Руководящий документ
Безопасность информационных технологий.
Руководство по формированию семейств профилей защиты

Гостехкомиссия России, 2003 год

1. Область применения

Настоящий руководящий документ устанавливает порядок формирования семейств профилей защиты для изделий информационных технологий.

Документ предназначен для использования заказчиками и разработчиками изделий ИТ при разработке профилей защиты для типовых изделий ИТ в соответствии с Руководящим документом Гостехкомиссии России «Критерии оценки безопасности информационных технологий».

2. Нормативные ссылки

В настоящем руководящем документе использованы ссылки на следующие нормативные документы.

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.

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.

Руководящий документ – Безопасность информационных технологий – Положение по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003.

3. Термины и определения

3.1 **Базовая стойкость функции безопасности:** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.

3.2 **Безопасность ИТ:** Характеристика защищенности информации и изделий ИТ от воздействия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способности изделий ИТ выполнять предусмотренные функции без нанесения неприемлемого ущерба.

3.3 **Высокая стойкость функции безопасности:** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

3.4 **Изделие ИТ:** Обобщенный термин для продуктов и систем ИТ.

3.5 **Информационная технология:** Приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

3.6 **Объект оценки:** Подлежащие оценке продукт или система ИТ с руководствами администратора и пользователя.

3.7 **Пакет доверия:** Предназначенная для многократного использования совокупность компонентов доверия для удовлетворения совокупности определенных целей безопасности. Примером ПД является оценочный уровень доверия.

3.8 **Профиль защиты:** Независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

3.9 **Продукт ИТ:** Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ.

3.10 **Семейство профилей защиты:** Совокупность упорядоченных взаимосвязанных ПЗ, которые относятся к определенному типу изделий ИТ.

3.11 **Система ИТ:** Специфическое воплощение изделия ИТ с конкретным назначением и условиями эксплуатации.

3.12 **Средняя стойкость функции безопасности:** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

3.13 **Стойкость функции безопасности:** Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности.

3.14 **Функциональный пакет:** Предназначенная для многократного использования совокупность функциональных компонентов, объединенных для удовлетворения совокупности определенных целей безопасности.

3.15 **Функция безопасности:** Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности.

4. Сокращения

ИТ - информационные технологии

ОК - Общие критерии

ОО - объект оценки

ОУД- оценочный уровень доверия к безопасности

ПД - пакет доверия

ПЗ - профиль защиты

РД - руководящий документ

СФБ -стойкость функции безопасности

ТДБ - требования доверия к безопасности

ФП - функциональный пакет

ФТБ - функциональные требования безопасности

5. Общие положения

5.1 Семейство профилей защиты предназначено для группирования и классификации профилей защиты одного типа изделий ИТ (например, операционных систем, межсетевых экранов и т.п.).

Общая схема построения семейства профилей защиты представлена на рисунке 1.

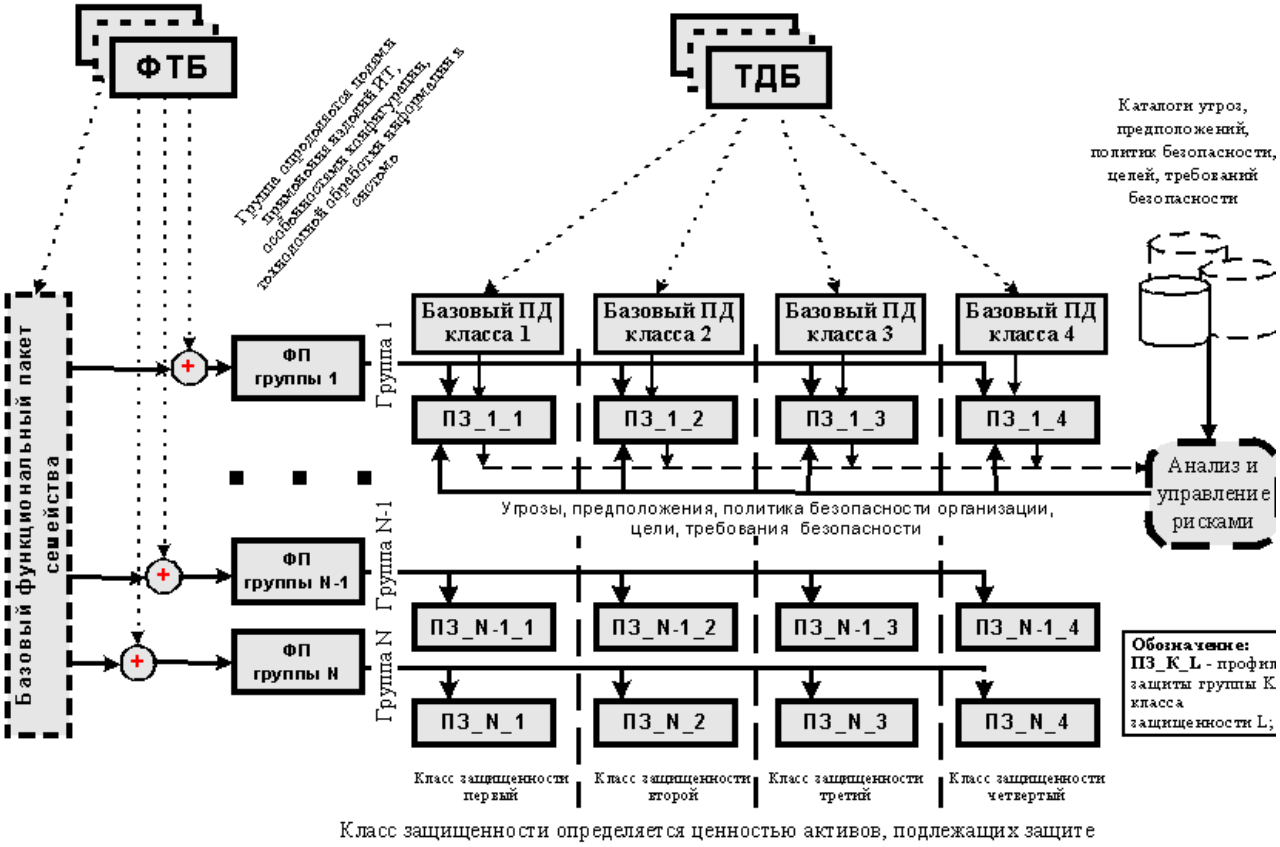

Рисунок 1 - Организация семейства профилей защиты

5.2 Тип изделий ИТ характеризуется общими функциональными требованиями безопасности. Функциональные требования безопасности, общие для всех изделий ИТ одного типа составляют базовый функциональный пакет семейства ПЗ.

Базовый функциональный пакет семейства разрабатывается в соответствии с Руководством по разработке профилей защиты и заданий по безопасности и регистрируется в соответствии с РД Гостехкомиссии России «Руководство по регистрации профилей защиты».

5.3 Исходя из специфики целей применения, особенностей конфигурации, технологии обработки информации и других признаков, изделия ИТ одного типа делятся на группы (см. рисунок 2).

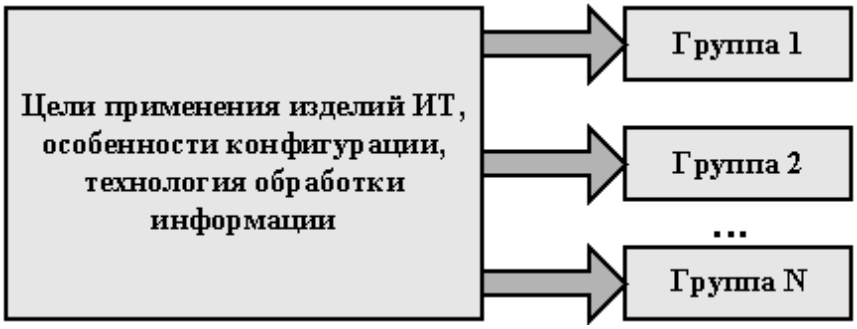

Рисунок 2 – Формирование групп изделий ИТ одного типа

Например, для изделий ИТ, отнесенных к типу «операционные системы», можно выделить следующие группы: «одноуровневые ОС», «многоуровневые ОС», «ОС реального времени» и др.

5.4 Функциональные требования безопасности, общие для всех изделий ИТ некоторой группы составляют функциональный пакет группы. В функциональный пакет группы включается базовый функциональный пакет семейства ПЗ и требования безопасности, специфичные для изделий ИТ данной группы (см. рисунок 3).

Рисунок 3 – Разработка функционального пакета группы

Функциональный пакет группы разрабатывается в соответствии с Руководством по разработке профилей защиты и заданий по безопасности и регистрируется в соответствии с РД Гостехкомиссии России «Руководство по регистрации профилей защиты».

5.5 Исходя из ценности (секретности/конфиденциальности, важности, стоимости) активов, изделия ИТ классифицируются по классам защищенности. Для каждого класса защищенности устанавливается базовый (минимальный) пакет доверия (см. рисунок 4) и специфицируется минимальный уровень стойкости (высокий, средний или базовый) для функций безопасности, реализуемых вероятностными или перестановочными механизмами (такими, например, как механизм паролей, хэширование).

Рисунок 4 – Формирование базовых пакетов доверия

Обязательные функциональные требования для каждого класса защищенности определяются спецификой изделия ИТ, составом учитываемых угроз, предположений безопасности и политик безопасности организации.

5.6 Соответствие классов защищенности изделий ИТ, базовых пакетов доверия и минимального уровня стойкости функций безопасности приведено в таблице 1.

Таблица 1

Соответствие классов защищенности изделий ИТ, базовых пакетов доверия и минимального уровня стойкости функций безопасности

Класс защищенности изделий ИТ	Базовый (минимальный) пакет доверия		Минимальный уровень стойкости функций безопасности
	Оценочный уровень доверия	Дополнительные требования доверия к безопасности ИТ(из РД «Критерии оценки безопасности информационных технологий»)	
1 (первый)	ОУД6	ALC_FLR.3 «Систематическое устранение недостатков» AVA_CCA.3 «Исчерпывающий анализ скрытых каналов»	Высокая СФБ
2 (второй)	ОУД5	ALC_FLR.3 «Систематическое	Высокая СФБ

		устранение недостатков» AVA_CCA.2 «Систематический анализ скрытых каналов» AVA_VLA.4 «Высоко стойкий»	
3 (третий)	ОУД4	ADV_IMP.2 «Реализация ФБО» ADV_INT.1 «Модульность» ALC_FLR.2 «Процедуры сообщений о недостатках» ATE_DPT.2 «Тестирование: проект нижнего уровня» AVA_CCA.1 «Анализ скрытых каналов» AVA_VLA.3 «Умеренно стойкий»	Средняя СФБ
4 (четвертый)	ОУД1		Базовая СФБ

6. Разработка профилей защиты семейства

6.1 Профиль защиты изделий ИТ определенной группы для конкретного класса защищенности разрабатывается в два этапа.

6.2 На первом этапе (см. рисунок 5) формируемый ПЗ наследует характеристики группы и класса, то есть в него включается функциональный пакет группы и базовый пакет доверия соответствующего класса защищенности. Кроме того, для функций безопасности, реализуемых вероятностными или перестановочными механизмами, специфицируется уровень СФБ не ниже минимального уровня СФБ, определенного для данного класса защищенности.

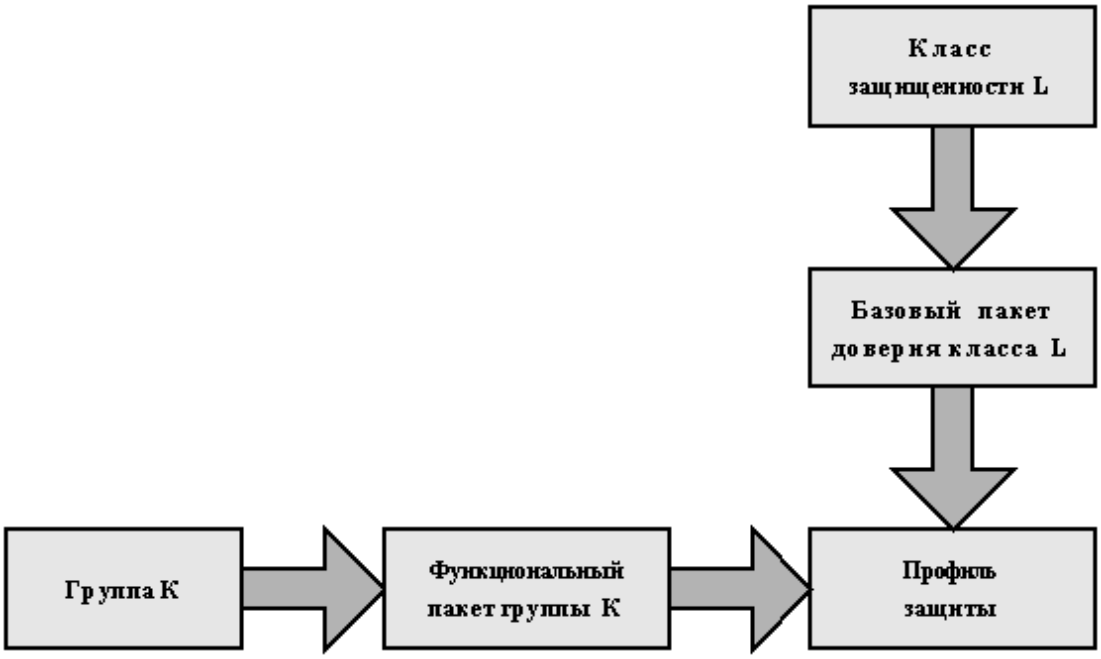

Рисунок 5 – Разработка профиля защиты (1 этап)

6.3 На втором этапе (см. рисунок 6) в ПЗ, исходя из результатов анализа рисков, угроз, политики безопасности организации и предположений о среде функционирования изделия ИТ, включаются все необходимые дополнительные функциональные требования и требования доверия (взятые из ОК либо сформулированные в явном виде).

Рисунок 6 – Разработка профиля защиты (2 этап)

7. Включение профилей защиты в семейство. модификация семейств

7.1 В семейство профилей защиты включаются ПЗ, разработанные в соответствии с требованиями РД Гостехкомиссии России «Положение по разработке профилей защиты и заданий по безопасности» и раздела 6 настоящего РД и прошедшие регистрацию в соответствии с РД Гостехкомиссии России «Руководство по регистрации профилей защиты».

7.2 Модификация семейства профилей защиты изделий ИТ производится в целях поддержания адекватности заложенных в ПЗ требований безопасности уровню развития ИТ, а также их адаптации к изменяющимся условиям эксплуатации изделий ИТ.

7.3 Модификация семейства профилей защиты изделий ИТ может осуществляться следующими основными способами:
- внесением изменений в соответствующие профили защиты, включенные ранее в состав семейства;
- заменой соответствующих профилей защиты, включенных ранее в состав семейства, на новые ПЗ;
- добавлением в семейство новых профилей защиты;
- добавлением новой группы изделий ИТ в структуру семейства.

Приложение А (обязательное)

Для защиты информации, ценность которой выражается в метрике «секретность/конфиденциальность», устанавливаются следующие классы защищенности изделий ИТ.

Первый класс применяется при защите информации с грифом «ОСОБОЙ ВАЖНОСТИ».

Второй класс защищенности изделий ИТ достаточен при защите информации с грифом «СОВЕРШЕННО СЕКРЕТНО».

Третий класс защищенности изделий ИТ достаточен при защите информации с грифом «СЕКРЕТНО».

Четвертый класс защищенности изделий ИТ достаточен при защите конфиденциальной информации.