Руководящий документ
Безопасность информационных технологий.
Положение по разработке профилей защиты и заданий по безопасности

Гостехкомиссия России, 2003 год

1. Область применения

Настоящее Положение определяет порядок разработки, оценки, регистрации и публикации профилей защиты и заданий по безопасности для продуктов и систем информационных технологий, предназначенных для обработки информации, отнесенной к информации ограниченного доступа в соответствии с законодательством Российской Федерации.

Положение предназначено для использования организациями-заказчиками профилей защиты, разработчиками профилей защиты, продуктов и систем информационных технологий, организациями-пользователями продуктов и систем информационных технологий, а также органами по сертификации и испытательными лабораториями при выполнении ими работ по обязательной сертификации средств защиты информации в соответствии с федеральным законом "О техническом регулировании".

2. Нормативные ссылки

В настоящем руководящем 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.

Руководящий документ - Безопасность информационных технологий - Руководство по разработке семейств профилей защиты, Гостехкомиссия России, 2003.

Безопасность информационных технологий - Руководство по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003.

Руководящий документ - Безопасность информационных технологий - Руководство по регистрации профилей защиты, Гостехкомиссия России, 2003.

3. Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями.

3.1 **Активы** (assets): Информация или ресурсы, подлежащие защите контрмерами изделия ИТ (ГОСТ Р ИСО/МЭК 15408).

3.2 **Доверие** (assurance): Основание для уверенности в том, что изделие ИТ отвечает своим целям безопасности(ГОСТ Р ИСО/МЭК 15408).

3.3 **Задание по безопасности** (security target): Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ(ГОСТ Р ИСО/МЭК 15408).

3.4 **Заявитель** (sponsor): физическое или юридическое лицо, подающее заявку на оценку, сертификацию и регистрацию ПЗ.

3.5 **Изделие ИТ** (IT product): Обобщенный термин для продуктов и систем ИТ.

3.6 **Орган регистрации** (registration body): Орган, уполномоченный Гостехкомиссией России для регистрации профилей защиты и пакетов.

3.7 **Оценка безопасности** (security evaluation): Исследования (испытания), проводимые для проверки соответствия ПЗ, ЗБ или изделия ИТ установленным требованиям безопасности.

3.8 **Политика безопасности организации** (organizational security policies): Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности(ГОСТ Р ИСО/МЭК 15408).

3.9 **Предположения** (assumptions): Условия, которые должны быть обеспечены в среде, чтобы изделие ИТ могло рассматриваться как безопасное.

3.10 **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(ГОСТ Р ИСО/МЭК

15408).
3.11 **Профиль защиты** (protection profile): Независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя(ГОСТ Р ИСО/МЭК 15408).
3.12 **Система ИТ** (IT system): Специфическое воплощение изделия ИТ с конкретным назначением и условиями эксплуатации(ГОСТ Р ИСО/МЭК 15408).
3.13 **Среда безопасности** (security environment): Область среды, в пределах которой предусматривается обеспечение необходимых условий для поддержания требуемого режима безопасности изделия ИТ.
3.14 **Угроза** (threat): Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его собственнику.
3.15 **Функция безопасности** (security function): Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности(ГОСТ Р ИСО/МЭК 15408).
3.16 **Цель безопасности** (security objective): Сформулированное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям(ГОСТ Р ИСО/МЭК 15408).

4. Сокращения

РД - руководящий документ

ИТ - информационная технология

ПЗ - профиль защиты

ЗБ - задание по безопасности

5. Общие положения

Требования безопасности, предназначенные для типовых механизмов, продуктов и систем информационных технологий, должны оформляться в виде профилей защиты в соответствии с РД Гостехкомиссии России "Критерии оценки безопасности информационных технологий", 2002 г.

Профиль защиты - это нормативный документ, предназначенный для изложения проблемы безопасности определенной совокупности продуктов и систем ИТ и формулирования требований безопасности для решении данной

проблемы. Структура и общие требования к содержанию ПЗ приведены в Приложении Б.

ПЗ не регламентирует, каким образом данные требования будут выполнены, обеспечивая, таким образом, независимое от реализации описание требований безопасности.

Профиль защиты разрабатывается для определения типового набора требований безопасности, которым должны удовлетворять один или более продуктов или которым должны удовлетворять системы ИТ, предназначенные для использования в определенных целях. Профиль защиты может применяться к определенному типу продуктов ИТ (например, операционным системам, системам управления базами данных, смарт-картам, межсетевым экранам и т.д.) или к совокупности продуктов, образующих систему ИТ (например, к инфраструктуре открытых ключей, виртуальным частным сетям).

Профили защиты используются как стандартизованные наборы требований с целью повышения обоснованности задания требований к безопасности изделий ИТ, оценки безопасности и возможности проведения сравнительного анализа уровня безопасности различных изделий ИТ.

Профили защиты подлежат оценке, сертификации и регистрации в соответствии с требованиями настоящего Положения.

Проекты ПЗ, предназначенных для регламентации обязательных требований к безопасности изделий ИТ, дополнительно проходят экспертизу в порядке, устанавливаемом Гостехкомиссией России. При экспертизе ПЗ оценивается полнота учета в ПЗ требований нормативных документов по защите соответствующих видов информации ограниченного доступа.

Задание по безопасности - это документ, содержащий требования безопасности для конкретного изделия ИТ, которые реализованы в нем для достижения установленных целей безопасности. Структура и общие требования к содержанию ЗБ приведены в Приложении В.

Требования безопасности, включаемые в ЗБ, могут быть определены ссылками на профили защиты, на отдельные стандартизованные требования, а также могут содержать требования в явном виде. Помимо требований безопасности, в ЗБ включается краткая спецификация изделия ИТ и необходимые обоснования и пояснения.

Одной из целей разработки ЗБ является демонстрация того, как изделие ИТ удовлетворяет потребностям безопасности, сформулированным в ПЗ. Тем

не менее, соответствие задания по безопасности профилю защиты не является обязательным. В ЗБ могут быть определены функции безопасности, заявляемые разработчиком продукта ИТ вне зависимости от того, имеется ли на данный момент ПЗ на соответствующий тип изделий ИТ.

Если соответствующий профиль защиты с обязательными требованиями отсутствует, заказчики (разработчики) изделий информационных технологий могут направить запрос в Гостехкомиссию России на экспертизу заданий по безопасности с тем, чтобы определить, имеет ли изделие ИТ необходимые функциональные возможности и соответствует ли оценочный уровень доверия той области, в которой предполагается использовать изделие ИТ.

ЗБ является основой для проведения оценки безопасности изделия ИТ.

6. Разработка профилей защиты

Разработчиком ПЗ может быть любое юридическое или физическое лицо. ПЗ может разрабатываться по заказу заинтересованных организаций либо в инициативном порядке.

Профиль защиты должен содержать:
- описание потребностей пользователей изделия ИТ в обеспечении безопасности;
- описание среды безопасности изделия ИТ, уточняющее формулировку потребности в безопасности с учетом порождаемых средой угроз, политики безопасности и сделанных предположений;
- цели безопасности изделия ИТ, основанные на описании среды безопасности и предоставляющие информацию относительно того, как и в какой мере должны быть удовлетворены потребности в безопасности. Посредством целей безопасности должно быть показано, что должно быть сделано для решения проблемы безопасности, определенной для изделия ИТ.
- функциональные требования безопасности и требования доверия к безопасности, которые направлены на решение проблемы безопасности в соответствии с описанием среды безопасности и целями безопасности для изделия ИТ. Функциональные требования безопасности выражают то, что должно выполняться изделием ИТ и его средой для удовлетворения целей безопасности. Требования доверия к безопасности определяют степень уверенности в правильности реализации функций безопасности изделия ИТ. Функциональные требования безопасности и требования доверия к безопасности должны обеспечивать достижение целей безопасности;
- обоснование, показывающее, что функциональные требования и требования доверия к безопасности являются достаточными для удовлетворения сформулированных потребностей пользователей изделия ИТ в его безопасности.

Требования безопасности профилей защиты определяются классом защищенности изделия ИТ, зависящим от ценности (секретности/конфиденциальности, важности, стоимости) информационных ресурсов, а также угрозами безопасности, современным состоянием (уровенем развития) продуктов безопасности, стоимостью и временем создания и проведения оценки безопасности изделия ИТ. При назначении требований безопасности в зависимости от класса защищенности изделия ИТ следует руководствоваться РД Гостехкомиссии России "Руководство по разработке семейств профилей защиты".

Рекомендации по разработке ПЗ изложены в РД Гостехкомиссии России "Руководство по разработке профилей защиты и заданий по безопасности".

7. Оценка и сертификация ПЗ

Оценка ПЗ выполняется согласно критериям оценки ПЗ, содержащимся в части 3 РД Гостехкомиссии России "Критерии оценки безопасности информационных технологий".

Оценка ПЗ осуществляется испытательными лабораториями в порядке, установленном для подтверждения соответствия средств защиты информации требованиям безопасности.

Целью оценки ПЗ является доказательство его полноты, непротиворечивости, технической правильности и возможности использования при изложении требований к безопасности изделий ИТ.

По результатам оценки подготавливается технический отчет в соответствии с установленными требованиями. Технический отчет направляется испытательной лабораторией в орган сертификации, а копия технического отчета - Заявителю.

При соответствии результатов испытаний требованиям нормативных документов орган сертификации оформляет отчет о сертификации и выдает сертификат соответствия.

8. Регистрация и публикация ПЗ

После завершения разработки проекта профиля защиты подается заявка на его регистрацию в орган регистрации профилей защиты в соответствии с РД Гостехкомиссии России "Руководство по регистрации профилей защиты". При положительном результате проверки ПЗ включается в реестр профилей защиты. Орган регистрации обеспечивает ведение реестра профилей защиты и его публикацию.

О разработке зарегистрированного проекта профиля защиты должно быть опубликовано уведомление в информационной системе общего пользования в электронно-цифровой форме по адресу WWW.GOSTEXKOM.RU.

Уведомление о разработке проекта ПЗ выполняется по форме Приложения А к данному Положению и должно содержать информацию о том, в отношении каких типов изделий ИТ будут устанавливаться разрабатываемые требования, с кратким изложением цели этого ПЗ, обоснованием необходимости его разработки и указанием тех разрабатываемых требований, которые отличаются от требований существующих ПЗ, а также информацию о способе ознакомления с проектом ПЗ, наименование организации или фамилию, имя, отчество разработчика проекта данного ПЗ, почтовый адрес и, при наличии, адрес электронной почты, по которым должен осуществляться прием в письменной форме замечаний заинтересованных лиц.

9. Разработка заданий по безопасности

Разработка заданий по безопасности осуществляется разработчиками изделий ИТ.

Структура задания по безопасности в основном соответствует ПЗ, но содержит дополнительную информацию, ориентированную на конкретную реализацию изделия ИТ и разъясняющую, каким образом требования безопасности реализуются в конкретном продукте или системе. ЗБ содержит следующую дополнительную информацию, отсутствующую в ПЗ:
- краткую спецификацию изделия ИТ, которая представляет функции безопасности и меры доверия к безопасности для конкретного изделия ИТ;
- дополнительный раздел, который включается в ЗБ в тех случаях, когда утверждается о соответствии ЗБ одному или более ПЗ;
- дополнительные материалы в разделе "Обоснование", подтверждающие, что ЗБ является полной и взаимосвязанной совокупностью требований, и что изделие ИТ обеспечивает безопасность в определенной среде. Обоснование также демонстрирует, что все утверждения о соответствии ПЗ справедливы.

Если в ЗБ утверждается о соответствии ПЗ и при этом не специфицируются дополнительные функциональные требования и требования доверия к безопасности, то содержание упомянутых выше разделов ЗБ может быть идентично содержанию соответствующих разделов ПЗ. В таких случаях рекомендуется в ЗБ делать ссылку на содержание ПЗ.

10. Оценка ЗБ

Оценка ЗБ является первым этапом процесса оценки безопасности изделия ИТ. Оценка ЗБ выполняется согласно критериям оценки ЗБ, содержащимся в части 3 РД Гостехкомиссии России "Критерии оценки безопасности информационных технологий".

Оценка имеет две цели: во-первых, определить, является ли ЗБ полным, непротиворечивым, технически правильным и, следовательно, пригодным для использования в качестве основы для оценки соответствующего изделия ИТ; во-вторых, в случае, когда в ЗБ имеется утверждение о соответствии некоторому ПЗ, - установить, что требования ЗБ должным образом соответствуют требованиям этого ПЗ.

Приложение А (справочное). Форма уведомления о разработке ПЗ

Уведомление
о разработке профиля защиты "Название изделия ИТ"

1) Разработчик:

2) Объект оценки:

3) Наименование профиля защиты:

4) Цели и обоснование необходимости разработки профиля защиты:

5) Срок публичного обсуждения проекта профиля защиты:

6) Окончательная дата представления замечаний и предложений по проекту профиля защиты:

7) Прием замечаний по проекту профиля защиты осуществляется по адресу:

Приложение Б (справочное). Содержание профиля защиты

Содержание ПЗ соответствует Приложению Б части 1 РД Гостехкомиссии России "Критерии оценки безопасности информационных технологий" и приведено в таблице Б1.

Таблица Б1.
1. Введение ПЗ
1.1. Идентификация ПЗ
1.2. Аннотация ПЗ
2. Описание изделия ИТ

3. Среда безопасности изделия ИТ
3.1. Предположения безопасности
3.2. Угрозы
3.3. Политика безопасности организации
4. Цели безопасности
4.1. Цели безопасности для изделия ИТ
4.2. Цели безопасности для среды изделия ИТ
5. Требования безопасности изделия ИТ
5.1. Функциональные требования безопасности изделия ИТ
5.2. Требования доверия к безопасности изделия ИТ
5.3. Требования безопасности для среды изделия ИТ
6. Замечания по применению
7. Обоснование
7.1. Обоснование целей безопасности
7.2. Обоснование требований безопасности

В разделе "Введение ПЗ" идентифицируется ПЗ и дается его аннотация в форме, наиболее подходящей для включения в каталоги и реестры ПЗ.

В раздел "Описание изделия ИТ" включается сопроводительная информация об изделии ИТ (или типе изделия ИТ), предназначенная для пояснения его назначения и требований безопасности.

В раздел ПЗ "Среда безопасности изделия ИТ" включается описание аспектов среды безопасности изделия ИТ, которые должны учитываться для изделия ИТ, в частности - детальное описание предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), и политики безопасности организации, которой должно удовлетворять изделие ИТ.

В раздел ПЗ "Цели безопасности" включается краткое изложение предполагаемой реакции на аспекты среды безопасности, как с точки зрения целей безопасности, которые должны быть удовлетворены изделием ИТ, так и с точки зрения целей безопасности, которые должны быть удовлетворены ИТ- и не-ИТ-мерами безопасности в пределах среды изделия ИТ.

В раздел ПЗ "Требования безопасности изделия ИТ" включаются функциональные требования безопасности изделия ИТ, требования доверия к безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды изделия ИТ.

В раздел ПЗ "Замечания по применению ПЗ" может включаться любая дополнительная информация, которую разработчик ПЗ считает полезной. Замечания по применению могут быть распределены по соответствующим разделам ПЗ.

В разделе ПЗ "Обоснование" демонстрируется, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности изделия ИТ, и что соответствующее изделие ИТ учитывает идентифицированные аспекты среды безопасности. Раздел "Обоснование" может быть оформлен в виде отдельного документа.

В ПЗ могут быть включены дополнительные разделы, которые могут быть необходимы для предоставления полезной информации, например:
а) раздел "Введение ПЗ" может включать подраздел, описывающий организацию ПЗ, а также содержать ссылки на другие ПЗ и другие документы;
б) раздел "Среда безопасности изделия ИТ" может включать отдельные подразделы для различных доменов в ИТ-среде для изделия ИТ;
в) раздел "Требования безопасности изделия ИТ" может быть расширен за счет включения, где необходимо, требований безопасности для не-ИТ-среды безопасности изделия ИТ.

В случае если подраздел не используется (например, политика безопасности организации, требования безопасности ИТ для среды изделия ИТ), необходимо включить в ПЗ соответствующее пояснение.

Приложение В (справочное). Содержание задания по безопасности

Содержание ЗБ соответствует Приложению В части 1 РД Гостехкомиссии России "Критерии оценки безопасности информационных технологий" и приведено в таблице В1.

Таблица В1.
1. Введение ЗБ
1.1. Идентификация ЗБ
1.2. Аннотация ЗБ
2. Описание изделия ИТ
3. Среда безопасности изделия ИТ
3.1. Предположения безопасности
3.2. Угрозы
3.3. Политика безопасности организации
4. Цели безопасности
4.1. Цели безопасности для изделия ИТ

4.2. Цели безопасности для среды изделия ИТ
5. Требования безопасности для изделия ИТ
5.1. Функциональные требования безопасности изделия ИТ
5.2. Требования доверия к безопасности изделия ИТ
5.3. Требования безопасности для среды изделия ИТ
6. Краткая спецификация изделия ИТ
6.1. Функции безопасности изделия ИТ
6.2. Меры обеспечения доверия к безопасности
7. Утверждения о соответствии ПЗ
7.1. Ссылка на ПЗ
7.2. Уточнение ПЗ
7.3. Дополнение ПЗ
8. Обоснование
8.1. Обоснование целей безопасности
8.2. Обоснование требований безопасности
8.3. Обоснование краткой спецификации изделия ИТ
8.4. Обоснование утверждений о соответствии ПЗ

В разделе "Введение ЗБ" идентифицируется ЗБ и изделие ИТ (включая номер версии) и дается аннотация ЗБ в форме, наиболее подходящей для включения в список оцененных (сертифицированных) изделий ИТ.

В раздел ЗБ "Описание изделия ИТ" включается сопроводительная информация об изделии ИТ, предназначенная для пояснения его назначения и требований безопасности. Раздел ЗБ "Описание изделия ИТ" должен также включать описание конфигурации, в которой изделие ИТ подлежит оценке.

В раздел ЗБ "Среда безопасности изделия ИТ" включается описание аспектов среды безопасности изделия ИТ, которые должны учитываться изделием ИТ, в частности, предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), политики безопасности организации, которой должно удовлетворять изделие ИТ.

В раздел ЗБ "Цели безопасности" включается краткое изложение предполагаемой реакции на аспекты среды безопасности, как с точки зрения целей безопасности, которые должны быть удовлетворены изделием ИТ, так и с точки зрения целей безопасности, которые должны быть удовлетворены ИТ- и не-ИТ-мерами безопасности в пределах среды изделия ИТ.

В раздел ЗБ "Требования безопасности изделия ИТ" включаются функциональные требования безопасности изделия ИТ, требования доверия к

безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды изделия ИТ.

В раздел "Краткая спецификация изделия ИТ" включается описание функций безопасности ИТ, реализуемых изделием ИТ и соответствующих специфицированным функциональным требованиям безопасности, а также любых мер доверия к безопасности, соответствующих специфицированным требованиям доверия к безопасности.

В разделе "Утверждения о соответствии ПЗ" идентифицируются ПЗ, о соответствии которым заявляется в ЗБ, а также дополнения или уточнения целей или требований из этих ПЗ.

В разделе ЗБ "Обоснование" демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что соответствующее изделие ИТ учитывает определенные аспекты среды безопасности изделия ИТ, и что функции безопасности изделия ИТ и меры доверия к безопасности соответствуют требованиям безопасности изделия ИТ.

Как и в случае ПЗ (см. Приложение Б), при разработке ЗБ можно отступать от вышеуказанной структуры путем включения дополнительных и исключения необязательных разделов (и/или подразделов) ЗБ.