Руководящий документ
Безопасность информационных технологий.
Руководство по регистрации профилей защиты

Гостехкомиссия России, 2003 год

1. Область применения

Руководящий документ (далее документ) определяет процедуры, которые используются при формировании, ведении и использовании реестра профилей защиты и пакетов, предназначенных для задания требований безопасности изделий информационных технологий.

Документ предназначен для заказчиков, разработчиков и пользователей изделий информационных технологий, а также для участников систем сертификации изделий ИТ по требованиям безопасности информации.

2. Нормативные ссылки

В документе использованы ссылки на следующие нормативные документы.

ГОСТ Р ИСО/МЭК 15408—2002 Информационная технология. – Методы и средства обеспечения безопасности. – Критерии оценки безопасности информационных технологий. – Части 1, 2, 3.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

ISO/IEC 15292-2001, Information technology – Security techniques – Protection Profile registration procedures.

3. Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями.

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта оценки (ГОСТ Р ИСО/МЭК 15408).

Заключение об успешной оценке: Заключение, подтверждающее, что профиль защиты был успешно оценен согласно критериям, приведенным в разделе 4 части 3 РД «Критерии оценки безопасности информационных технологий».

Заявитель: Физическое или юридическое лицо, подающее заявку на включение ПЗ или пакета в реестр.

Объект оценки: Подлежащие оценке продукт ИТ или система ИТ(ГОСТ Р ИСО/МЭК 15408).

Орган регистрации: Орган, уполномоченный Гостехкомиссией России для регистрации профилей защиты и пакетов.

Пакет: Многократно используемая совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединенных для достижения определенных целей безопасности (ГОСТ Р ИСО/МЭК 15408).

Профиль защиты: Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя (ГОСТ Р ИСО/МЭК 15408).

Регистрационная метка: Метка, присваиваемая ПЗ или пакету при включении в реестр и уникально его идентифицирующая.

Регистрация: Процесс включения ПЗ или пакета в реестр.

Реестр: Совокупность записей (в электронном или электронном и бумажном виде), включающих в себя регистрационные метки, а также связанную с ними дополнительную информацию.

Сертификат ПЗ: Документ, удостоверяющий соответствие ПЗ критериям, приведенным в разделе 4 части 3 РД «Критерии оценки безопасности информационных технологий».

Элемент реестра: Информация из реестра, относящаяся к конкретному ПЗ или пакету.

4. Сокращения

ЗБ — задание по безопасности

ИТ — информационная технология

ОО — объект оценки

ОР — орган регистрации

ОУД — оценочный уровень доверия

ПД — пакет требований доверия

ПЗ — профиль защиты

РД — руководящий документ

ФП — функциональный пакет

5. Технические спецификации

5.1. Регистрационная метка

Каждый ПЗ или пакет, зарегистрированный в соответствии с настоящим документом, должен иметь регистрационную метку, присвоенную ОР, которая уникально идентифицирует ПЗ или пакет в реестре. Регистрационная метка состоит из следующих частей, разделенных дефисами:
- тип элемента реестра;
- год регистрации;
- регистрационный номер.

Установлены следующие три типа элемента реестра:
-"ПЗ – для профиля защиты;
-"ПД – для пакета требований доверия;
-"ФП – для функционального пакета.

Год регистрации — год внесения элемента в реестр (четыре цифры).

Регистрационный номер — порядковый номер в текущем году (три цифры).

Пример: ПЗ?2003?001.

5.2. Описание элемента реестра

5.2.1. Профили защиты

Каждая заявка на регистрацию ПЗ должна включать описание регистрируемого ПЗ. Описание должно соответствовать требованиям к содержанию ПЗ, приведенным в приложении Б к части 1 РД «Критерии оценки безопасности информационных технологий».

5.2.2. Пакеты

Каждая заявка на регистрацию функционального пакета или пакета требований доверия должна включать описание пакета. Описание должно содержать:
- краткий обзор пакета;
- спецификацию совокупности функциональных компонентов или компонентов доверия.

Компоненты для функциональных пакетов должны быть выбраны из части 2 РД «Критерии оценки безопасности информационных технологий» или же сформулированы в соответствии с требованиями к спецификации функциональных компонентов, приведенными в разделе 2 части 2 указанного РД.

Компоненты для пакетов требований доверия должны быть выбраны из части 3 РД «Критерии оценки безопасности информационных технологий» или же сформулированы в соответствии с требованиями к спецификации компонентов доверия, приведенными в подразделе 2.1 части 3 указанного РД.

Описание пакета может содержать и другую информацию. Эта информация может быть представлена в виде одного или нескольких разделов ПЗ или ЗБ, определенных соответственно в приложениях Б и В к части 1 РД «Критерии оценки безопасности информационных технологий». В этом случае эта информация может быть непосредственно включена в ПЗ или ЗБ, в котором применяется данный пакет.

6. Функции органа регистрации ПЗ и пакетов

Основными функциями ОР являются:
- ведение учета заявок на регистрацию ПЗ и пакетов;
- рассмотрение заявок на регистрацию ПЗ и пакетов;
- назначение уникальных регистрационных меток ПЗ и пакетам, включаемым в реестр;
- уведомление заявителей о решениях по их заявкам;
- уведомление заявителей о результатах действий, касающихся их элементов реестра;
- сопровождение реестра в соответствии с установленными правилами;

- обеспечение доступа к актуальной версии реестра;
- выполнение процедуры апелляции, приведенной в разделе 13 настоящего документа;
- разработка методических документов по регистрации ПЗ и пакетов.

7. Информация, включаемая в заявку на регистрацию

Заявка на регистрацию ПЗ или пакета должна содержать следующую информацию.

- Название организации (физического лица) заявителя и его контактную информацию. Контактная информация должна включать почтовый адрес и/или адрес E-mail, номер телефона и/или факса.
- Тип объекта, представленного для регистрации (ПЗ, функциональный пакет или пакет требований доверия).
- Декларацию того, представлен ли ПЗ или пакет для регистрации как новый элемент или заменяющий элемент. Если ПЗ или пакет представлен как заменяющий элемент, то должны быть указаны регистрационные метки действующих элементов реестра, подлежащих удалению при замене.
- Подтверждение от заявителей заменяемых элементов, что при принятии заменяющих элементов они согласны на удаление своих элементов.
- Декларацию того, представлен ли ПЗ или пакет для регистрации как завершенный или как проект.
- Описание нового ПЗ или пакета, структурированное в соответствии с подразделом 5.2 настоящего документа.
- Аннотацию ПЗ или пакета.
- Декларацию, что описание ПЗ или пакета, представленного для регистрации, удовлетворяет требованиям подраздела 5.2 настоящего документа.

Описание ПЗ или пакета, представленного для регистрации, должно содержать все обязательные структурные элементы, требуемые подразделом 5.2 настоящего документа.

Описание не должно иметь ссылки на спецификации других ПЗ или пакетов вне зависимости от того, зарегистрированы эти ПЗ (пакеты) или нет.

Лектронная копия описания должна поставляться вместе с заявкой в формате, установленном ОР.

8. Рассмотрение заявок на регистрацию ПЗ или пакетов

8.1. Начальная обработка

При начальной обработке заявки в ОР проверяется наличие информации, перечисленной в разделе 7 настоящего документа. ОР должен либо отклонить заявку, либо присвоить ПЗ или пакету регистрационную метку и ввести ПЗ или пакет в реестр со статусом "проходящий подтверждение соответствия". Заявитель должен быть уведомлен об этом. Если заявка отклонена, ОР должен указать причины отклонения заявки.

Начальная обработка должна занимать не более 14 дней после получения заявки.

8.2. Подтверждение соответствия

ОР должен выполнить структурную проверку описания, представленного в заявке на регистрацию. Если выявлено отсутствие разделов или представленная информация не совместима с действующей версией РД «Критерии оценки безопасности информационных технологий», ОР должен сообщить о недостатках заявителю для разъяснения или исправления. Если заявитель не может устранить недостатки в течение 14 дней после получения уведомления, процедура подтверждения соответствия ПЗ или пакета должна быть прекращена.

Если представлено заключение об успешной оценке или сертификат, то ОР должен связаться с организацией, которая выдала заключение или сертификат, и отослать ей копию заявки. От организации, проводившей оценку или сертификацию, требуется в течение месяца подтвердить, что описание ПЗ, проходившего оценку, идентично представленному для регистрации, и что ПЗ был успешно оценен. Если подтверждение в указанный срок не получено, ОР должен объявить заключение или сертификат не принятым и уведомить об этом заявителя.

ОР должен завершить процедуру подтверждения соответствия, включая, при необходимости, уведомление заявителя о недостатках, в течение трех месяцев после получения заявки. Если заявитель не устранил отмеченные недостатки, то элементу реестра присваивается статус "отклонен как не прошедший подтверждение соответствия". При положительном результате элементу реестра присваивается статус "зарегистрирован" или, для завершенного ПЗ с проверенным заключением об успешной оценке или сертификатом, – соответственно "оценен" или "сертифицирован".

Примечание. Проводимое ОР подтверждение соответствия ограничено проверкой структуры и согласованности элемента реестра, определенными выше, но не включает оценку описания с использованием РД «Критерии оценки безопасности информационных технологий». ОР не выполняет

какую-либо техническую проверку описания ПЗ или пакета, и поэтому возможно, что на регистрацию будет принято неполное или противоречивое описание ПЗ или пакета. Только там, где элемент имеет статус "оценен" или "сертифицирован", в реестре фактически зафиксировано утверждение о технической правильности элемента реестра.

9. Критерии отклонения заявок на регистрацию

Заявка на регистрацию ПЗ или пакета должна быть отклонена, если:
- отсутствуют обязательные составляющие заявки;
- в заявке отсутствует или не полностью представлена требуемая информация (кроме случаев, когда это разрешено настоящим документом);
- описание ПЗ или пакета для регистрации не соответствует требованиям настоящего документа.

10. Операции над элементами реестра

10.1. Уведомление об устаревших элементах

Заявитель элемента реестра может уведомить ОР о том, что рассматриваемый элемент неприемлем для дальнейшего использования как устаревший. Статус элемента реестра должен быть заменен на "устарел".

10.2. Обновление проектов технических спецификаций

Заявитель проекта элемента реестра может подать заявку на обновление (полностью или частично) зарегистрированного описания элемента реестра или его аннотации. ОР должен произвести структурную проверку пересмотренного описания или аннотации. Если ОР выявит отсутствие требуемых разделов или представленная информация будет не совместима с настоящим документом или действующей версией РД «Критерии оценки безопасности информационных технологий», то ОР должен сообщить об этом заявителю для разъяснения или исправления. При отсутствии указанных проблем элемент должен быть обновлен в соответствии с представленными материалами в течение 14 дней после получения заявки.

10.3. Уведомление о недостатках

ОР обязан принимать к сведению сообщения об обнаруженных ошибках, противоречии или неоднозначности в элементе реестра. После получения сообщения ОР должен уведомить заявителя элемента реестра о заявленном недостатке.

Для незавершенных элементов реестра (проектов) заявителю разрешается не отвечать на сообщение о недостатках, а представить обновленное описание ПЗ или пакета для решения проблемы.

Завершенный элемент реестра останется без изменений, если в течение месяца лицо, заявившее о недостатке, аннулирует свое уведомление. В противном случае заявитель элемента должен за то же время предоставить уведомление об устранении недостатка, в котором изложена проблема и предоставлено ее решение. ОР должен дополнить элемент реестра сообщением о недостатке и уведомлением о его устранении. ОР должен также послать копию уведомления об устранении лицу, сообщившему о недостатке.

Если требуется уведомление об устранении недостатка, но оно не представлено заявителем в установленный срок, то элемент реестра получает статус "устарел".

Элемент остается со статусом "устарел" в течение 18 месяцев. По истечении этого срока его статус автоматически понижается до "исключен", указывая, что данный элемент более не предназначен для использования. Элементы со статусом "исключен" остаются в реестре, чтобы сохранить возможность ссылки на них.

10.4. Другие запросы на обновление элементов

В случае, если элемент реестра ПЗ со статусом "зарегистрирован" успешно оценен или сертифицирован, то статус элемента должен быть обновлен соответственно на "оценен" или "сертифицирован".

10.5. Удаление элементов реестра

После получения регистрационной метки элемент реестра не может быть удален из реестра.

Примечание. Элементам, которые более не применимы, присваивается статус "исключен".

11. Конфиденциальность информации, содержащейся в реестре

Элементы реестра не должны содержать секретные или конфиденциальные материалы. ОР должен обеспечить доступность всей информации, содержащейся в имеющихся элементах реестра.

12. Публикация реестра

ОР должен вести реестр всех ПЗ и пакетов, которые он принял для регистрации. Реестр должен публиковаться на русском языке. Перевод реестра или его отдельных элементов может, по усмотрению ОР, предоставляться на других языках.

Элемент реестра для каждого ПЗ или пакета должен содержать, по меньшей мере, следующую информацию:
- регистрационную метку данного элемента;
- тип зарегистрированного объекта: "профиль защиты", "функциональный пакет" или "пакет требований доверия";
- является элемент новым или заменяющим;
- является элемент завершенным или проектом;
- статус элемента: "проходящий подтверждение соответствия", "отклонен как не прошедший подтверждение соответствия", "зарегистрирован", "оценен", "сертифицирован", "устарел", "исключен";
- дату включения элемента в реестр;
- дату последнего изменения элемента;
- название организации (или ФИО) и контактную информацию заявителя элемента;
- при статусе элемента "оценен" или "сертифицирован" – название и контактную информацию организации, выдавшей заключение об успешной оценке или сертификат;
- аннотацию ПЗ или пакета;
- описание ПЗ или пакета, структурированное в соответствии с подразделом 5.2 настоящего документа;
- для завершенных элементов – все актуальные сообщения о недостатках и уведомления об устранении недостатков;
- версия РД «Критерии оценки безопасности информационных технологий», по которой элемент был проверен ОР;
- регистрационные метки всех элементов, замененных данным элементом;
- регистрационную метку элемента, заменяющего данный элемент.

Извлечения из реестра и полные копии реестра должны содержать обязательное примечание, что за содержание элементов реестра отвечает не ОР, а заявители элементов. В примечании должно быть также указано, что подтверждение соответствия элементов реестра, выполняемое ОР, ограничено их структурой и непротиворечивостью и не включает оценку описания на основе РД «Критерии оценки безопасности информационных технологий». Только для элементов со статусом "оценен" или "сертифицирован" в реестре зафиксировано утверждение о технической правильности описания.

13. Процедура апелляции

В случае разногласий между заявителем элемента реестра и ОР, заявитель должен в письменном виде обратиться к руководителю ОР, излагая суть разногласий и предложения по их разрешению.

Руководитель ОР должен рассмотреть вопрос по существу и в течение одного месяца сообщить решение в письменном виде заявителю.

Если заявитель не удовлетворен решением руководителя ОР, то он должен в течение месяца подать апелляцию руководителю ОР в письменной форме, излагая свои основания несогласия с решением.

Руководитель ОР должен рассмотреть суть апелляции и в течение месяца подтвердить или изменить свое предыдущее решение.

Если заявитель не удовлетворен решением руководителя ОР по апелляции, то он должен в течение одного месяца обратиться в письменном виде в вышестоящий орган, излагая суть разногласий, решение руководителя ОР и основания для неприятия его решения.