ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ»

КОРПОРАТИВНАЯ СИСТЕМА НОРМАТИВНО-МЕТОДИЧЕСКИХ ДОКУМЕНТОВ В ОБЛАСТИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ ОАО «ГАЗПРОМ»

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОАО «ГАЗПРОМ»

СТАНДАРТ ОРГАНИЗАЦИИ

РУКОВОДСТВО ПО РАЗРАБОТКЕ ТРЕБОВАНИЙ К ОБЪЕКТАМ ЗАЩИТЫ

СТО Газпром 4.2-3-001-2009

Москва 2009

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ»

СТАНДАРТ ОРГАНИЗАЦИИ

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОАО «ГАЗПРОМ»

РУКОВОДСТВО ПО РАЗРАБОТКЕ ТРЕБОВАНИЙ К ОБЪЕКТАМ ЗАЩИТЫ

СТО Газпром 4.2-3-001-2009

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ»

Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»

Общество с ограниченной ответственностью «Газпром экспо»

Москва 2009

Предисловие

1 РАЗРАБОТАН	Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»
2 ВНЕСЕН	Службой корпоративной защиты ОАО «Газпром»
3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ	распоряжением ОАО «Газпром» от 11 марта 2009 г. № 54.
4 ВВЕДЕН ВПЕРВЫЕ	

Содержание

СТАНДАРТ ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ГАЗПРОМ»

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОАО «ГАЗПРОМ»

РУКОВОДСТВО ПО РАЗРАБОТКЕ ТРЕБОВАНИЙ К ОБЪЕКТАМ ЗАЩИТЫ

Дата введения–2009-12-28

1 Область применения

Настоящий стандарт определяет порядок и процедуры разработки (формирования) требований по технической защите информации на объектах ОАО «Газпром» на различных стадиях их жизненного цикла и предназначен для использования при проведении работ по обеспечению информационной безопасности (ОИБ) в ОАО «Газпром», его дочерних обществах и организациях (далее – Общество).

2 Нормативные ссылки

В настоящем документе использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.602-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК ТО 15271-2002 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

СТО Газпром 4.2-0-003-2009 Система обеспечения информационной безопасности ОАО «Газпром». Общие положения

СТО Газпром 4.2-3-002-2009 Система обеспечения информационной безопасности ОАО «Газпром». Требования по технической защите информации при использовании информационных технологий

СТО Газпром 4.2-1-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Основные термины и определения

СТО Газпром 4.2-5-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Оценка соответствия объектов защиты.

Примечание – При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов по соответствующим указателям, составленным на 1 января текущего года, и информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по СТО Газпром 4.2-1-001.

4 Общие положения

4.1 В процессе организации обеспечения безопасности информации в автоматизированных системах (далее – АС) Общества должны быть решены следующие основные задачи:

- анализ обстановки, в том числе определение уровня важности АС, определение перечня защищаемой информации и оценка последствий нарушений безопасности АС, анализ и выявление потенциальных угроз безопасности информации, возможностей и условий их реализации, оценка эффективности и достаточности принятых мер по ОБИ, подготовку и принятие решения о необходимости дополнительных мер по ОБИ;
- разработка политики ОБИ;
- формирование (обоснование) требований по ОБИ для АС;

- выбор целесообразного состава мер и средств ОБИ в АС в соответствии с политикой ОБИ;

- решение вопросов обеспечения (материального, финансового, технического, кадрового);

- планирование мероприятий по ОБИ в АС;

- организация проведения НИОКР по разработке системы ОБИ создаваемой (используемой) АС;

- разработка документации по вопросам ОБИ в АС и эксплуатации системы ОБИ;

- внедрение системы ОБИ для используемой (разрабатываемой) АС.

4.2 Направления деятельности по ОБИ определяются политикой информационной безопасности Общества, на основе концепции информационной безопасности, определяющей принятую в Обществе систему взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности.

4.3 Безопасность АС достигается комплексным применением организационных и технических мер на всех этапах и стадиях жизненного цикла АС. Применение мер по ОБИ необходимо сочетать с возможностями используемых технологий создания АС, которые должны соответствовать действующим стандартам и нормативным документам (ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК ТО 15271, ГОСТ Р ИСО/МЭК 15408).

4.4 Правила ОБИ должны формироваться на основе выбора модели жизненного цикла, охватывающей все стадии разработки и сопровождения АС. В общем случае задание требований по ОБИ в АС производится на этапах:

- обоснования требований к АС;

- разработки (модернизации) АС;

- ввода АС в действие;

- эксплуатации АС;

- снятия АС с эксплуатации.

Для каждого из этапов жизненного цикла должны быть установлены однозначно сформулированные правила ОБИ АС, адекватные ожидаемым угрозам безопасности информации, обрабатываемой в АС.

4.5 Мероприятия по ОБИ в АС Общества являются составной частью управленческой, научной и производственной деятельности и осуществляются в тесной взаимосвязи с другими мерами по обеспечению установленного режима работы с информацией ограниченного доступа.

4.6 Требования безопасности информации задаются Обществом в техническом задании на разработку АС или формируются разработчиком при самостоятельном создании им

технических и программных средств, исходя из назначения и планируемой области применения в интересах Общества.

4.7 Решение задач по ОБИ должно начинаться одновременно с формированием замысла создания АС.

4.8 Требования по безопасности информации в АС должны формулироваться на основе анализа назначения АС, защищаемых элементов АС и среды применения АС в конкретной организации. Необходимые данные для формирования требований получаютя в процессе проведения обследования АС.

4.9 При обследовании проводятся анализ и идентификация процессов, связанных с обработкой защищаемой информации. Анализируются документы, используемые при организации и проведении работ по ОБИ. В результате обследования определяются узловые элементы процессов обработки, передачи и хранения защищаемой информации, для каждого из которых должны быть установлены:

- объекты и процессы, связанные с защищаемой информацией;
- субъекты, участвующие в обработке, передаче и хранении информации;
- их роли (полномочия и ответственность) в отношении к обрабатываемой информации;
- правила, которыми они должны руководствоваться при обработке информации.

4.10 При проведении информационного обследования устанавливаются также факторы, которые способны негативно повлиять на информацию, и процессы ее обработки и передачи.

4.11 По результатам обследования устанавливаются угрозы безопасности, которые имеют отношение к АС.

Угрозы характеризуются:

- источником;
- предполагаемыми способами реализации;
- уязвимостями АС, которые могут быть использованы для реализации угроз;
- элементами АС, которые могут быть подвергнуты воздействию;
- видами воздействий на элементы АС.

Источник угрозы характеризуется такими аспектами, как компетентность, доступные ресурсы и мотивация.

4.12 На основании анализа нормативных документов по ОБИ устанавливается уровень ценности (конфиденциальности, важности, стоимости) защищаемых элементов АС и требуемый класс защиты АС.

4.13 Установленные характеристики безопасности АС являются исходными данными для определения целей ОБИ в АС, связанных с противодействием выявленным угрозам безопасности и проведением оценки риска нарушения безопасности информации и/или выполнением соответствующих правил политики информационной безопасности Общества.

4.14 Необходимость определения целей безопасности состоит в том, чтобы сформулировать все намерения в отношении ОБИ АС и определить, какие из них будут реализовываться средствами АС, а какие обеспечиваться дополнительно.

4.15 Требования по ОБИ в АС реализуются путем задания двух видов правил:

- функциональных правил;
- правил доверия к безопасности.

4.16 К функциональным правилам относятся правила ОБИ в АС:

- по идентификации и аутентификации;
- доступу к АС;
- доступности используемых ресурсов;
- защите данных пользователя;
- обеспечению доверенного маршрута/канала связи с функциями безопасности АС;
- криптографической поддержке;
- управлению безопасностью;
- защите функций безопасности АС;
- оценке (проверке) уровня безопасности.

4.17 Правила доверия к безопасности определяют такие правила, выполнение которых дает основание для уверенности в том, что при создании АС приняты меры, обеспечивающие достижение поставленных целей безопасности. В их состав входят правила, определяющие требования:

- к поддержке жизненного цикла;
- процессу разработки;
- тестированию и анализу уязвимости АС;
- проектной и эксплуатационной документации;
- поставке и вводу в эксплуатацию;
- поддержанию доверия к безопасности при эксплуатации.

4.18 Оценка (проверка) уровня безопасности включает:

- установление степени соответствия правильности организации и проведения работ с использованием АС с точки зрения обеспечения целостности и конфиденциальности обрабатываемой информации требованиям действующих руководящих и нормативных документов;

- проверку порядка организации и проведения работ по обеспечению безопасности сторонней конфиденциальной (в том числе запатентованной) информации;

- проверку порядка организации и проведения работ по защите открытых данных (информации), используемых в процессе повседневной деятельности, от несанкционированной модификации или блокирования;

- оценку степени надежности защиты от несанкционированного доступа и утечки по техническим каналам персональных данных работников Общества и взаимодействующих с Обществом организаций;

- анализ и оценку используемых программных средств обработки информации и иных программных продуктов с точки зрения соблюдения правил их лицензирования.

4.19 На основе анализа результатов обследования АС принимается решение о том, какие из элементов АС подлежат защите. В первую очередь рассматриваются:

- аппаратные средства;

- программное обеспечение;

- информация, обрабатываемая и накапливаемая в АС (текущие данные, автономные архивы, многопользовательские архивы, резервные копии, регистрационные журналы, базы данных, а также данные, передаваемые по каналам связи);

- документация.

4.20 Применительно к указанным элементам АС выделяются две группы угроз безопасности информации:

- угрозы, связанные с утечкой защищаемой информации, как в интересах несанкционированного ознакомления со сведениями, составляющими коммерческую или иную тайну Общества, так и для нанесения ущерба Обществу (при реализации угроз данной группы непосредственного воздействия на саму информацию не производится);

- угрозы, связанные с нарушением целостности, доступности и достоверности защищаемой информации и возможности ее использования по назначению, реализуемые с использованием преднамеренных деструктивных воздействий на информацию.

4.21 Основными способами реализации угроз безопасности информации применительно к подлежащим защите элементам АС являются:

- несанкционированный доступ к защищаемым информационным ресурсам и информации;

- утечка защищаемой информации по техническим каналам;

4.22 Угрозы безопасности информации реализуются за счет:

- преднамеренной деятельности, в том числе – с использованием специальных программно-технических средств;

- недостатков и ошибок в общей схеме организации и проведения работ с защищаемой информацией;

- специально созданных фрагментов (программных закладок) или ошибок в общем и специальном программном обеспечении, применяемом в системах обработки информации;

- непреднамеренных ошибок пользователей, установленным порядком допущенных к защищаемой информации.

5 Правила обеспечения безопасности информации в автоматизированных системах на этапах жизненного цикла

5.1 Общая структура правил обеспечения безопасности информации в автоматизированных системах

5.1.1 Правила ОБИ для АС включают:

- правила, выполнение которых обеспечивает достижение поставленных целей безопасности при создании АС (правила ОБИ при создании АС);

- правила, выполнение которых обеспечивает достижение поставленных целей безопасности при эксплуатации АС (правила управления информационной безопасностью в АС);

- правила, выполнение которых обеспечивает достижение необходимого уровня безопасности АС (функциональные правила).

5.1.2 Правила ОБИ при создании АС определяют порядок выполнения мероприятий по ОБИ, реализуемых на этапе жизненного цикла АС:

- в процессе обоснования и задания требований по ОБИ в техническом задании на разработку (модернизацию) АС;

- при разработке (модернизации) АС;

- в процессе тестирования и анализа уязвимости АС;

- при создании проектной и эксплуатационной документации;

- при поставке и вводе в эксплуатацию АС;

- в процессе эксплуатации АС;

- при снятии АС с эксплуатации.

5.1.3 ОБИ на этапах жизненного цикла АС должно осуществляться на основе выбора (утверждения) и использования модели жизненного цикла, охватывающей все стадии разработки и сопровождения АС. Модель жизненного цикла определяет правила, методы, процедуры и инструментальные средства, используемые при разработке, поставке и сопровождении АС.

В модели жизненного цикла должны быть отдельно выделены и охарактеризованы вопросы ОБИ АС, среды ее разработки и эксплуатации.

При разработке модели жизненного цикла следует руководствоваться положениями ГОСТ Р ИСО/МЭК 12207 и ГОСТ Р ИСО/МЭК ТО 15271.

Модель жизненного цикла должна быть принята до начала проектирования и разработки АС.

5.1.4 Для каждого из периодов жизненного цикла должны быть установлены однозначно сформулированные правила по ОБИ АС, адекватные ожидаемым угрозам безопасности информации и соответствующие возможным последствиям реализации этих угроз.

5.1.5 Правила ОБИ в АС должны обеспечиваться при минимальных затратах и не препятствовать реализации основных целей создания и применения АС.

5.2 Правила обоснования и задания требований по обеспечению безопасности информации в техническом задании на разработку автоматизированных систем

5.2.1 Обоснование требований по ОБИ в техническом задании на разработку (модернизацию) АС осуществляется на основе принятой в Обществе политики информационной безопасности, анализа спектра возможных угроз безопасности информации и последствий, которые могут возникать вследствие реализации этих угроз.

5.2.2 Требования по ОБИ к АС необходимо задавать в техническом задании (ТЗ) на разработку (модернизацию) АС.

Ответственность за включение в ТЗ требований по ОБИ возлагается на структурное подразделение Общества, в интересах которого осуществляется разработка (модернизация) АС.

ТЗ в части требований по ОБИ подлежит согласованию с подразделением безопасности Общества.

5.2.3 ТЗ на АС должно разрабатываться в соответствии с требованиями федерального законодательства, стандартов, руководящих документов федерального органа исполнительной власти, уполномоченного в области технической защиты информации, применительно к конкретному виду АС.

В ТЗ может содержаться требование соответствия АС одному или нескольким профилям защиты (ПЗ). Требования соответствия ПЗ обязательно включаются в ТЗ в случае, если АС предназначена для обработки информации ограниченного доступа и имеются зарегистрированные ПЗ, определяющие обязательные требования для соответствующих видов АС.

5.2.4 Описание требований соответствия выбранному ПЗ должно содержать:

- обоснование выбора ПЗ, соответствие которому требуется выполнить (обоснованное требование соответствия подразумевает, что АС отвечает всем требованиям ПЗ);

- уточнение ПЗ, определяющее описание требований безопасности, для которых производится дальнейшая детализация требований ПЗ;

- дополнение ПЗ, определяющее формулировки целей и требований безопасности АС, которые дополняют цели и требования ПЗ.

5.2.5 ТЗ разрабатывается по ГОСТ 34.602.

Подготовленные ТЗ могут подвергаться экспертизе в организациях, специализирующихся на разработке или оценке профилей защиты.

5.3 Правила обеспечения безопасности информации при разработке (модернизации) автоматизированных систем

5.3.1 При разработке (модернизации) АС осуществляется разработка программы ОБИ в АС.

5.3.2 При разработке АС должна обеспечиваться безопасность среды разработки АС.

Среда безопасности АС – техническое, программное, организационное окружение АС, а также установленные ограничения, в пределах которых обеспечиваются необходимые условия для поддержания требуемого режима безопасности.

Организация безопасности среды разработки должна быть направлена на устранение или уменьшение угроз безопасности, существующих в месте разработки АС.

Разработчик АС должен иметь документацию по обеспечению безопасности среды разработки, содержащую описание всех мер безопасности, которые необходимы для защиты конфиденциальности и целостности проектных документов и реализации АС в среде разработки. В документации должны быть, как минимум, представлены меры по управлению доступом к АС (его версиям), проектным документам и инструментальным средствам разработки и осуществлению возможных действий с ними.

Должны быть предусмотрены процедуры для пересмотра и оценки (проверки) мер обеспечения безопасности среды разработки.

5.3.3 При разработке и сопровождении АС должен разрабатываться и утверждаться документ, определяющий порядок ОБИ.

В данном порядке, с учетом принятой модели жизненного цикла, для каждого этапа жизненного цикла АС должны быть определены и охарактеризованы соответствующие ему меры ОБИ, в частности:

- уточнение структуры системы ОБИ АС, перечня и содержания задач ОБИ и соответствующих им задач технической защиты информации;

- выбор механизмов решения задач ОБИ и технических путей их реализации в АС, в том числе – контроля эффективности их решения;

- планирование и проведение организационных и технических (с использованием программных и аппаратных средств) мероприятий по ОБИ при разработке АС;

- детальное проектирование функциональных элементов системы ОБИ АС;

- определение порядка решения задач ОБИ в АС на этапах его жизненного цикла (поддержка жизненного цикла АС), в том числе – в случае возникновения нештатных ситуаций вследствие реализации угроз безопасности информации;

- разработка (приобретение), интеграция, конфигурирование АС, тестирование его функций безопасности и разработка документации;

- подготовка АС к процедуре подтверждения соответствия требования по ОБИ (сертификации);

- подготовка к обучению работников.

Структура «Порядка обеспечения безопасности информации при разработке и сопровождении автоматизированных систем» приведена в приложении А.

5.3.4 Процесс проектирования, разработки и сопровождения АС должен поддерживаться необходимым набором методик и инструментальных средств.

К их числу относятся:

- методики выполнения отдельных видов работ;
- интегрированные среды разработки;
- компиляторы;
- СУБД;
- сервисное и специализированное ПО;
- средства автоматизации управления конфигурацией;
- документация к ним и др.

Используемые инструментальные средства должны удовлетворять требованиям принятых стандартов, быть лицензионно чистыми, хорошо апробированными и, при необходимости, сертифицированными в соответствующих системах сертификации.

Все применяемые при разработке и сопровождении АС инструментальные средства и их настройки должны быть описаны в документации разработчика АС.

5.4 Правила обеспечения безопасности информации в процессе тестирования и анализа уязвимости автоматизированных систем

5.4.1 При разработке АС разработчик должен предусмотреть выявление и устранение недостатков в АС в процессе ее сопровождения при эксплуатации.

5.4.2 Меры и процедуры по устранению недостатков должны быть описаны в документации, содержащей методы реагирования на недостатки всех возможных типов.

5.4.3 Документация по процедурам устранения недостатков должна содержать описание способов предоставления пользователям АС информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Если некоторые недостатки не могут быть исправлены немедленно, в процедурах устранения недостатков должно быть предусмотрено применение других, например организационных мер.

5.5 Правила обеспечения безопасности информации при создании проектной и эксплуатационной документации

5.5.1 Правила ОБИ при создании проектной документации

В целях наиболее полного удовлетворения предъявленных к АС требований безопасности, вопросы ОБИ должны рассматриваться на всех уровнях представления проектных решений, начиная с самого абстрактного и завершая окончательной реализацией АС.

Проектная документация включает:

- функциональную спецификацию;
- эскизный проект;
- технический проект;
- рабочий проект.

Конкретные виды разрабатываемых проектных документов должны определяться в соответствии со стандартами, которые используются при разработке АС.

5.5.1.1 Функциональная спецификация должна использоваться для понимания того, как были учтены все функциональные требования по ОБИ АС. Для этого она должна содержать:

- описание всех функций безопасности АС и режимов их выполнения;
- назначение и способы использования всех внешних интерфейсов функций безопасности (далее – ФБИ) АС с обеспечением, где это необходимо, детализации результатов, нештатных ситуаций и сообщений об ошибках.

В целях повышения доверия к соответствию функциональной спецификации функциональным требованиям безопасности АС должна предусматриваться разработка политики информационной безопасности АС.

5.5.1.2 Эскизный проект АС должен использоваться для обоснования того, что АС имеет архитектуру, приемлемую для реализации функциональных требований безопасности.

Эскизный проект должен:

- уточнять функциональную спецификацию, преобразуя ее в представление ФБИ на уровне подсистем;

- определять все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБИ, с описанием функций, поддерживаемых механизмами защиты, реализуемыми этими средствами;

- определять все интерфейсы подсистем ФБИ, которые являются видимыми извне;

- содержать описание назначения и методов использования интерфейсов с детализацией результатов, нештатных ситуаций и сообщений об ошибках.

5.5.1.3 Технический проект должен использоваться как основа для программирования и/или проектирования аппаратуры. Он представляет собой детализированную проектную спецификацию, уточняющую эскизный проект.

Технический проект АС должен содержать описание внутреннего содержания ФБИ в терминах модулей, их взаимосвязей и зависимостей. Для каждого модуля ФБИ технический проект должен описывать назначение, функции, интерфейсы, зависимости и реализацию всех функций, участвующих в осуществлении политики информационной безопасности (далее – ПИБ) АС.

Модули ФБИ не обязательно однозначно отождествляются с конкретными функциями безопасности. В то время как данный модуль может прямо соответствовать как одной, так и нескольким функциям безопасности, возможно также, что несколько модулей необходимо объединить для реализации единственной функции безопасности.

Технический проект должен содержать описание того, как предоставляется каждая из функций, осуществляющих ПИБ АС.

Технический проект должен идентифицировать все интерфейсы модулей ФБИ и определять, какие из интерфейсов модулей ФБИ являются видимыми извне. Представление интерфейсов модулей ФБИ должно содержать описание назначения и методов использования интерфейсов, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

5.5.1.4 Рабочий проект должен использоваться для описания детализированного внутреннего содержания ФБИ на уровне исходного текста программ, схем аппаратных средств и т.д.

Рабочий проект должен однозначно определять ФБИ на таком уровне детализации, что ФБИ могут быть реализованы без дальнейших проектных решений. Он должен быть внутренне непротиворечивым и включать описание взаимосвязей между всеми частями реализации ФБИ.

В представлении материалов рабочего проекта так же, как и для технического проекта, должны учитываться требования по представлению внутренней структуры ФБИ.

5.5.2 Эксплуатационная документация должна использоваться для обеспечения правильной настройки и безопасного применения АС.

Условия безопасной эксплуатации АС должны быть указаны в следующих документах:

- руководство администратора безопасности;
- руководство пользователя.

Информация, представленная в руководствах администратора безопасности и пользователя, должна обеспечивать полное и точное доведение до них ограничений среды применения АС.

5.5.2.1 Руководство администратора безопасности предназначено для понимания им функций безопасности, предоставляемых АС, включая функции, требующие выполнения действий, критичных для безопасности, а также функции, предоставляющие защищаемую информацию.

В руководстве администратора безопасности должны быть отражены все упомянутые в профиле защиты предупреждения пользователям АС, относящиеся к среде безопасности и целям безопасности АС.

Руководство администратора безопасности должно содержать:

- описание функций администрирования безопасности;
- предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации;
- описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией АС;
- описание всех параметров безопасности, контролируемых администратором безопасности, указывая, при необходимости, безопасные значения;
- описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБИ;
- описание всех требований безопасности к среде АС, которые относятся к администрированию безопасности.

Руководство администратора должно быть включено в состав эксплуатационной документации, разрабатываемой для АС.

5.5.2.2 Руководство пользователя должно включать описание реализованных в АС функций безопасности и интерфейсов, руководящие принципы и инструкции по их использованию.

Информация, содержащаяся в руководстве пользователя, должна давать возможность пользователям сформировать правильное представление о возможностях ФБИ и порядке их безопасного использования.

В руководстве необходимо:

- изложить назначение доступных пользователю функции безопасности и порядок их использования для того, чтобы пользователи имели возможность последовательно и действенно обеспечивать безопасность информации;

- требуется разъяснить роль пользователя в поддержании безопасности АС.

В руководстве пользователя должны быть отражены все упомянутые в ПЗ предупреждения пользователям АС, относящиеся к среде безопасности и целям безопасности АС.

Руководство пользователя должно четко представлять все обязанности пользователя, необходимые для безопасной эксплуатации АС, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности АС.

Руководство пользователя должно быть включено в состав эксплуатационной документации, разрабатываемой для АС.

5.6 Правила обеспечения безопасности информации при поставке и вводе автоматизированных систем в эксплуатацию

5.6.1 Организация поставки включает процедуры поддержки безопасности в процессе передачи АС как при первоначальной поставке, так и при последующей модификации. При организации поставки предусматривают специальные меры и процедуры, требуемые для подтверждения подлинности передаваемой АС, исключения возможности преднамеренного и непреднамеренного внесения изменений в актуальную версию, замену ее фальсифицированной версией.

5.6.2 Документация по организации поставки включает описание всех процедур, необходимых для поддержки безопасности. В документации должны быть описаны процедуры и технические меры, обеспечивающие обнаружение и предотвращение нарушения информационной безопасности.

5.6.3 Процедуры установки, генерации и запуска должны обеспечивать безопасный переход от нахождения АС под контролем системы управления конфигурацией разработчика к начальным операциям в среде эксплуатации. Они должны предусматривать меры и процедуры контроля правильности формирования поставляемой версии АС, настройки всех необходимых параметров и функций информационной безопасности АС.

Процедуры должны содержаться в отдельном документе или включаться в другую эксплуатационную документацию.

5.6.4 Контроль ОБИ АС при ее установке, генерации и запуске осуществляется подразделением безопасности Общества.

5.7 Правила обеспечения безопасности информации на этапе эксплуатации автоматизированных систем

5.7.1 Правила ОБИ в АС в процессе ее эксплуатации включают:

- правила планирования и организации применения мер и средств обеспечения безопасности АС;
- правила установления и поддержания среды безопасности АС;
- правила контроля эффективности обеспечения безопасности информации в процессе эксплуатации АС;
- правила анализа проблем и выявленных недостатков в части эффективности ОБИ в АС;
- правила доработки модернизации АС;
- правила поддержки пользователей АС;
- правила допуска сторонних организаций и их представителей к обслуживанию и модернизации АС;
- правила реагирования на возникновение нештатных ситуаций;
- правила ОБИ при эксплуатации АС.

5.7.2 Планирование и организация применения мер и средств обеспечения безопасности как входящих в состав системы ОБИ АС, так и дополнительно используемых в случае необходимости в соответствии с нормативными документами и эксплуатационной документацией осуществляется в соответствии с разрабатываемым «Порядком обеспечения информационной безопасности при эксплуатации АС».

Данный порядок должен основываться на политике информационной безопасности, разработанной для АС.

Структура документа приведена в приложении Б.

5.7.3 Установление и обеспечение среды безопасности АС связаны с соблюдением задания по безопасности.

Факторами, определяющими среду безопасности АС, являются:

- угрозы безопасности АС;
- требования ПИБ АС;
- другие факторы, относящиеся к месту эксплуатации АС.

Должны быть предусмотрены процедуры для оценки (проверки) и пересмотра мер обеспечения среды безопасности АС.

5.7.4 Контроль эффективности ОБИ в процессе эксплуатации АС проводится с целью оценки соответствия параметров и характеристик АС и ее среды безопасности принятой ПИБ АС.

Контроль эффективности ОБИ в процессе эксплуатации АС проводится в форме оценки (проверки).

Контроль эффективности ОБИ проводится:

- при вводе АС в эксплуатацию;
- периодически в процессе эксплуатации АС;
- при изменениях ПИБ АС.

При контроле эффективности ОБИ АС оцениваются:

- соответствие мер, применяемых в среде АС, требованиям, определенным в задании по безопасности;
- соответствие настроек АС значениям, определяемым эксплуатационной документацией и ПИБ АС;
- реализация установленных мер по нейтрализации выявленных уязвимостей АС.

Контроль эффективности ОБИ АС осуществляется подразделениям безопасности Общества.

5.7.5 Анализ возникающих проблем и выявленных недостатков в части эффективности ОБИ в АС проводится с целью устранения проблемных вопросов, возникающих при эксплуатации АС.

Анализ проблем и выявленных недостатков в части эффективности ОБИ в АС проводится:

- при вводе АС в эксплуатацию;
- постоянно в процессе эксплуатации АС;
- периодически путем тестирования АС на предмет выявления угроз безопасности;
- при изменениях в ПИБ АС.

5.7.6 При проведении доработок и модернизации АС осуществляется:

- проведение анализа влияния изменений на информационную безопасность АС;
- осуществление оценки соответствия АС требованиям по ОБИ после проведенных доработок и изменений.

5.7.7 При планировании изменений в АС и ее среде безопасности проводится анализ влияния планируемых изменений на ОБИ АС.

Для каждого изменения, относящегося к заданию по безопасности или представлению функций безопасности АС, анализ влияния на ОБИ должен содержать краткое описание изменения и всех последствий, к которым оно приводит.

Для каждого изменения, которое приводит к модификации рабочего проекта АС, анализ влияния на безопасность должен содержать результаты тестирования, показывающие, что функции безопасности АС правильно реализованы и после проведения изменения.

Для каждого применяемого требования по оценке уязвимости анализ влияния на ОБИ должен содержать все данные, необходимые для оценки АС, которые подлежат изменению, и обоснование необходимости изменения данных.

5.7.8 Свидетельство, отражающее проведенные изменения и их результаты, должно включать:

- состав АС;
- список идентифицированных уязвимостей в АС.

Состав АС содержит описание элементов конфигурации, которые составляют текущую версию АС.

Список идентифицированных уязвимостей содержит уязвимости, выявленные в результате:

- анализа разработчиком при оценке уязвимости АС (если она проводилась для сертифицированной версии АС);
- обнаружения любых других недостатков безопасности, обработанных с использованием процедур устранения недостатков, требуемых для сертифицированной версии АС.

Список идентифицированных уязвимостей в текущей версии АС должен для каждой уязвимости содержать доказательства, что она не может быть реализована в среде АС.

5.7.9 Оценка соответствия АС требованиям по ОБИ после проведенных доработок и изменений в АС осуществляется по СТО Газпром 4.2-5-001.

5.7.10 Правила поддержки пользователей АС

Пользователи АС должны иметь беспрепятственный доступ к документам, регламентирующим ОБИ в процессе эксплуатации АС.

С пользователями АС необходимо проводить плановые (не реже 1 раза в 6 месяцев) и внеплановые (при изменении системы ОБИ) занятия (инструктажи).

5.7.11 Правила допуска сторонних организаций и их представителей к обслуживанию и модернизации АС

Порядок допуска к АС должен быть определен в нормативных документах Общества.

Свободный доступ к АС должен быть запрещен.

5.7.12 Правила реагирования на возникновение нештатных ситуаций

В Обществе должен быть разработан «План реагирования на внештатные ситуации (при возникновении или угрозе возникновения угроз безопасности информации)», в котором однозначно определяется:

- порядок действий по обеспечению сохранности и целостности информации при внештатной ситуации;

- меры предосторожности для предотвращения угрозы безопасности информации при внештатной ситуации;

- меры предосторожности для предотвращения ущерба работникам при возникновении угрозы безопасности информации.

План подлежит периодическому пересмотру, а также уточнению с появлением новых потенциальных угроз безопасности информации.

5.7.14 Обеспечение требований по ОБИ возлагается на структурное подразделение Общества, осуществляющее эксплуатацию АС.

Контроль выполнения установленных требований по ОБИ осуществляет подразделение безопасности Общества.

5.7.15 В процессе эксплуатации должна осуществляться поддержка доверия к информационной безопасности АС. Для этого в документацию своевременно должны вноситься изменения, вызванные обнаружением новых угроз или уязвимостей безопасности, изменением условий эксплуатации АС.

Подтверждение выполнения АС установленных целей безопасности при изменениях в сертифицированной версии АС или среде ее применения может быть осуществлено двумя путями:

- посредством оценки новой версии АС;

- посредством реализации процедур поддержки доверия к безопасности АС.

Для обеспечения поддержки доверия к безопасности АС разработчиком должны быть подготовлены:

- план поддержки доверия;

- отчет о категорировании компонентов АС.

5.7.15.1 План поддержки доверия

План поддержки доверия определяет процедуры, которые необходимо выполнять разработчику по мере изменений в АС или ее среде безопасности для обеспечения поддержки доверия, которое было установлено в сертифицированной АС.

План поддержки доверия распространяется на один цикл поддержки доверия, который представляет собой период от завершения последней выполненной оценки АС до завершения следующей запланированной переоценки (новой оценки).

План поддержки доверия должен определять пределы изменений, которые могут быть сделаны в АС без необходимости его переоценки. За пределами плана поддержки доверия находятся следующие типы изменений, которые обязательно приводят к переоценке:

- значительное изменение задания по безопасности (т.е. значительные изменения среды безопасности, целей безопасности, функциональных требований безопасности или любое повышение требований доверия);

- значительное изменение внешних интерфейсов функций безопасности АС, отнесенных к категории обеспечивающих осуществление политики безопасности АС;

- значительное изменение подсистем функций безопасности АС, отнесенных к категории обеспечивающих осуществление политики безопасности АС.

В плане поддержки доверия требуется определить или сослаться на процедуры, которые будут использоваться для обеспечения поддержки доверия к АС на протяжении данного цикла поддержки.

Рекомендуется применять следующие типы процедур:

- по управлению конфигурацией, которые контролируют и регистрируют изменения в АС для поддержки анализа их влияния на безопасность, проводимого разработчиком, а также в сопроводительной документации (включая собственно план поддержки доверия);

- поддержке документального свидетельства поддержки доверия;

- анализу влияния на безопасность изменений, затрагивающих АС (включая изменения типа новых угроз или методов воздействия в среде безопасности АС), а также сопровождению отчета о категорировании компонентов АС по мере внесения изменений;

- устранению недостатков, включая отслеживание и исправление всех недостатков безопасности, о которых было сообщено.

5.7.15.2 Отчет о категорировании компонентов АС

Назначение отчета о категорировании компонентов АС состоит в том, чтобы определить категорирование компонентов АС (например, подсистем функций безопасности АС) по их отношению к безопасности. Это категорирование занимает центральное место как в анализе влияния на безопасность, проводимом разработчиком, так и при последующей переоценке АС.

Отчет о категорировании компонентов АС распространяется на все представления функций безопасности АС на поддерживаемом уровне доверия. Отчет о категорировании компонентов АС должен также идентифицировать:

- любые аппаратные, программно-аппаратные и программные компоненты, которые являются внешними по отношению к АС (например, аппаратные или программные платформы) и удовлетворяют требованиям безопасности АС, определенным в задании по безопасности (ЗБ);

- любые инструментальные средства разработки, модификация которых будет влиять на требуемое доверие к тому, что АС удовлетворяет своему заданию по безопасности.

Отчет о категорировании компонентов АС должен содержать описание подхода, используемого для категорирования компонентов АС. Как минимум, компоненты АС требуется разделить на осуществляющие и не осуществляющие политику безопасности АС. Описание схемы категорирования предназначено дать возможность разработчику выбрать категорию, к которой следует отнести каждый новый компонент АС, а также, когда потребуется, изменить категорию существующего компонента после изменений в АС или ее ЗБ.

Начальное категорирование компонентов АС должно быть основано на свидетельстве, представленном разработчиком для оценки АС и независимо подтвержденном испытательной лабораторией.

Во всех тех случаях, когда требуется поддержка доверия в последующих версиях АС, в задание по безопасности целесообразно включать компонент AMA_CAT.1 требований ИСО/МЭК 15408. Он применяется независимо от того, достигается ли поддержка доверия использованием этих требований или же путем периодической переоценки АС.

Требования поддержки доверия к безопасности АС определяются в соответствии с ИСО/МЭК 15408 в зависимости от выбранной разработчиком стратегии поддержки доверия.

5.7.15.3 Анализ влияния изменений на безопасность АС

Назначение анализа влияния на безопасность состоит в том, чтобы посредством проводимого разработчиком анализа по определению влияния на безопасность всех изменений, затрагивающих АС после ее сертификации, получить уверенность в том, что доверие к АС поддерживается на установленном уровне.

При анализе влияния на безопасность, проводимом разработчиком, должен использоваться отчет о категорировании компонентов АС, так как изменения в компонентах, осуществляющих политику безопасности АС, могут повлиять на доверие к тому, что АС продолжает отвечать своему заданию по безопасности после изменений. Поэтому все такие изменения требуют анализа их влияния на безопасность, чтобы показать, что они не нарушают доверия к безопасности АС.

Анализ влияния на безопасность должен идентифицировать все новые и модифицированные компоненты АС, которые категорированы как осуществляющие политику безопасности изделия.

Для каждого изменения, относящегося к ЗБ или представлению ФБИ АС, анализ влияния на безопасность должен содержать краткое описание изменения и всех последствий, к которым оно приводит на более низких уровнях представления, идентифицировать все ФБИ и компоненты АС, категорированные как осуществляющие ПИБ, на которые влияет данное изменение.

Для каждого изменения, которое приводит к модификации рабочего проекта АС или ее среды, анализ влияния на безопасность должен идентифицировать свидетельство тестирования, показывающее для требуемого уровня доверия, что ФБИ остаются правильно реализованными и после проведения изменения.

Для каждого применяемого к АС требования по управлению конфигурацией, поддержке жизненного цикла, поставке и вводу в эксплуатацию и эксплуатационной документации анализ влияния на безопасность должен идентифицировать все материалы, поставляемые для оценки, которые изменяются, и содержать краткое описание каждого изменения и его воздействия на доверие к безопасности АС.

Для каждого применяемого требования по оценке уязвимости анализ влияния на безопасность должен определять, какие материалы, поставляемые для оценки АС, изменяются, а какие нет, и привести доводы для принятого решения, обновлять или нет данный поставляемый материал.

5.7.15.4 Свидетельство поддержки доверия к безопасности АС

Свидетельство поддержки доверия должно демонстрировать, что разработчик следует процедурам поддержки доверия, указанным в плане поддержки доверия к безопасности. Свидетельство поддержки доверия представляется разработчиком в установленных в плане поддержки доверия к безопасности контрольных точках текущего цикла поддержки доверия к безопасности АС.

Документация поддержки доверия, представляемая разработчиком, должна включать:

- список конфигурации АС;
- список идентифицированных уязвимостей в АС;
- свидетельство следования процедурам поддержки доверия, определенным в плане поддержки доверия к безопасности.

Список конфигурации должен содержать описание элементов конфигурации, которые составляют текущую версию АС.

В список уязвимостей следует включить уязвимости, выявленные в результате:

- анализа разработчиком при оценке уязвимости АС (если она проводилась для сертифицированной версии АС);

- обнаружения любых других недостатков безопасности, обработанных с использованием процедур устранения недостатков, требуемых для сертифицированной версии АС.

Список идентифицированных уязвимостей в текущей версии АС должен показать для каждой уязвимости, что она не может быть использована в предполагаемой среде АС.

Свидетельство следования процедурам поддержки доверия из плана поддержки доверия к безопасности распространяется на все процедуры, относящиеся к управлению конфигурацией, поддержке свидетельства доверия, выполнению анализа влияния на безопасность и устранению недостатков.

5.7.15.5 Сертификация версии АС

Соответствие АС требованиям безопасности информации должно подтверждаться в порядке, установленном СТО Газпром 4.2-5-001.

5.7.15.6 Оценка (проверка) поддержки доверия

Действия разработчика по выполнению планов и процедур поддержки доверия и анализу влияния на безопасность изменений, которым подвергается АС в процессе мониторинга поддержки доверия, должны независимо проверяться испытательной лабораторией. Эта проверка, называемая «аудит поддержки доверия» (аудит поддержки доверия к безопасности), должна проводиться периодически в фазе мониторинга цикла поддержки доверия к АС.

Оценку (проверку) поддержки доверия к безопасности проводят в соответствии с графиком, определенным в плане поддержки доверия к безопасности. В основу планирования может быть положен определенный период времени (например, ежегодная оценка (проверка) поддержки доверия к безопасности), или же планирование может быть связано с ожидаемыми новыми выпусками АС.

Испытательная лаборатория должна непосредственно ознакомиться с условиями разработки и сопровождения АС, чтобы выполнить экспертизу требуемого свидетельства поддержки доверия, но не исключаются и другие способы проверки.

Центральное место в оценке (проверке) поддержки доверия к безопасности занимает проверка испытательной лабораторией анализа влияния на безопасность, проведенного разработчиком. Оценка (проверка) поддержки доверия к безопасности будет способствовать подтверждению анализа, проведенного разработчиком (и, следовательно, уверенности в качестве анализа), обеспечивая подтверждение правильности утверждения разработчика, что доверие к АС поддерживается для ее текущей версии.

В порядке оценки (проверки) поддержки доверия к безопасности испытательная лаборатория проверяет согласованность списка конфигурации и анализа влияния на безопасность с текущей версией АС для компонентов АС, которые изменились по сравнению с сертифицированной версией АС.

При оценке (проверке) поддержки доверия к безопасности требуется, чтобы испытательная лаборатория подтвердила, что выполнялось функциональное тестирование текущей версии АС. Испытательная лаборатория должна выборочно проверить тестовую документацию для подтверждения, что тестирование разработчиком показывает правильность выполнения функций безопасности АС, а покрытие тестами и глубина тестирования соразмерны поддерживаемому уровню доверия.

5.8 Правила устранения недостатков автоматизированных систем в процессе эксплуатации

5.8.1 При разработке АС разработчик должен определить порядок выявления и устранения недостатков при эксплуатации АС.

Меры и процедуры по устранению недостатков должны быть описаны в документации, содержащей методы реагирования на недостатки всех возможных типов.

5.8.2 Процедуры устранения недостатков должны предусматривать представление описания сути и последствий каждого недостатка безопасности и описание действий по исправлению каждого недостатка безопасности.

5.8.3 Документация по процедурам устранения недостатков должна содержать описание способов предоставления пользователям АС информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Если некоторые недостатки не могут быть исправлены немедленно, в процедурах устранения недостатков должно быть предусмотрено применение других (например, организационных) мер.

5.9 Правила обеспечения безопасности информации при снятии автоматизированных систем с эксплуатации

5.9.1 Действия по снятию с эксплуатации должны гарантировать последовательный вывод АС или отдельных частей АС из применения и сохранение связанной с ними значимой информации таким образом, чтобы вся информация или какая-то ее часть могла бы быть восстановлена в будущем в случае необходимости.

При снятии АС с эксплуатации осуществляется планирование и реализация мероприятий по архивированию необходимых информационных ресурсов и очистке носителей информации, использовавшихся в АС.

5.9.2 Правила архивирования информационных ресурсов

При сохранении информации должны выбираться такие методы ее архивирования, которые позволили бы ее восстановить в будущем с учетом изменения применяемых программно-аппаратных платформ. Особое внимание должно уделяться надлежащему сохранению функционально-ориентированных данных, используемых в процессе функционирования АС, так, чтобы эти данные были либо переданы в другую АС, либо архивированы для потенциального будущего использования. Должны быть также рассмотрены все юридические аспекты, связанные с уничтожением и архивированием информации, использовавшейся в АС.

5.9.3 Правила очистки носителей информации

В зависимости от уровня конфиденциальности информации, хранящейся на носителях информации, должны применяться методы их очистки, гарантирующие уровни остаточного магнитного, электростатического или иного представления информации, исключающие ее считывание.

Приложение А

(справочное)

Порядок обеспечения безопасности информации при разработке и сопровождении автоматизированных систем

Приложение Б

(справочное)

Порядок обеспечения информационной безопасности при эксплуатации автоматизированных систем

ОКС 01.120

Ключевые слова: информационная безопасность, требования к объектам защиты, этапы жизненного цикла
