе базового анализа решаются следующие основные задачи:

1. Оценка адекватности требований безопасности.
2. Оценка адекватности механизмов безопасности.
3. Проверка существования механизмов безопасности.
4. Обзор методологии реализации механизмов безопасности.

Оценка адекватности требований безопасности

Основной целью аттестации является проверка соответствия механизмов безопасности АС предъявляемым к ним требованиям. Поэтому требования безопасности должны быть четко определены и должны быть адекватны существующим рискам. Для большинства АС не существует четко определенного набора адекватных требований безопасности.

На этапе базового анализа существующие требования безопасности должны быть критически исследованы с целью определения их пригодности для целей аттестации и соответствия ожиданиям пользователей, политике безопасности организации, законодательной и нормативной базе. Основная часть требований может содержаться в техническом задании на создание АС.

Если требования безопасности ранее не были определены и документированы, то их необходимо сформулировать и документировать в процессе анализа рисков.

Как при определении, так и при оценке адекватности требований безопасности рассматриваются два класса требований: общие требования и требования, специфичные для исследуемой АС. Общие требования формулируются на основе федеральных законов, руководящих документов государственных органов, стандартов и политики безопасности организации. Специфичные требования формулируются в процессе анализа рисков.

Мероприятия по анализу и управлению рисками

Анализ рисков — это то, с чего должно начинаться построение любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности АС, целью которых является определение того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками. Ниже раскрываются сущность и содержание мероприятий по анализу и управлению рисками.

Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам АС в случае осуществления угрозы безопасности.

Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину, т. е. дать им количественную оценку. Его можно разделить на несколько последовательных этапов:

- Идентификация ключевых ресурсов АС.
- Определение важности тех или иных ресурсов.
- Идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз.

- Вычисление рисков, связанных с осуществлением угроз безопасности.

Ресурсы АС можно разделить на три категории:

- Информационные ресурсы.
- Программное обеспечение.
- Технические средства.

В каждой категории ресурсы можно разделить на классы и подклассы. Необходимо идентифицировать только те ресурсы, которые определяют функциональность АС и существенны с точки зрения обеспечения безопасности.

Важность (или стоимость) ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса. В ходе оценки стоимости ресурсов определяется величина возможного ущерба для каждой категории ресурсов:

- Данные были раскрыты, изменены, удалены или стали недоступны.
- Аппаратура была повреждена или разрушена.
- Нарушена целостность ПО.

Типичные угрозы безопасности включают в себя:

- локальные и удаленные атаки на ресурсы АС;
- стихийные бедствия;
- ошибки персонала;
- сбои в работе АС, вызванные ошибками в ПО или неисправностями аппаратуры.

Под уровнем угрозы понимается вероятность ее осуществления.

Оценка уязвимостей предполагает определение вероятности успешного осуществления угроз безопасности. Успешное осуществление угрозы означает нанесение ущерба ресурсам АС. Наличие уязвимостей в АС обусловлено слабостями защиты.

Таким образом, вероятность нанесения ущерба определяется вероятностью осуществления угрозы и величиной уязвимости.

Величина риска определяется на основе стоимости ресурса, уровня угрозы и величины уязвимости. С увеличением стоимости ресурса, уровня угрозы и величины уязвимости возрастает и величина риска. На основе оценки величины рисков определяются требования безопасности.

Задача управления рисками включает выбор и обоснование выбора контмер, позволяющих снизить величину рисков до приемлемого уровня. Управление рисками включает в себя оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контмер и величиной возможного ущерба должна быть тем больше, чем меньше вероятность причинения ущерба.

Контрмеры могут способствовать уменьшению величины рисков различными способами:

- уменьшая вероятность осуществления угроз безопасности;
- ликвидируя уязвимости или уменьшая их величину;
- уменьшая величину возможного ущерба;
- выявляя атаки и другие нарушения безопасности;
- способствуя восстановлению ресурсов АС, которым был нанесен ущерб.

При выполнении работ по анализу и управлению рисками в компании Инфосистемы Джет используется методика CRAMM и соответствующие инструментальные средства. Метод CRAMM (the UK Government Risk Analysis and Management Method) используется начиная с 1985 г. правительственными и коммерческими организациями Великобритании. За это время он приобрел популярность во всем мире.

CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа защищенности?». На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

Методика CRAMM для каждого этапа определяет набор исходных данных, последовательность мероприятий, анкеты для проведения опросов, списки проверки и набор выходных документов (отчетов).

Единые критерии оценки безопасности информационных технологий

В основе аттестации АС в настоящее время лежат «Единые критерии оценки безопасности ИТ» (Common Criteria for Information Technology Security Evaluation). «Единые критерии» — это нормативный документ, определяющий требования безопасности, на основании которых проводится оценка уровня защищенности продуктов ИТ, общий набор понятий, структур данных и язык для формулирования вопросов и утверждений относительно безопасности продуктов ИТ.

Международная организация по стандартизации (ISO) начала разработку критериев оценки защищенности в 1990 году. Затем авторы канадского (CTCPEC), европейского (ITSEC) и американских (FC и TCSEC) критериев оценки защищенности в 1993 году объединили свои усилия и начали разработку проекта «Единых критериев». Целью проекта было устранение концептуальных и технических различий между существующими критериями. 1 декабря 1999 года версия 2.1 «Единых критериев» была принята ISO в качестве международного стандарта ISO 15408.

В «Единых критериях» определен ряд ключевых понятий, лежащих в основе концепции оценки защищенности продуктов ИТ. Среди них понятие Профиля защиты (PP — Protection Profile), Задания по безопасности (ST — Security Target) и Объекта оценки (TOE — Target of Evaluation). В качестве Объекта оценки может выступать любое СВТ или АС.

PP представляет собой жестко структурированный документ, содержащий требования безопасности для определенного класса программно-технических средств. Помимо требований безопасности PP описывает множество угроз безопасности и задач защиты, а также содержит обоснование соответствия между угрозами безопасности, задачами защиты и требованиями безопасности.

ST представляет собой жестко структурированный документ, определяющий, помимо требований безопасности, функциональную спецификацию механизмов безопасности конкретного продукта ИТ. Содержащиеся в ST требования безопасности определяются при помощи ссылок на соответствующие Профили защиты и требования «Единых критериев». Специфичные для конкретного продукта ИТ требования формулируются отдельно и также включаются в ST. Кроме этого, ST содержит обоснование соответствия между требованиями безопасности и функциональной спецификацией TOE.

В «Единых критериях» представлены две категории требований безопасности: функциональные требования и требования адекватности (гарантированности) механизмов безопасности. Функциональные требования определяют совокупность функций TOE, обеспечивающих его безопасность. Адекватность — это свойство TOE, дающее определенную степень уверенности в том, что механизмы безопасности TOE достаточно эффективны и правильно реализованы. Выводы об адекватности TOE делаются на основании знаний о спецификации, реализации и функционировании TOE. Для выражения функциональных требований и требований адекватности в «Единых критериях» используется единая терминология и стиль.

Аттестация — сложный, длительный и очень ресурсоемкий процесс. Из-за невозможности произвести формальную верификацию или исчерпывающее тестирование всей АС, приходится говорить лишь о достижении определенного уровня адекватности (гарантированности) результатов аттестационных испытаний. В «Единых критериях» вводится единая шкала уровней адекватности оценки (EAL — Evaluation Assurance Level). Каждый EAL представлен определенной совокупностью требований адекватности «Единых критериев».

Вводится семь уровней адекватности оценки: EAL1, EAL2, ..., EAL7. Эти уровни упорядочены по возрастанию. Минимальный уровень адекватности — EAL1 (функциональное тестирование) предоставляет минимальные гарантии адекватности путем проведения анализа механизмов безопасности с использованием спецификаций функций и интерфейса TOE, сопровождаемого независимым тестированием каждого механизма безопасности по методу «черного ящика». EAL1 предназначен для обнаружения только самых очевидных уязвимостей защиты при минимальных издержках. Он применим в тех случаях, когда отсутствуют серьезные риски, связанные с безопасностью. Максимальный уровень адекватности — EAL7 (формальная верификация проекта и тестирование) характеризуется использованием при проектировании комплекса средств защиты формальной модели, формального представления функциональных спецификаций, полуформального представления проекта нижнего уровня и формальной или полуформальной демонстрации соответствия между ними. Анализы сопровождаются независимым тестированием механизмов безопасности по методу «белого ящика». Уровень EAL7 представляет верхнюю границу уровней адекватности оценки АС, которую реально достичь на практике. Его использование следует рассматривать только в качестве экспериментального для аттестации простых и особо критичных АС.

Согласно «Единым критериям» этапы оценки защищенности TOE определяются, исходя из различных уровней абстракции представления: угрозы безопасности → задачи защиты → требования безопасности → спецификация → реализация.

Выделяют два основных этапа проведения оценивания:

1. Оценка базовых Профилей защиты.
2. Анализ Объекта оценки.

Оценка базовых Профилей защиты включает анализ угроз безопасности, задач защиты, требований безопасности и установку соответствия между ними.

Анализ Объекта оценки проводится в два этапа: *Оценка Задания по безопасности и Оценка TOE*.

Оценка Задания по безопасности имеет целью демонстрацию того, что спецификация (формальное, полуформальное или неформальное описание) механизмов безопасности полностью отвечает требованиям Профиля защиты и является пригодным для использования в качестве основы для оценивания TOE;

Оценка TOE заключается в проверке соответствия реализации TOE его спецификации, содержащейся в Задании по безопасности.

Анализ механизмов безопасности

Используемая методика анализа механизмов безопасности зависит от того, имеется ли четко определенный набор требований безопасности либо по тем или иным причинам он отсутствует.

Когда требования безопасности определены

Когда требования безопасности определены и задокументированы, основной задачей этапа базо-

вого анализа становится проверка соответствия реализованных в АС механизмов безопасности этим требованиям. При проведении испытаний АС используются списки проверки, которые содержат, например, следующие вопросы: Обеспечен ли индивидуальный учет пользователей? Идентифицированы ли субъекты и объекты и присвоены ли им метки доступа? Обеспечивается ли режим доступа к данным «только на чтение»? Выполняется ли регистрация всех попыток доступа к файлам? Имеются планы восстановления работоспособности и реагирования на попытки НСД? и т. п.

Требования безопасности могут быть сформулированы с различной степенью детализации. В некоторых случаях требования только определяют необходимость наличия некоторого механизма безопасности, например, такого, как аутентификация удаленных пользователей. В других случаях требования могут определять необходимость использования конкретной схемы аутентификации. В обоих ситуациях проверяется наличие соответствующих механизмов безопасности и их адекватность существующим угрозам.

Когда требования безопасности не определены

Бывают ситуации, когда требования безопасности не могут быть четко определены. Например, когда требуется обеспечить защиту ресурсов корпоративной сети от сетевых атак, то практически невозможно идентифицировать все способы возможных атак, от которых требуется защищаться. В таких ситуациях целесообразно использовать методы активного тестирования механизмов безопасности АС. Эти методы основаны на оценке эффективности противодействия механизмов безопасности определенным видам угроз. Например, активное тестирование механизмов контроля доступа выполняется путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную). Для поиска известных уязвимостей защиты АС используются различные автоматизированные средства анализа защищенности, наиболее распространенными из которых являются сетевые сканеры.

Большинство методов оценки требований безопасности также годятся и в данной ситуации. Однако, без четко сформулированных требований трудно определить адекватность механизмов безопасности.

Уровень детализации

Важным вопросом анализа механизмов безопасности является выбор уровня детализации. В общем случае базовый анализ должен выполняться на функциональном уровне. Функциональный уровень — это уровень абстракции, представленный спецификациями функций АС. Это относится как к внутренним механизмам безопасности, так и к внешним (физическим и административным мерам защиты), хотя последние обычно не определяются в функциональных спецификациях.

Для многих АС функциональных спецификаций просто не существует, либо они бывают неполны. Поэтому экспертам для того, чтобы определить функциональные спецификации АС, приходится изучать принципы ее функционирования, проектную и эксплуатационную документацию.

Проверка существования механизмов безопасности

На этапе базового анализа проверяется существование механизмов безопасности, представленных функциональными спецификациями АС. Установить факт существования большинства физических и административных мер защиты можно простой визуальной проверкой и проверкой наличия соответствующей организационно-распорядительной документации. Для проверки наличия механизмов безопасности, реализованных программными или техническими средствами, необходимо проведение тестирования. При тестировании не ставится задача определения качества функционирования защитных механизмов, т. к. это выходит за рамки базового анализа. С другой стороны, в случае наличия серьезных недостатков, ставящих под вопрос общую эффективность комплекса средств защиты АС, качество реализации защитных механизмов должно учитываться. Обычно для проверки наличия механизмов безопасности бывает достаточно проведения тестирования по методу «черного ящика».

Обзор методологии реализации механизмов безопасности

Проверка существования механизмов безопасности не дает гарантий эффективности функционирования этих механизмов. Лучшим способом получить определенные гарантии, не погружаясь в тестирование и детальные анализы, является рассмотрение методологии, использовавшейся при разработке АС. Рассмотрение методологии производится независимо от того, находится ли АС на этапе разработки или эксплуатации.

Обзор методологии позволяет судить о степени надежности реализации механизмов безопасности и о вероятности наличия брешей в защите АС. Недостатки используемых методов проектирования и разработки приводят к ошибкам в реализации АС. Если в результате анализа методологии установлено, что качеству реализации доверять нельзя, то, обычно, требуется проведение детального анализа для поиска конкретных ошибок в реализации АС.

Американские источники, посвященные методологии разработки средств защиты информации, содержат множество государственных стандартов, устанавливающих порядок разработки и анализа защищенности критичных АС и ПО.

В нашей стране Гостехкомиссией РФ был принят РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ», определяющий следующие основные вопросы:

- организационную структуру и порядок проведения работ по защите информации от НСД и взаимодействия при этом на государственном уровне;
- систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;
- порядок разработки и приемки защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;
- порядок приемки указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля за работоспособностью этих средств и систем в процессе эксплуатации.

Повышенное внимание во время обзора методологии уделяется следующим вопросам:

1. Полнота и качество проектной и эксплуатационной документации.
2. Наличие четко определенных требований к проектированию АС.
3. Используемые методы управления проектом. Наличие у разработчиков методики анализа и тестирования механизмов безопасности АС.
4. Используемые в процессе создания АС методы пректирования. Учет основных принципов архитектурной безопасности. Используемые стандарты и технологии программирования.
5. Осведомленность разработчиков АС в вопросах информационной безопасности. Учет требований безопасности на этапах проектирования и реализации.

Детальный анализ

Во многих случаях для проведения аттестации бывает недостаточно одного базового анализа. Примерами могут служить случаи, при которых (1) во время базового анализа обнаруживаются проблемы, требующие проведения дальнейших исследований; (2) АС имеет высокую степень критичности; или (3) основные механизмы безопасности встроены во внутренние функции, которые не видны на функциональном уровне. В подобных случаях требуется проведение детального анализа.

Детальный анализ концентрируется на оценке эффективности реализации механизмов безопасности. АС исследуется с трех точек зрения:

1. Оценка правильности функционирования механизмов безопасности.
2. Оценка эксплуатационных характеристик, таких как надежность и производительность.
3. Оценка устойчивости к попыткам взлома.

При детальном анализе используется множество подходов, выбор которых определяется скорее существующими угрозами и их последствиями, чем общими характеристиками и критичностью АС. Например, если главной задачей является обеспечение конфиденциальности закрытой информации, основной упор делается на контроле доступа к этой информации и закрытии ее содержания при помощи криптографических средств. Организации, предоставляющие пользователям критичные сервисы, должны сконцентрировать свои усилия, прежде всего, на вопросах доступности этих сервисов. Если главной задачей приложения является обработка клиентских счетов, то особое внимание должно быть уделено механизмам контроля целостности данных.

Подходы к проведению детального анализа

Проверка правильности функционирования механизмов безопасности

При проверке правильности функционирования механизмов безопасности ставится задача оценить, выполняют ли защитные механизмы возложенные на них функции. Наиболее часто для решения этой задачи используются различные методы тестирования.

При тестировании защитных механизмов изучаются следующие вопросы:

1. Работоспособность механизмов безопасности.
2. Проверка правильности обработки недопустимых параметров функций.
3. Обработка исключительных ситуаций.
4. Мониторинг механизмов безопасности и регистрация событий, связанных с безопасностью.
5. Проверка правильности функционирования средств администрирования.

Механизмы безопасности АС должны быть адекватно защищены как от ошибок пользователей, так и от внутренних ошибок. Следовательно, при тестировании особое внимание должно уделяться системным интерфейсам, через которые могут распространяться эти ошибки:

1. человек-человек (сообщения оператора);
2. человек-система (команды, процедуры);
3. система-система (внутренние функции системы);
4. процесс-система (системные вызовы);
5. процесс-процесс (межпроцессорное взаимодействие).

Здесь может использоваться большинство известных методов тестирования. Тестирование может быть либо внешним (метод «черного ящика»), либо внутренним (метод «белого ящика», тестирова-

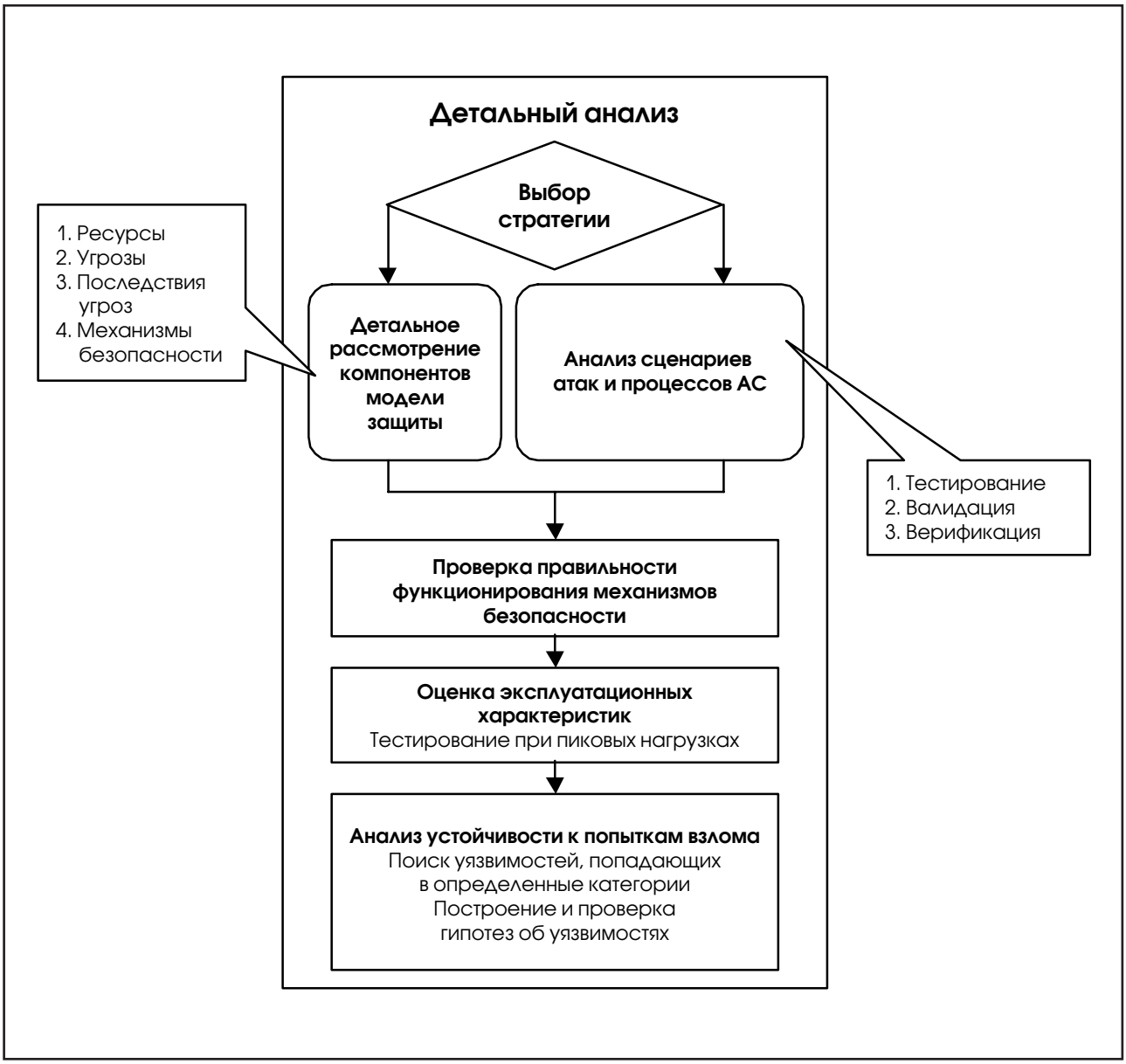

Рис. 4. Детальный анализ механизмов безопасности АС

ние отдельных программных модулей и связей между модулями), в зависимости от типа интерфейса, который подвергается тестированию. Тестирование может быть выполнено группой экспертов, проводящих анализ, разработчиками, пользователями или смешанным коллективом.

Когда тестирование внутренних интерфейсов выполняется независимо от разработчика АС, оно может быть связано с определенными техническими проблемами. Может потребоваться написание фиктивных подпрограмм (пустышек), инструментарий для генерации и сбора тестовых данных и множество вспомогательного программного обеспечения. Может потребоваться инструментарий для разработки ПО, специально приспособленный для конкретной ОС или конкретной АС. Идеальным решением является использование средств, при помощи которых АС первоначально разрабатывалась.

Помимо тестирования, существуют также другие методы анализа, которые можно использовать для проверки правильности функционирования механизмов безопасности.

В качестве одного из методов при проведении детального анализа может использоваться формальная верификация. Формальная верификация дает возможность математически точно доказать соответствие реализации функций безопасности АС на языке программирования ее формальной спецификации.

Представляется весьма перспективным использование автоматизированных систем доказательства корректности программ. К настоящему времени существует уже более двадцати подобных систем. Каждая из этих систем разрабатывалась для верификации широкого класса программ определенной предметной области. В их основе лежат разные математические аппараты и разные принципы

функционирования. Однако можно выделить компоненты, необходимые любой подобной системе:

1. Язык формальной спецификации.

   На этом языке описываются входные и выходные данные (структуры данных, абстрактные типы данных).

2. Язык программирования.

   На этом языке пишется программа. Для того, чтобы правильность этой программы можно было доказать, семантика этого языка должна быть формально определена.

3. Блок синтаксического анализа.

   На вход этого блока поступает уже аннотированная программа, т. е. программа на языке программирования вместе с ее спецификацией на языке спецификации. Блок синтаксического анализа осуществляет синтаксический контроль и преобразует программу к специальному виду, удобному для дальнейшей обработки.

4. Генератор условий корректности (генератор теорем).

   Выдает список условий корректности на вход блока доказательства. Реализует алгоритмы обратного и прямого прослеживания.

5. Блок доказательства теорем.

   Является наиболее сложным. Он выдает список упрощенных условий корректности на вход блока анализа выхода, среди которых выделены доказанные условия. Блок доказательства имеет дополнительный вход, на который подается информация от пользователя в виде аксиом.

6. Блок анализа выходных данных.

   Осуществляет, совместно с пользователем, анализ списка условий корректности. Если все условия доказаны, то входная программа частично корректна.

Например, система FDM позволяет пользователю написать спецификацию формальной модели (включая инварианты и ограничения по безопасности) на языке спецификации Ina Jo, а генератор теорем автоматически генерирует теоремы (критерий правильности), которые должны быть доказаны, чтобы гарантировать, что спецификация верхнего уровня соответствует модели. Генератор теорем также автоматически генерирует теоремы, которые необходимо доказать, чтобы гарантировать, что спецификация каждого нижележащего уровня следует из спецификации более высокого уровня.

Система AFFIRM доказывает корректность программ на языке Паскаль, расширенных за счет абстрактных типов данных. Основная особенность системы — использование базы данных и модуля доказательства в эквациональных теориях на основе алгоритма Кнута-Бендикса. Модуль применяется для доказательства свойств абстрактных типов данных, аксиоматизированных посредством равенств. База данных используется для хранения аксиом и свойств абстрактных типов данных, установленных с помощью канонических систем подстановок термов, а также для хранения промежуточных утверждений, возникающих в процессе доказательства условий корректности. Система AFFIRM включает также модуль доказательства теорем в процессе диалога с пользователем, который выбирает стратегию доказательства. Этот модуль базируется на универсальном методе доказательства теорем (метод естественного вывода, включающий правило индукции) и в процессе работы использует информацию из базы данных. Задача синтеза инвариантов циклов в этой системе возлагается на пользователя.

Существуют успешные примеры применения автоматизированных систем доказательства корректности программ для верификации механизмов безопасности. Например, в проекте защищенной операционной системы UNIX, выполненном в Калифорнийском университете в городе Лос-Анжелес (UCLA), для проверки механизмов защиты данных от несанкционированного доступа использовались методы формальной спецификации и верификации. В этом проекте для доказательства правильности программного кода использовался генератор условий корректности для языка Паскаль системы AFFIRM. Доказательства условий правильности уровня проектирования были выполнены вручную, однако, система AFFIRM использовалась для проверки части этих доказательств.

Формальные методы из-за своей трудоемкости, высокой стоимости и недостаточной изученности пока не получили широкого распространения. Однако, они используются при разработке и верификации механизмов контроля вооружений, космических аппаратов и других АС, связанных с высоким риском. Эти методы в перспективе будут играть более важную роль при проведении аттестации.

Оценка эксплуатационных характеристик

Эффективность механизмов безопасности определяется не только корректностью их функционирования. Многие показатели, определяющие эффективность, можно отнести к общей категории под названием «эксплуатационные характеристики», которая является второй областью исследования при детальном анализе. К показателям эффективности относятся: надежность, отказоустойчивость, восстанавливаемость, время реакции и производительность. Они применимы как к отдельным механизмам, так и к АС в целом.

Тестирование является лучшим способом оценки эксплуатационных характеристик, при этом для измерения каждого показателя эффективности необходимы специальные виды тестов. Употребительным методом является тестирование на пиковых нагрузках. Для создания пиковых нагрузок требуется создание множества запросов на обслужива-

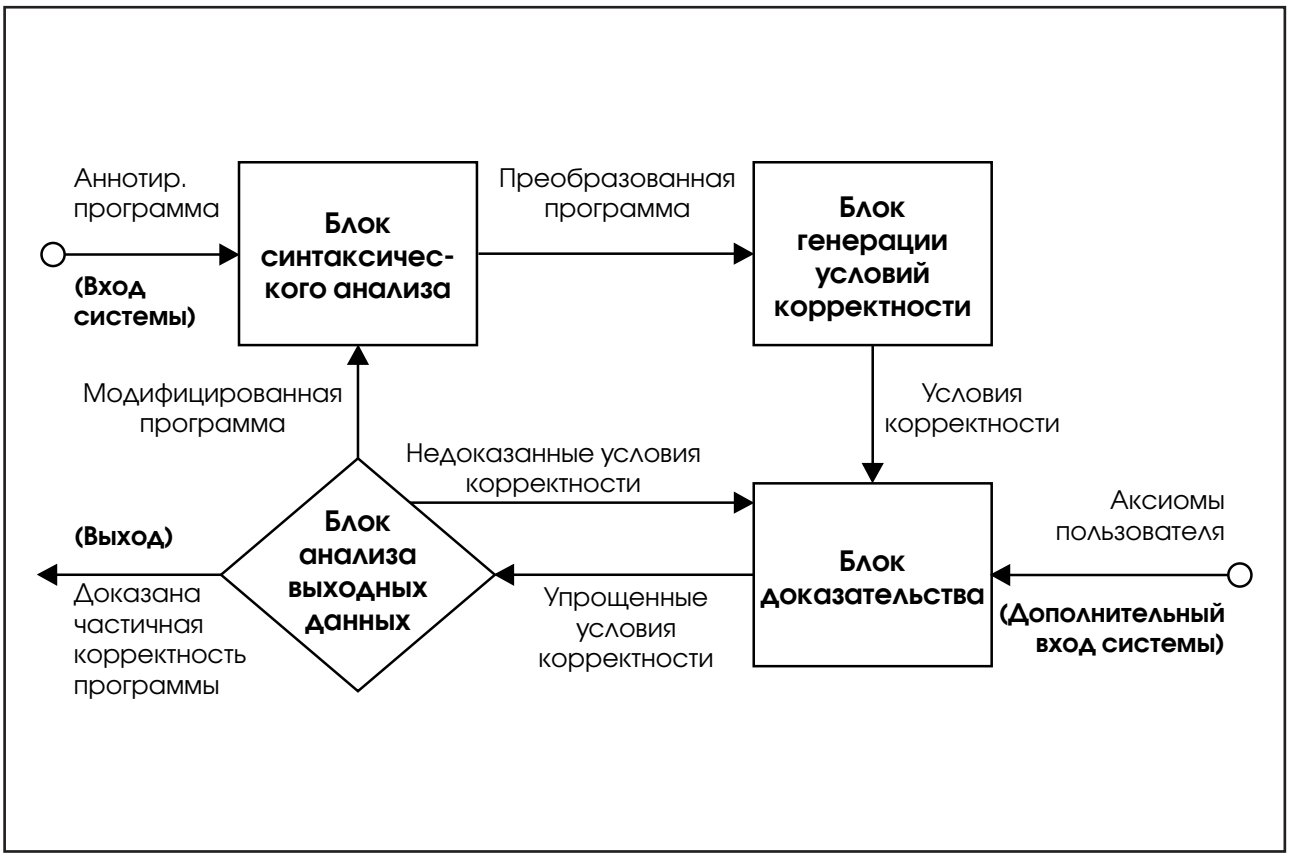

Рис. 5. Обобщенная схема автоматизированной системы доказательства корректности программ

ние, использование большого количества фоновых процессов и задействование максимального количества системных ресурсов. Этот метод годится и для тестирования механизмов безопасности, т. к. в процессе эксплуатации пиковые нагрузки часто перемежаются с нормальной работой.

Тестирование при пиковых нагрузках также используется в более направленной манере, путем осуществления попыток исчерпать квоты на использование конкретных системных ресурсов, таких как буферы, очереди, таблицы, порты и т. п. Направленное тестирование при пиковых нагрузках особенно полезно при оценке устойчивости АС к отказам в обслуживании.

Устойчивость к попыткам взлома

При использовании этого подхода ставится задача оценить устойчивость механизмов безопасности АС к попыткам их взлома или обхода. Устойчивость — это способность АС блокировать и оперативно реагировать на возможные атаки. Методы криптоанализа, например, могут использоваться для взлома конкретного механизма безопасности — шифрования. Создание и использование перехватчика паролей — это пример обхода механизмов безопасности.

Используемые методы анализа устойчивости АС определяются моделью нарушителя. В соответствии с моделью нарушителя обычно все потенциальные нарушители делятся на две категории: внешние и внутренние. В качестве внутреннего нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень (уровень пользователя) определяет самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень (уровень прикладного программиста) определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень (уровень администратора) определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы, на состав и конфигурацию ее оборудования.

Четвертый уровень (уровень системного программиста или разработчика АС) определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Внешние нарушители по уровню своих возможностей также могут подразделяться на уровни.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

Понятие устойчивости к попыткам взлома относится не только к атакам на данные, но также к атакам, направленным против физических и программных ресурсов АС.

Оценка устойчивости к попыткам взлома может оказаться технически наиболее сложной задачей при детальном анализе. Эта часть анализа производится с целью повышения уровня гарантированности, а также поиска и устранения брешей в защите АС. Однако, опыт показывает неадекватность метода «найти и устранить» для обеспечения безопасности. Здесь выделяются три задачи:

1. Оценка устойчивости АС к попыткам взлома.
2. Определение величины уязвимостей (с какими трудностями связано использование брешей в защите).
3. Демонстрация возможностей использования брешей в защите.

Существует несколько подходов к анализу устойчивости АС:

1. Поиск уязвимостей, попадающих в определенную категорию или соответствующих определенному шаблону.
2. Построение гипотезы о наиболее характерных уязвимостях и определение того, существуют ли они в данной программе.

Хотя эти подходы применяются при анализе программного обеспечения, существуют аналогичные подходы к анализу технических средств, а также физических и административных механизмов безопасности.

Стратегии сосредоточения усилий при детальном анализе

Даже при детальном анализе редко удается охватить целиком все аспекты обеспечения безопасности АС. Ниже представлены две стратегии сосредоточения усилий, которые применяются при проведении анализа с использованием обсуждавшихся выше подходов. Одна основана на анализе компонентов модели защиты, а другая — на анализе конкретных сценариев атак и процессов, происходящих в АС.

Анализ компонентов модели защиты АС

Эта стратегия сосредоточения усилий базируется на четырех основных компонентах модели защиты АС, в число которых входят ресурсы, угрозы, возможные последствия угроз и механизмы безопасности. Все эти компоненты должны быть уже рассмотрены на этапе базового анализа и в ходе анализа рисков. Текущая задача предполагает их более детальное рассмотрение на основе уже имеющихся данных.

Информационные, программные и физические ресурсы АС выступают в качестве объекта защиты. Может потребоваться произвести детальное исследование ресурсов (файлов, записей, программ, устройств, каналов связи и т. п.) вместе с их атрибутами (количество, параметры, способы использования, характеристики).

Угрозы безопасности для ресурсов АС определяются в терминах модели нарушителя, способа осуществления угрозы и объекта нападения. При анализе угроз важно различать виды угроз: случайные, намеренные или обусловленные естественными причинами. Защита от намеренных угроз, называемых также атаками, может оказаться наиболее сложной.

Атаки на ресурсы АС, предпринимаемые как внешними, так и внутренними нарушителями, подразделяются на удаленные (сетевые) и локальные.

Локальные атаки характеризуются следующими атрибутами:

1. Источник угрозы, описываемый моделью нарушителя.
2. Вид атаки, указывает на принадлежность к тому или иному известному виду атак, согласно их классификации.
3. Способ атаки, указывает на принадлежность к тому или иному известному способу атаки данного вида, согласно их классификации.
4. Объект атаки (ресурс АС, против которого направлена атака).
5. Цель и последствия (результат) осуществления угрозы (описание последствий и оценка вероятного ущерба). Возможными целями осуществления угроз безопасности являются нарушение конфиденциальности, целостности или доступности информационных ресурсов АС, а также доступности программных и технических компонентов АС.
6. Условия (предпосылки) возникновения угрозы безопасности, такие как наличие определенных видов уязвимостей, нарушения технологического процесса проектирования и разработки ПО и т. п.
7. Жизненный цикл угрозы, который состоит из следующих процессов:
   - зарождение,
   - развитие,
   - проникновение в АС,
   - проникновение в критичную информацию,
   - инициализация,
   - результат действия,
   - регенерация.

Удаленные (сетевые) атаки дополнительно могут характеризоваться следующими атрибутами:

1. Условие начала осуществления воздействия:
   - Атака по запросу от атакуемого объекта.

- Атака по наступлению ожидаемого события на атакуемом объекте.
- Безусловная атака.

2. По наличию обратной связи с атакуемым объектом:
   - С обратной связью.
   - Без обратной связи.
3. По расположению субъекта атаки относительно атакуемого объекта:
   - Внутрисегментное.
   - Межсегментное.
4. По уровню эталонной модели OSI, на котором осуществляется воздействие:
   - Физический.
   - Канальный.
   - Сетевой.
   - Транспортный.
   - Сеансовый.
   - Представительский.
   - Прикладной.
5. По характеру воздействия:
   - Активное.
   - Пассивное.

В процессе анализа исследуются факторы, влияющие на вероятности успешного осуществления угроз. Вероятности осуществления угроз зависят от состояния и степени критичности ресурсов, последствий, связанных с реализацией угрозы, существующих защитных механизмов и ожидаемого выигрыша, получаемого злоумышленником. Вероятности успешного осуществления угроз зависят от величины уязвимостей защиты АС, которые также оцениваются.

На выбор методов анализа оказывает влияние природа угроз. Например, стандартным является метод анализа исходных текстов программы с целью определения их соответствия установившейся технологии и стилю программирования, поиска ошибок и брешей в реализации механизмов безопасности. Однако, если источником угрозы является разработчик приложения, то встает задача поиска программных закладок и, вместо исходных текстов и спецификации, проводится изучение объектного кода, т.к. злонамеренные действия разработчика в этом случае не будут задокументированы.

Последствия реализации угроз — это формы возможных потерь, характеризуемые величиной ущерба, наносимого владельцу или пользователям АС. Примерами последствий реализации угроз могут служить раскрытие конфиденциальной информации, принятие ошибочных решений руководством организации и кража денежных средств путем компьютерного мошенничества. При оценке возможного ущерба рассматривается наихудший вариант развития событий.

Анализ механизмов безопасности предполагает детальное исследование эффективности их противодействия угрозам. На этом этапе осуществляется поиск слабостей механизмов безопасности, которые обуславливают существование уязвимостей защиты, определение реальных трудностей, связанных с использованием слабостей конкретного механизма безопасности, анализ накладных расходов на обеспечение безопасности и исследование альтернативных способов реализации защитных механизмов.

Анализ конкретных сценариев атак и процессов

Размеры и сложность современных АС часто не позволяют получить исчерпывающую информацию обо всех аспектах ее функционирования. В этом случае оценку уровня защищенности АС приходится давать, основываясь на неполной информации. Эффективным решением в данной ситуации является использование подхода, связанного с анализом конкретных сценариев атак и процессов, происходящих в АС. Данный подход дополняет результаты базового анализа конкретными примерами, и позволяет сосредоточиться на частных и наиболее важных аспектах работы отдельных приложений.

Сценарий атаки описывает стадии реализации угрозы безопасности, рассмотренные выше. Примером сценария атаки может служить пошаговое описание попытки несанкционированного проникновения в АС (включая последовательность действий злоумышленника и процесс планирования атаки), используемых уязвимостей, скомпрометированных ресурсов АС и последствий атаки (включая оценку ущерба).

Данный подход предполагает широкое использование методов активного тестирования защищенности АС с применением соответствующих инструментальных средств. Идея активного тестирования заключается в имитации действий возможного злоумышленника по преодолению системы защиты с использованием известных методов осуществления локальных и удаленных атак. По результатам тестирования делается вывод о наличии либо отсутствии в АС известных уязвимостей. На данном принципе основана работа сетевых сканеров, являющихся в настоящее время основным инструментом активного тестирования АС.

Подготовка отчетных документов по результатам аттестации

Основными отчетными документами по результатам аттестации являются Заключение и прилагаемый к нему Протокол аттестационных испытаний. Заключение содержит выводы относительно соответствия механизмов безопасности АС критериям аттестации, оценку уровня защищенности и рекомендации по обеспечению режима информацион-

ной безопасности АС, дополняющие существующие организационные меры защиты. Заключение основывается на данных, содержащихся в Протоколе аттестационных испытаний. На основании Заключения председатель аттестационной комиссии принимает решение о выдаче Аттестата соответствия.

Содержание отчетных документов

В американских руководящих документах предлагается следующая структура итогового отчета:

1. Введение и краткое содержание. Коротко описываются назначение, основные характеристики и особенности исследуемой АС, делаются выводы по результатам базового и детального анализов и даются рекомендации по устранению замеченных недостатков в организации защиты.
2. Описание объекта оценки. Этот раздел содержит информацию, необходимую для принятия решения о возможности выдачи Аттестата соответствия, разрешающего обработку в АС информации заданной степени критичности. Одним из основных вопросов здесь является соответствие АС стандартам, нормативным документам и требованиям политики безопасности. Также в данном параграфе описываются характеристики АС, влияющие на принятие решения о выдаче аттестата, ограничения, накладываемые на использование АС, и ее границы.
3. Результаты аттестационных испытаний. В первой части этого раздела описываются механизмы безопасности АС и их роль в противодействии существующим угрозам безопасности. Во второй части раздела дается описание уязвимостей АС, которые делятся на две категории: остаточные уязвимости, которые по экономическим соображениям можно оставить, и уязвимости, которые необходимо ликвидировать. Эта часть раздела служит одновременно кратким изложением результатов анализа и рекомендацией по ликвидации обнаруженных уязвимостей или принятию остаточных рисков.
4. Мероприятия по устранению недостатков системы защиты. В этом разделе описываются мероприятия по устранению уязвимостей, оценивается стоимость реализации контрмер и их влияние на работу АС, а также расставляются приоритеты на выполнение указанных задач.

К итоговому отчету прилагаются следующие документы:

- Протокол аттестационных испытаний.
- Заключение по результатам аттестации с указанием возможности обработки в АС информации заданного уровня критичности.
- отчеты по результатам предварительного обследования АС, базового и детального анализов.

В случае несоответствия АС предъявляемым к ней требованиям по безопасности информации и невозможности оперативно устранить выявленные недостатки может быть принято решение об отказе в выдаче аттестата. При этом может быть назначен срок проведения повторной аттестации.

При наличии замечаний непринципиального характера Аттестат может быть выдан после проверки устранения этих замечаний.

Многие уязвимости защиты, выявленные при аттестации, не могут являться достаточным основанием для отказа в выдаче Аттестата. В подобной ситуации для закрытия брешей в программно-технической защите АС возможно использование различных контрмер организационного уровня, перечень которых обязательно указывается в Аттестате соответствия. Примерами подобных контрмер могут служить запрещение осуществления удаленного доступа к ресурсам АС по коммутируемым каналам связи в приказном порядке, ограничение уровня конфиденциальности информации, разрешенной для обработки в АС, изъятие из состава АС наиболее уязвимых ее компонентов и т. п.