ФСТЭК РОССИИ

РУКОВОДЯЩИЙ ДОКУМЕНТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Концепция оценки соответствия автоматизированных систем требованиям безопасности информации

(проект, первая редакция)

Введен в действие приказом
ФСТЭК России
от г. №

2004

Содержание

1 Область применения

Настоящая Концепция содержит систему взглядов и основных принципов, определяющих решение проблем оценки соответствия автоматизированных систем требованиям безопасности информации (далее – оценки соответствия АС).

Оценка соответствия АС основывается на положениях и требованиях действующих законов, технических регламентов, стандартов, нормативных и методических документов, регламентирующих деятельность в сфере обеспечения безопасности информации.

Концепция предназначена для использования органами государственной власти, заказчиками, разработчиками и пользователями АС при формировании требований, разработке и эксплуатации автоматизированных систем, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Концепция предназначена также для органов оценки соответствия, органов по сертификации и испытательных лабораторий для использования при проведении оценки соответствия АС.

Концепция служит методологической основой нормативных и методических документов, направленных на обеспечение решения следующих задач:

- формирования требований безопасности информации, предъявляемых к АС;
- регламентации мероприятий по оценке соответствия АС;
- поддержания безопасности АС при эксплуатации.

Концепция направлена на совершенствование и развитие нормативно-методической базы и организационных основ оценки соответствия АС на основе положительной отечественной практики обеспечения безопасности информационных технологий с использованием последних достижений международной стандартизации и передового зарубежного опыта.

2 Термины и определения

В настоящей Концепции применяются следующие термины с соответствующими определениями.

2.1 **Автоматизированная система** (automated system): Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.2 **Активы** (assets): Информация или ресурсы, подлежащие защите в АС.

2.3 **Безопасность автоматизированной системы** (automated system security): Состояние АС, определяющее защищенность обрабатываемой информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность АС выполнять предписанные функции без нанесения неприемлемого ущерба объектам и субъектам информационных отношений.

2.4 **Воздействие** (impact): Последствие нежелательного инцидента, произошедшего преднамеренно или случайно, которое влияет на активы.

2.5 **Доверие** (assurance): Основание для уверенности в том, что АС отвечает своим целям безопасности.

2.6 **Задание по безопасности** (security target): Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ или автоматизированной системы.

2.7 **Изделие ИТ** (IT production): Обобщенный термин для продуктов и систем ИТ.

2.8 **Инцидент** (incident): Действие, явление или событие, нарушающее безопасность АС.

2.9 **Информационная технология** (Information technology): Приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

2.10 **Средства обеспечения безопасности** (Security controls): Аппаратные, программно-аппаратные и программные средства, реализующие совокупность всех функций безопасности АС.

2.11 **Меры обеспечения безопасности** (safeguard): Методы, процедуры или механизмы, использование которых позволяет обеспечивать защиту от угроз,

снижать уязвимости, ограничивать воздействия нежелательных инцидентов и облегчать восстановление безопасности АС.

2.12 **Объект оценки** (target of evaluation): Подлежащие оценке изделие ИТ или АС с эксплуатационной документацией.

2.13 **Остаточный риск** (residual risk): Риск, который остается после реализации мер и средств обеспечения безопасности АС.

2.14 **Оценка соответствия** (assessment of conformance): Прямое или косвенное определение соблюдения требований предъявляемых к объекту.

2.15 **Подтверждение соответствия** (confirmation of conformance): документальное удостоверение соответствия объектов требованиям технических регламентов, положениям стандартов и другим нормативным документам.

2.16 **Политика безопасности организации** (organisational security policies): Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

2.17 **Предположения** (assumptions): Условия, которые должны быть обеспечены в среде, чтобы изделие ИТ или АС в целом могли рассматриваться как безопасные.

2.18 **Продукт ИТ** (IT product): Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ и АС.

2.19 **Профиль защиты** (protection profile): Независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ или АС, отвечающая специфическим запросам потребителя.

2.20 **Ресурсы** (resource): Данные, программные, программно-аппаратные или аппаратные средства, используемые для обеспечения выполнения АС установленных функций.

2.21 **Риск** (risk): Потенциальная опасность нанесения ущерба в результате реализации некоторой угрозы.

2.22 **Система ИТ** (IT system): Специфическое воплощение изделия ИТ с конкретным назначением и условиями эксплуатации – программно-техническая основа АС.

2.23 **Угроза** (threat): Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба функционированию АС, защищаемым активам или отдельным лицам.

2.24 **Уязвимость** (vulnerability): Недостаток актива или группы активов, автоматизированной системы или среды функционирования, который может использоваться одной или несколькими угрозами.

2.25 **Функция безопасности** (security function): Функциональные возможности части или частей АС, а также АС в целом, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности.

2.26 **Цель безопасности** (security objective): Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям.

3 Сокращения

АС – автоматизированная система

ЗБ – задание по безопасности

ИТ – информационная технология

ПЗ – профиль защиты

РД – руководящий документ

ФСТЭК – Федеральная служба по техническому и экспортному контролю

4 Общие положения

В соответствии с «Доктриной информационной безопасности Российской Федерации» обеспечение безопасности информационных и телекоммуникационных систем представляет одну из составляющих национальных интересов России в информационной сфере. Это определяет необходимость формирования требований безопасности хранящейся, обрабатываемой и передаваемой информации (прежде всего, в ключевых системах информационной инфраструктуры) и выполнения специальных действий по оценке соответствия используемых АС этим требованиям.

Цель настоящей Концепции заключается в определении основных направлений совершенствования нормативно-методической базы и организационных основ проведения оценки соответствия АС требованиям безопасности информации.

4.1 Общая характеристика системы оценки соответствия автоматизированных систем требованиям безопасности информации

В Российской Федерации сложилась и достаточно эффективно действует система оценки соответствия АС требованиям безопасности информации. Основы деятельности этой системы определяются относящимися к сфере информатизации и информационной безопасности федеральными законами, указами Президента Российской Федерации, руководящими и методическими документами федеральных органов исполнительной власти.

Оценка соответствия осуществляется в форме аттестации АС по требованиям безопасности информации. Под аттестацией АС понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации.

Аттестация по требованиям безопасности информации предшествует началу обработки в АС подлежащей защите информации и определяется необходимостью подтверждения эффективности комплекса используемых в АС и на конкретном объекте информатизации мер и средств защиты информации.

Обязательной аттестации подлежат АС, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер и может осуществляться по инициативе заказчика или владельца АС.

Аттестация предусматривает комплексную проверку АС в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

При аттестации АС подтверждается её соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на АС (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в АС.

Аттестация проводится органом по аттестации в установленном порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации.

Активное развитие информационных технологий, расширяющаяся сфера их применения в деятельности организаций всех форм собственности, возрастающая зависимость систем критического применения от эффективности информационных технологий, расширение состава угроз информационной безопасности, изменения в законодательной базе требуют постоянного развития нормативных и методических основ обеспечения безопасности АС.

Сложившаяся к началу 2000-х годов нормативная база оценки соответствия АС требованиям безопасности информации имеет ряд недостатков, основными из которых являются:

- статичность и недостаточная конкретность требований, слабый учет особенностей АС и имеющихся угроз безопасности информации, недостаточная проработанность процедурных и методических аспектов оценки соответствия АС;
- преобладание технических мер по отношению к организационным и технологическим мерам обеспечения безопасности АС;
- дисбаланс между нормативной базой сертификации изделий ИТ и нормативной базой оценки соответствия АС, порождающий ряд

методических и процедурных проблем при проведении работ по оценке соответствия АС;

- недостаточность развития критериальной базы оценки организационных и технологических мер обеспечения безопасности информации в АС.

Все это отрицательно сказывается на достоверности и повторяемости результатов оценки соответствия АС требованиям безопасности информации.

В качестве основных направлений совершенствования нормативной и методической базы системы оценки соответствия АС в настоящей Концепции определены следующие:

- развитие критериальной базы в направлении охвата всей совокупности организационных, технологических и технических мер обеспечения информационной безопасности информации, четкая структуризация и дифференциация требований в зависимости от категории АС, уровня ценности защищаемых активов, состава угроз и условий среды функционирования;
- совершенствование организационных и процедурных основ оценки соответствия АС в направлении четкой регламентации видов работ, выполняемых на различных этапах жизненного цикла, формализации состава и структуры разрабатываемых документов, порядка их актуализации с учетом динамики изменения АС и среды их функционирования.
- развитие методов и форм проведения оценки соответствия АС в направлении разработки общей методологии и формализованных процедур выполнения работ, обеспечивающих объективность, достоверность и повторяемость результатов.

4.2 Основные принципы оценки соответствия автоматизированных систем

Основными принципами, на которых должна основываться оценка соответствия АС, являются следующие:

- оценка соответствия АС должна иметь целью определение соответствия применяемых в АС мер и средств обеспечения безопасности информации установленным для них требованиям;

- требования безопасности информации должны включать организационные, технические и эксплуатационные требования, устанавливаемые на основе анализа риска, определяемого исходя из ценности защищаемых активов и идентифицированных для АС угроз и уязвимостей;
- требования безопасности должны разрабатываться на основе стандартизованной структурированной базы точно определенных требований безопасности и представляться в установленном формате;
- методология формирования требований безопасности для различных уровней объектов (АС, изделий ИТ) должна быть тесно взаимосвязана в целях обеспечения их взаимного учета;
- оценка соответствия АС должна осуществляться в соответствии с четко определенными критериями и общей методологией, которые должны позволять проводить доказательную оценку выполнения установленных требований, обеспечивать объективность и повторяемость результатов, а также обеспечивать возможность учета результатов сертификации применяемых в АС изделий ИТ;
- процессы оценки соответствия АС должны состоять из четко определенных, взаимоувязанных этапов и работ, выполнение которых приводит к принятию обоснованного решения о соответствии (несоответствии) АС установленным для нее требованиям;
- все работы по оценке соответствия АС и их результаты должны точно персонифицироваться, идентифицироваться и документироваться по установленным форматам;
- поддержание безопасности АС должно обеспечиваться постоянным мониторингом и периодической переоценкой безопасности АС.

4.3 Организационная структура оценки соответствия автоматизированных систем

Организационная структура оценки соответствия автоматизированных систем требованиям безопасности информации включает следующих участников:

- ФСТЭК России (федеральный орган исполнительной власти, уполномоченный организовывать работу по оценке соответствия АС требованиям безопасности информации);

- органы оценки соответствия АС требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики АС, оцениваемых по требованиям безопасности информации).

ФСТЭК России в части организации работ по оценке соответствия АС требованиям безопасности информации выполняет следующие функции:

- организует, финансирует разработку и утверждает нормативные и методические документы по оценке соответствия АС требованиям безопасности информации;
- организует и осуществляет экспертизу тактико-технических и технических заданий на создание АС ключевых систем информационной инфраструктуры;
- аккредитует органы оценки соответствия АС и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил оценки соответствия АС и эксплуатацией оцененных АС;
- осуществляет координацию действий всех участников оценки соответствия АС требованиям безопасности информации.

Органы оценки соответствия АС требованиям безопасности информации выполняют следующие функции:

- участвуют в экспертизе тактико-технических и технических заданий на создание АС ключевых систем информационной инфраструктуры;
- осуществляют координацию действий всех участников оценки соответствия конкретных АС;
- проводят оценку соответствия АС требованиям безопасности информации, выдают «Аттестат соответствия» на АС;
- на основе анализа результатов мониторинга, выполняемого заявителем, принимают решения о необходимости корректировки требований безопасности информации, предъявляемых к АС, и/или переоценки соответствия АС требованиям безопасности информации;
- ведут информационную базу АС, для которых этими органами выдан «Аттестат соответствия»;
- регулярно информируют ФСТЭК России о результатах своей деятельности в области оценки соответствия АС требованиям безопасности информации.

Заявители, в качестве которых могут выступать заказчики, владельцы, эксплуатирующие организации АС, оцениваемых по требованиям безопасности информации, выполняют следующие функции:

- организуют и осуществляют выполнение организационно-технических мероприятий, направленных на подготовку АС к оценке соответствия требованиям безопасности информации;
- инициируют процесс оценки соответствия АС;
- привлекают органы оценки соответствия АС для организации и проведения оценки соответствия АС требованиям безопасности информации;
- согласуют исходные данные для оценки соответствия АС с органом оценки соответствия АС;
- привлекают (в необходимых случаях) испытательные лаборатории для проведения сертификационных испытаний по требованиям безопасности информации несертифицированных изделий ИТ, составляющих программно-техническую основу конкретной АС;
- осуществляют эксплуатацию АС в соответствии с условиями и требованиями, установленными в «Аттестате соответствия»;
- осуществляют постоянный мониторинг эксплуатируемой АС и среды функционирования, анализ влияния изменений на безопасность АС и извещают орган оценки соответствия АС, выдавший «Аттестат соответствия», обо все изменениях, которые могут повлиять на эффективность применяемых в АС мер и средств обеспечения безопасности информации;
- осуществляют финансирование и материально-техническое обеспечение процесса оценки соответствия АС.

4.4 Нормативно-методическая база оценки соответствия автоматизированных систем

Нормативно-методическая база оценки соответствия АС должна строится на основе преемственности со сложившейся практикой оценки соответствия АС в Российской Федерации, а также с учетом гармонизации критериев оценки с международными стандартами и нормативно-методической базой сертификации изделий ИТ по требованиям безопасности информации.

Структура нормативно-методической базы оценки соответствия АС должна включать:

- базовые документы;
- нормативное обеспечение;
- методическое обеспечение.

Базовые документы определяют подход к оценке соответствия АС требованиям безопасности информации, критерии оценки АС на уровне технических регламентов и национальных стандартов, общий порядок оценки соответствия АС, участников оценки и распределение ответственности между ними.

Нормативное обеспечение включает документы Федеральной службы по техническому и экспортному контролю, регламентирующие вопросы категорирования АС, исходя из ценности обрабатываемой информации и/или критичности выполняемых функций, формирования наборов требований безопасности к АС, процедуры проведения оценки соответствия АС и инспекционного контроля, роли и обязанности участников оценки соответствия АС, требования к органам оценки соответствия АС м др.

Методическое обеспечение включает модели, руководства, и методики, позволяющие наиболее эффективно выполнять требования нормативных документов по оценке соответствия АС.

Нормативно-методическая база оценки соответствия АС должна быть поддержана *инструментальным обеспечением*, позволяющим автоматизировать процессы разработки, регистрации и каталогизации наборов требований безопасности информации, предъявляемых к АС, и проведение оценки выполнения этих требований.

5 Подход к оценке соответствия автоматизированных систем требованиям безопасности информации

Подход к оценке соответствия АС должен обеспечивать объективную, достоверную и повторяемую оценку соответствия АС установленным для неё требованиям в соответствии с процедурами и критериями, установленными в нормативных документах.

Требования безопасности АС должны формироваться в процессе разработки технического задания на создание АС и представляться в документе «Профиль защиты АС», который должен являться неотъемлемой частью технического задания.

Профили могут разрабатываться также для определенных классов автоматизированных систем.

Оценка соответствия АС требованиям безопасности информации должна проводиться на соответствие документу «Задание по безопасности». В ЗБ приводятся требования безопасности информации, соответствующие профилю защиты и описываются организационные и технические меры и средства, реализованные в АС для удовлетворения предъявленных требований безопасности информации. В процессе оценки соответствия АС проверяется обоснованность выбора требований безопасности информации, эффективность и достаточность реализованных мер и средств обеспечения безопасности информации с учетом реальных условий применения АС на конкретных объектах информатизации.

Критерии, методы и процедуры оценки соответствия АС должны обеспечивать выполнение следующих условий для проведения и получаемых результатов оценки:

- объективность – результаты оценки соответствия АС должны основываться на используемых исходных документах (свидетельствах) и содержать минимум субъективного мнения оценщика;
- беспристрастность – результаты оценки должны быть непредубежденными даже в тех случаях, когда требуется субъективное суждение;
- повторяемость – действия одного и того же оценщика, выполняемые с использованием одной и той же совокупности свидетельств для оценки, должны приводить к одним и тем же результатам;
- воспроизводимость – действия другого оценщика, выполняемые с использованием одной и той же совокупности свидетельств для оценки, должны приводить к одним и тем же результатам;
- корректность – должны выполняться действия оценщика, которые требуются, и они должны выполняться надлежащим образом, чтобы обеспечить правильные результаты оценки;
- достаточность – каждый вид действий оценщика по оценке должен осуществляться до уровня, необходимого для удовлетворения всех заданных требований;
- приемлемость – каждое действие оценщика должно способствовать повышению доверия к безопасности АС, по меньшей мере, пропорционально затраченным усилиям.

Подтверждение соответствия АС требованиям по безопасности информации оформляется документом «Аттестат соответствия автоматизированной системы требованиям безопасности информации» (далее – Аттестат соответствия).

Выдачей Аттестата соответствия процесс оценки соответствия АС требованиям безопасности информации не завершается. В ходе эксплуатации должен осуществляться постоянный мониторинг изменений АС и среды ее функционирования, анализ влияния изменений на безопасность АС, уточнение соответствующей организационно-распорядительной, эксплуатационной документации и задания по безопасности. При изменениях в АС и среде ее функционирования, приводящих к необходимости существенного изменения требований безопасности и реализующих их мер и средств обеспечения безопасности, должна проводиться новая оценка соответствия АС.

6 Критерии оценки соответствия автоматизированных систем

Критерии оценки соответствия АС требованиям безопасности информации должны представлять собой систематизированную совокупность требований безопасности информации и методологии оценки удовлетворения АС требованиям на основании результатов исследования материалов разработчика АС, документов эксплуатирующей организации и фактического материала, получаемого в ходе работ по непосредственной оценке соответствия АС.

Требования безопасности АС содержат две категории требований:

- функциональные требования безопасности АС;
- требования доверия к безопасности АС.

Функциональные требования безопасности АС предъявляются к тем функциональным возможностям мер и средств обеспечения безопасности АС, которые предназначены для обеспечения безопасности АС и определяют желательный безопасный режим функционирования АС.

Функциональные требования безопасности АС включают:

- организационные требования безопасности АС;
- эксплуатационные требования безопасности АС;
- требования безопасности информационных технологий АС.

Требования доверия к безопасности АС предъявляются к действиям разработчика АС, документам (свидетельствам), представляемым для оценки, действиям по оценке соответствия АС и действиям эксплуатирующей организации.

Требования доверия к безопасности АС включают:

- требования доверия к мерам и средствам обеспечения безопасности при разработке АС;
- требования доверия к мерам и средствам обеспечения безопасности при эксплуатации АС;
- требования доверия к безопасности информационных технологий АС.

Оценка соответствия АС требованиям безопасности информации должна проводиться на основе единой методологии оценки, предусматривающей конкретные виды действий оценщика по оценке соответствия АС требованиям безопасности информации.

7 Процесс оценки соответствия автоматизированных систем требованиям безопасности информации

Основными стадиями процесса оценки соответствия АС требованиям безопасности информации являются:

- подготовка к оценке соответствия АС требованиям безопасности информации;
- оценка соответствия АС.

На рисунке 1 представлены основные стадии и этапы процесса оценки соответствия АС требованиям безопасности информации.

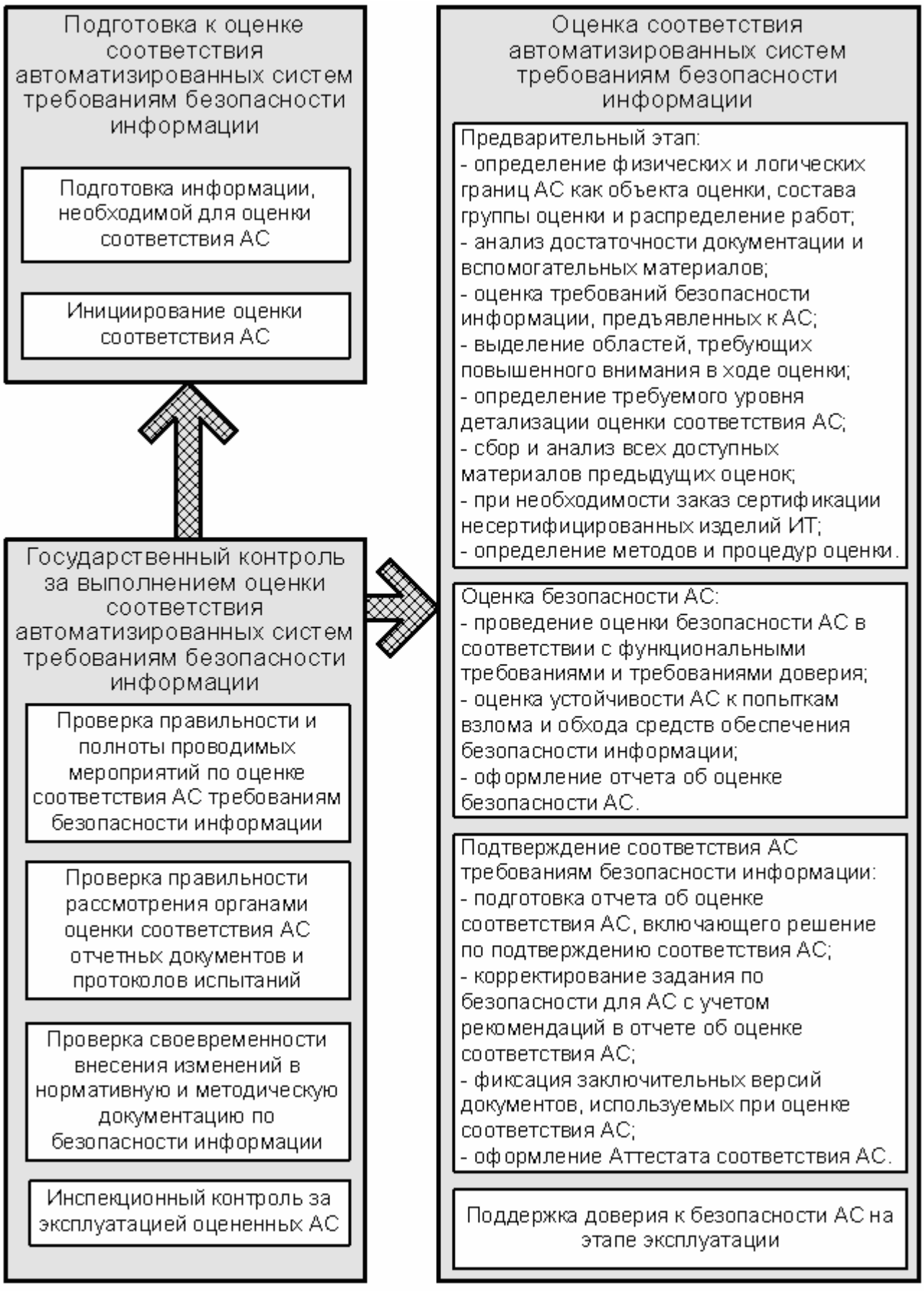

Рисунок 1 – Основные стадии и этапы процесса оценки соответствия АС требованиям безопасности информации

7.1 Подготовка к оценке соответствия автоматизированных систем требованиям безопасности информации

Подготовка к оценке соответствия АС требованиям безопасности информации включает следующие этапы:

- подготовку информации, необходимой для оценки соответствия АС;
- инициирование оценки соответствия АС: определение состава участников оценки, согласование исходных данных для оценки, планирование оценки соответствия и определение требуемых ресурсов.

Подготовка информации, необходимой для оценки соответствия АС, предусматривает:

- документирование описания АС и подлежащих защите информационных активов;
- категорирование АС и документирование результатов категорирования;
- идентификацию и документирование угроз безопасности информации для АС;
- оценку рисков безопасности информационных активов АС и документирование результатов в свидетельстве оценки рисков;
- определение требований безопасности, на соответствие которым должна проводиться оценка АС, мер и средств обеспечения безопасности информации в задании по безопасности для АС.

Результатом выполнения данного этапа подготовки к оценке соответствия АС требованиям безопасности информации должны быть следующие документы:

1) свидетельство оценки рисков;

2) акт категорирования автоматизированной системы;

3) задание по безопасности для оцениваемой АС;

4) совокупность свидетельств, характеризующих выполнение требований доверия, включенных в задание по безопасности.

Инициирование оценки соответствия АС требованиям безопасности информации предусматривает:

- определение состава участников оценки соответствия АС;
- заключение необходимых договоров и соглашений о неразглашении между заявителем, органом оценки соответствия АС и при необходимости – испытательной лабораторией;

- предоставление и согласование исходных данных для оценки соответствия АС;
- планирование выполнения оценки соответствия АС, включая:
  - определение общей схемы выполнения оценки соответствия АС и ее согласование с заказчиком и исполнителями работ;
  - планирование и выделение ресурсов (финансовых, временных, людских, технических), необходимых для оценки соответствия АС (с учетом возможных незапланированных ситуаций);
  - документирование плана проведения оценки соответствия АС требованиям безопасности информации.

7.2 Оценка соответствия автоматизированных систем требованиям безопасности информации

Оценка соответствия АС требованиям безопасности информации включает следующие этапы:

- предварительный этап, связанный с подбором исполнителей (испытателей и экспертов), анализом достаточности материалов для оценки, оценкой предъявленных к АС требований безопасности информации, определением методов и процедур оценки;
- оценку безопасности АС;
- подтверждение соответствия АС требованиям безопасности информации;
- поддержку доверия к безопасности АС на этапе эксплуатации.

Предварительный этап оценки соответствия АС требованиям безопасности информации предусматривает:

- определение физических и логических границ АС как объекта оценки, состава группы оценки и распределение работ между ее членами;
- анализ достаточности документации и вспомогательных материалов, необходимых для проведения оценки соответствия АС;
- оценку требований безопасности информации, предъявленных к АС, с учетом требований законодательства, технических регламентов и других нормативных документов, включая:
  - проверку правильности категорирования АС, зафиксированного в акте категорирования АС;

- определение соответствия требований безопасности информации, законодательной и нормативной базе, политике безопасности организации;
- анализ соответствия требований безопасности информации существующим угрозам и рискам в отношении АС;
- корректировку требований безопасности информации по результатам оценки и с учетом рекомендаций органа оценки соответствия АС.

– выделение областей, требующих повышенного внимания в ходе оценки соответствия АС (с учетом критичности хранимой, обрабатываемой и передаваемой информации, степени изученности уязвимостей и других факторов);
– определение требуемого уровня детализации оценки соответствия АС (в целом или в разрезе ее отдельных компонентов и подсистем), исходя из критичности АС, состава исходных данных, характеристик механизмов безопасности, размера и сложности АС;
– сбор и анализ всех доступных заключений (выводов), результатов, свидетельств и документации предыдущих оценок безопасности АС (в том числе отдельных сертифицированных изделий ИТ, используемых в АС);
– при необходимости заказ сертификации несертифицированных изделий ИТ, входящих в состав оцениваемой АС;
– выбор и, при необходимости, разработка соответствующих методов и процедур оценки всех категорий мер и средств обеспечения безопасности информации в АС на основе общей методологии оценки безопасности АС.

Оценка безопасности АС проводится с использованием выбранных и/или разработанных на предварительном этапе методов и процедур и предусматривает:

– проведение оценки безопасности АС в соответствии с функциональными требованиями и требованиями доверия, представленными в ЗБ;
– оценку устойчивости АС к попыткам взлома и обхода средств обеспечения безопасности информации;

- оформление отчета об оценке безопасности АС, включающего результаты оценки безопасности АС, рекомендации по эксплуатации АС, а также рекомендации по уменьшению или устранению идентифицированных уязвимостей.

Подтверждение соответствия АС требованиям безопасности информации предусматривает:

- подготовку отчета об оценке соответствия АС, включающего решение по подтверждению соответствия АС;
- корректирование задания по безопасности для АС с учетом рекомендаций в отчете об оценке соответствия АС;
- фиксация заключительных версий документов, используемых при оценке соответствия АС;
- оформление Аттестата соответствия АС.

Поддержка доверия к безопасности АС на этапе эксплуатации предусматривает:

- постоянный мониторинг изменений в АС, прежде всего, мер и средств обеспечения безопасности информации, а также – изменений среды функционирования АС;
- анализ влияния изменений на безопасность АС;
- информирование органа оценки соответствия АС обо всех изменениях, которые могут повлиять на безопасность АС.

В случае необходимости орган оценки соответствия АС может принять решение о необходимости новой оценки соответствия эксплуатируемых АС требованиям безопасности информации.

8 Государственный контроль за выполнением оценки соответствия автоматизированных систем требованиям безопасности информации

Государственным органом, уполномоченным на осуществление контроля и надзора за соблюдением правил оценки соответствия АС требованиям безопасности информации, является Федеральная служба по техническому и экспортному контролю.

Основными составляющими государственного контроля и надзора являются:

1) проверка правильности и полноты проводимых мероприятий по оценке соответствия АС требованиям безопасности информации;

2) проверку правильности рассмотрения органами оценки соответствия АС отчетных документов и протоколов оценки безопасности АС;

3) проверку своевременности внесения изменений в нормативную и методическую документацию по безопасности информации;

4) инспекционный контроль за эксплуатацией оцененных АС.

9 Направления реализации Концепции

9.1 Совершенствование нормативно-методической базы

В целях реализации настоящей Концепции разработке подлежат следующие составляющие нормативно-методической базы оценки соответствия АС требованиям безопасности информации (базовые, нормативные и методические документы):

1) в качестве базовых документов, кроме самой Концепции, должны быть разработаны следующие документы:

- РД «Безопасность информационных технологий. Критерии оценки безопасности автоматизированных систем»;
- Положение по порядку оценки соответствия автоматизированных систем требованиям безопасности информации;
- Положение по аккредитации органов оценки соответствия автоматизированных систем требованиям безопасности информации;

2) основу нормативного обеспечения должны составить следующие документы:

- Положение о категорировании АС требованиям безопасности информации;
- Положение по разработке профилей защиты и заданий по безопасности для автоматизированных систем;
- Профили защиты для автоматизированных систем;
- Положение по инспекционному контролю за деятельностью органов оценки соответствия автоматизированных систем требованиям безопасности информации;

- Требования к органам оценки соответствия автоматизированных систем требованиям безопасности информации;

3) основу методического обеспечения должны составить следующие документы:

- Базовая модель угроз безопасности автоматизированных систем;
- Руководство по оценке рисков безопасности информации в автоматизированных системах;
- Руководство по разработке профилей защиты и заданий по безопасности для автоматизированных систем;
- Общая методология оценки безопасности автоматизированных систем;
- Руководство по оценке автоматизированных систем по требованиям безопасности информации;
- Руководство по обеспечению безопасности в жизненном цикле АС;
- Руководство для органов оценки соответствия АС требованиям безопасности информации.

Первоочередными документами нормативно-методической базы оценки соответствия АС требованиям информационной безопасности, подлежащими разработке являются следующие:

1) Организационно-распорядительный документ «Положение по порядку оценки соответствия автоматизированных систем требованиям безопасности информации»;

2) Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности автоматизированных систем»;

3) Руководящий документ «Общая методология оценки безопасности автоматизированных систем».

В организационно-распорядительном документе «Положение по порядку оценки соответствия автоматизированных систем требованиям безопасности информации» необходимо:

- определить основные принципы оценки соответствия АС требованиям безопасности информации;
- определить роли основных участников оценки соответствия АС требованиям безопасности информации;
- описать основные этапы работ по оценке соответствия АС требованиям безопасности информации;

- определить порядок контроля и надзора за проведением оценки соответствия АС требованиям безопасности информации;
- определить порядок мониторинга и переоценки эксплуатируемых АС по требованиям безопасности информации.

В ходе совершенствования нормативно-методической базы оценки соответствия АС необходимо максимально использовать положения современных международных стандартов.

9.2 Разработка инструментальных средств поддержки оценки соответствия автоматизированных систем требованиям безопасности информации

В поддержку нормативно-методической базы оценки соответствия АС требованиям безопасности информации должно быть разработано соответствующее инструментальное обеспечение, позволяющее:

- каталогизировать модели угроз безопасности АС и требования безопасности АС, обеспечить их выбор и конкретизацию;
- автоматизировать процесс разработки ПЗ и ЗБ для АС;
- вести реестр разработанных пакетов требований безопасности, ПЗ и ЗБ для АС;
- осуществлять поддержку процесса оценки соответствия АС требованиям безопасности информации.

Реализация настоящей концепции позволит выйти на новый уровень обеспечения безопасности информации в автоматизированных системах различного назначения, в первую очередь – ключевых систем информационной инфраструктуры.