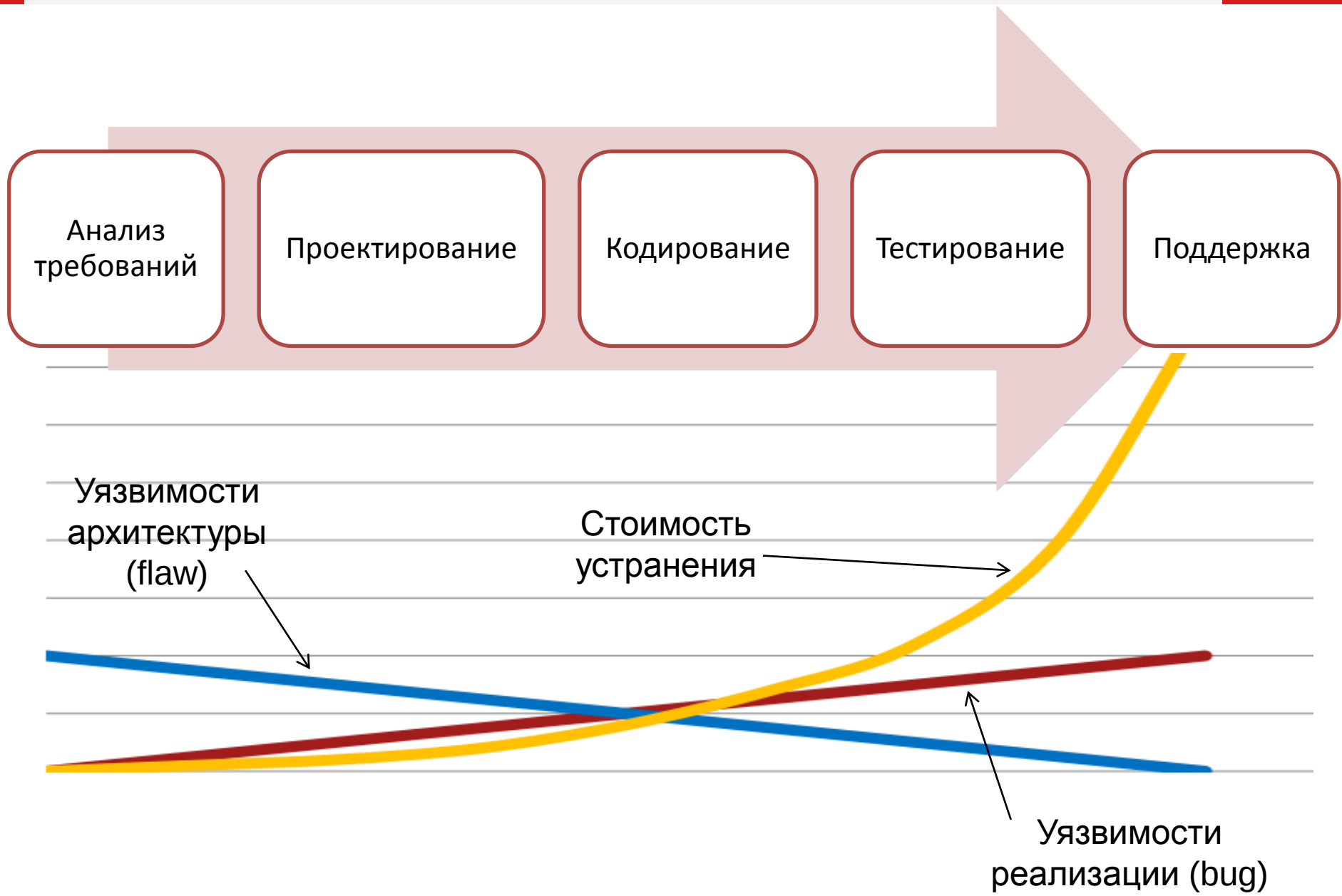
Эшелон
комплексная безопасность

infosecurity
RUSSIA

Обзор требований по разработке безопасного программного обеспечения ГОСТ Р 56939

Александр Барабанов,
кандидат технических наук, CISSP, CSSLP

Безопасность в жизненном цикле ПО



ГОСТ Р 56939-2016: предпосылки создания стандарта

Оценка программного обеспечения

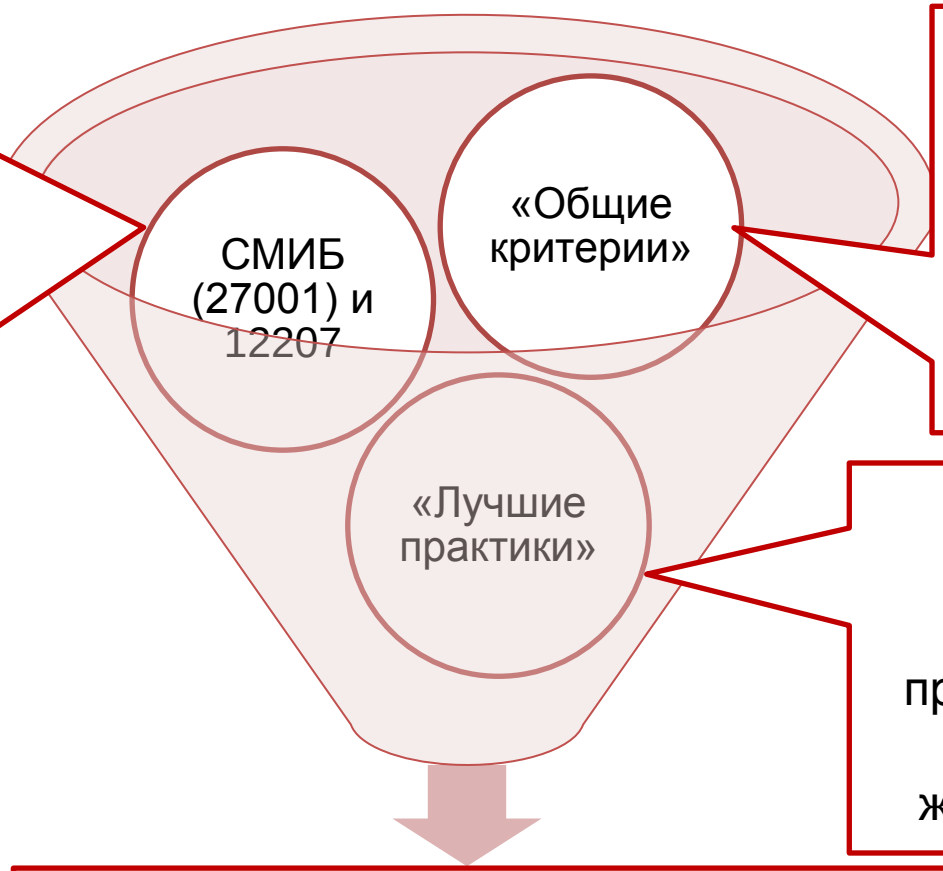
1. Создание и поддержка базы данных уязвимостей ПО
2. Проведение анализа уязвимостей в рамках сертификации (ISO/IEC TR 20004)
3. НПА нового поколения (AVA_VAN)
4. Создание ГОСТ Р по уязвимостям ИС
5. Рекомендации по обновлению сертифицированных средств защиты информации (проект)

Оценка процесса разработки

Специальные требования к процессу разработки программного обеспечения **не были определены**

Разработанный национальный стандарт: учитываемые особенности

Возможность интеграции с СМИБ, согласованность с процессами жизненного цикла по ГОСТ Р ИСО/МЭК 12207



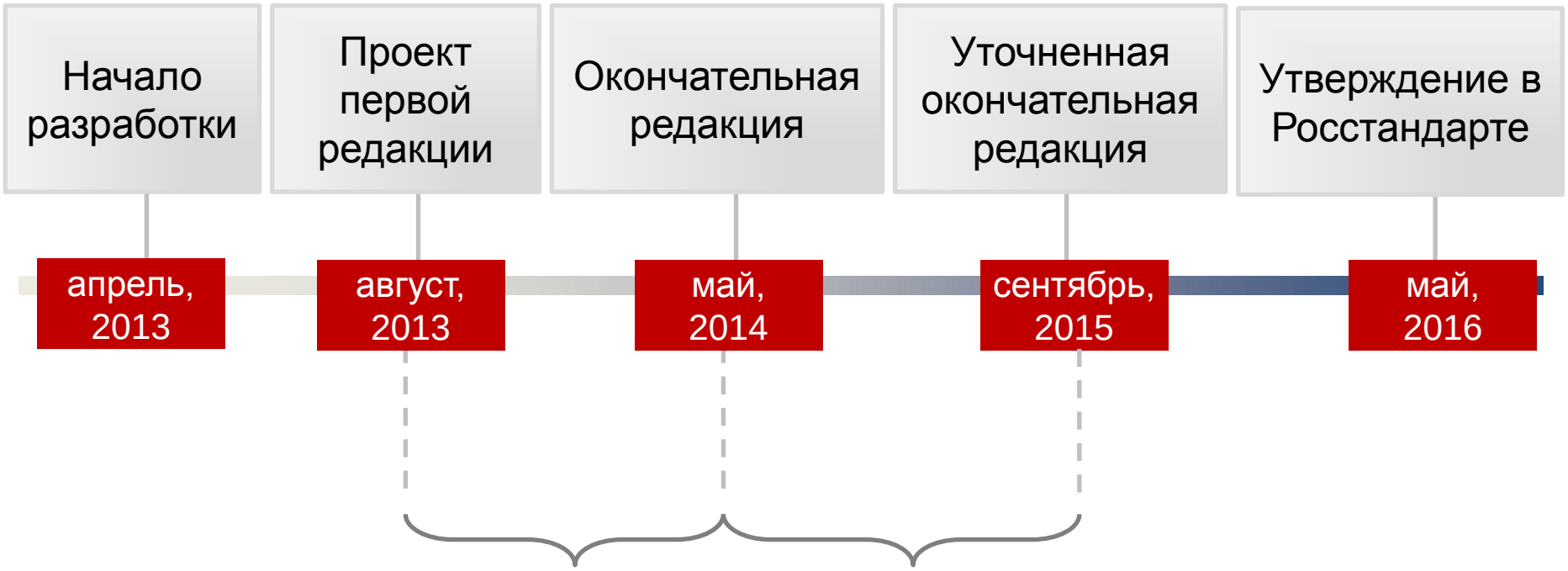
Совместимость с ГОСТ Р ИСО/МЭК 15408, возможность проведения оценки соответствия

Обеспечение внедрения необходимых процедур на самых ранних стадиях жизненного цикла

Разработанный ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

Эшелон
комплексная безопасность

Разработанный национальный стандарт: этапы выполнения проекта



Публичные обсуждения в рамках ТК 362 «Защита информации»:

- 22 организации
- ~ 200 замечаний и предложений

Эшелон
комплексная безопасность

Разработанный национальный стандарт: целевая аудитория

Целевая аудитория национального стандарта

Разработчики и производители программного обеспечения:

- основная аудитория
- представлены требования к реализации мер и свидетельствам
- документ может использоваться для декларации соответствия

Оценщики

- не является основной аудиторией (планируется отдельный ГОСТ)
- Органы по сертификации (системы добровольной сертификации), аккредитованные испытательные лаборатории
- требования к действиям оценщиков не предъявляются
- представлены требования к свидетельствам

Меры по разработке безопасного программного обеспечения

Меры по разработке безопасного программного обеспечения

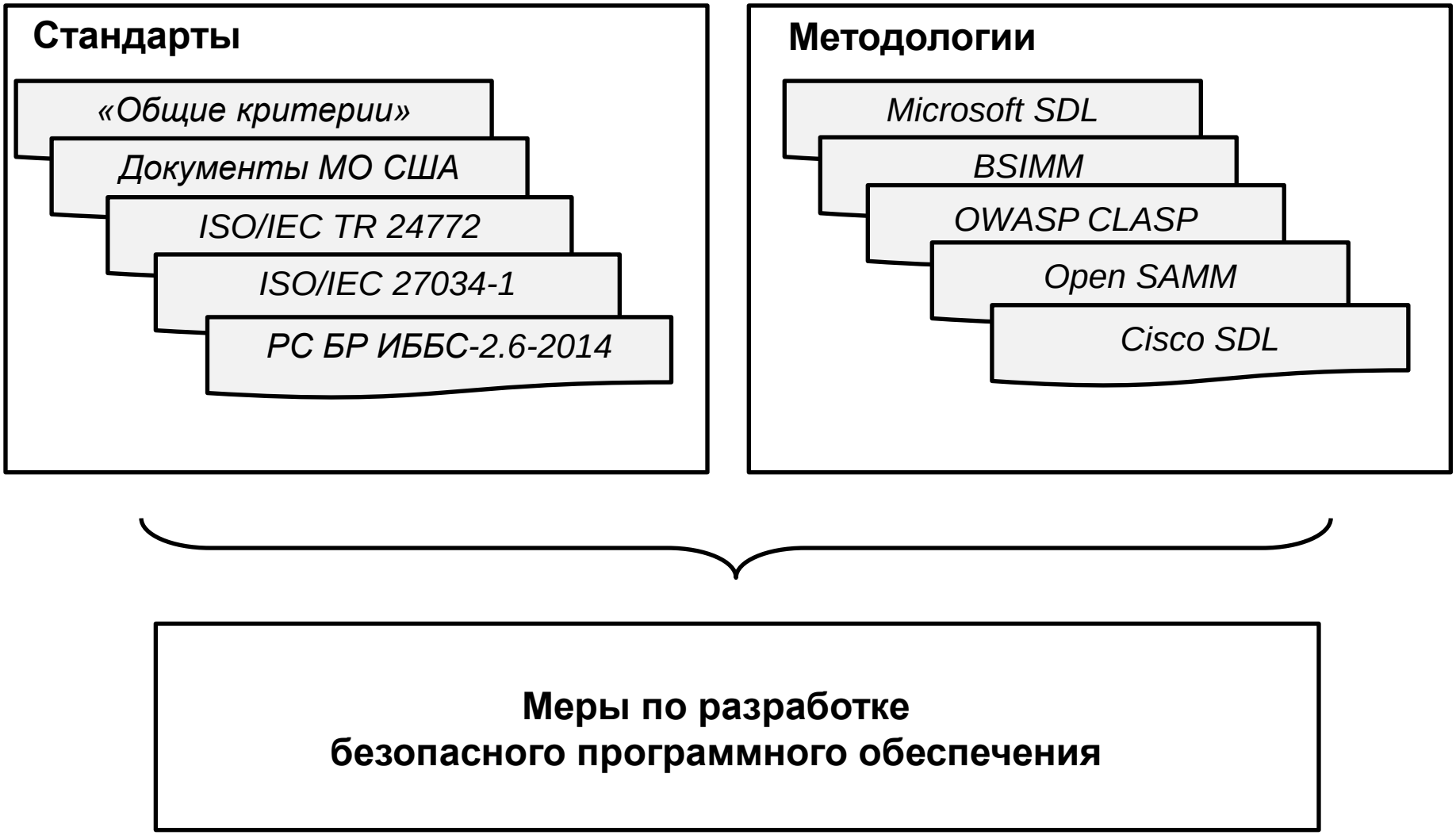
Общие меры:

- содержатся в 4 разделе (аналог основной части ISO/IEC 27001)

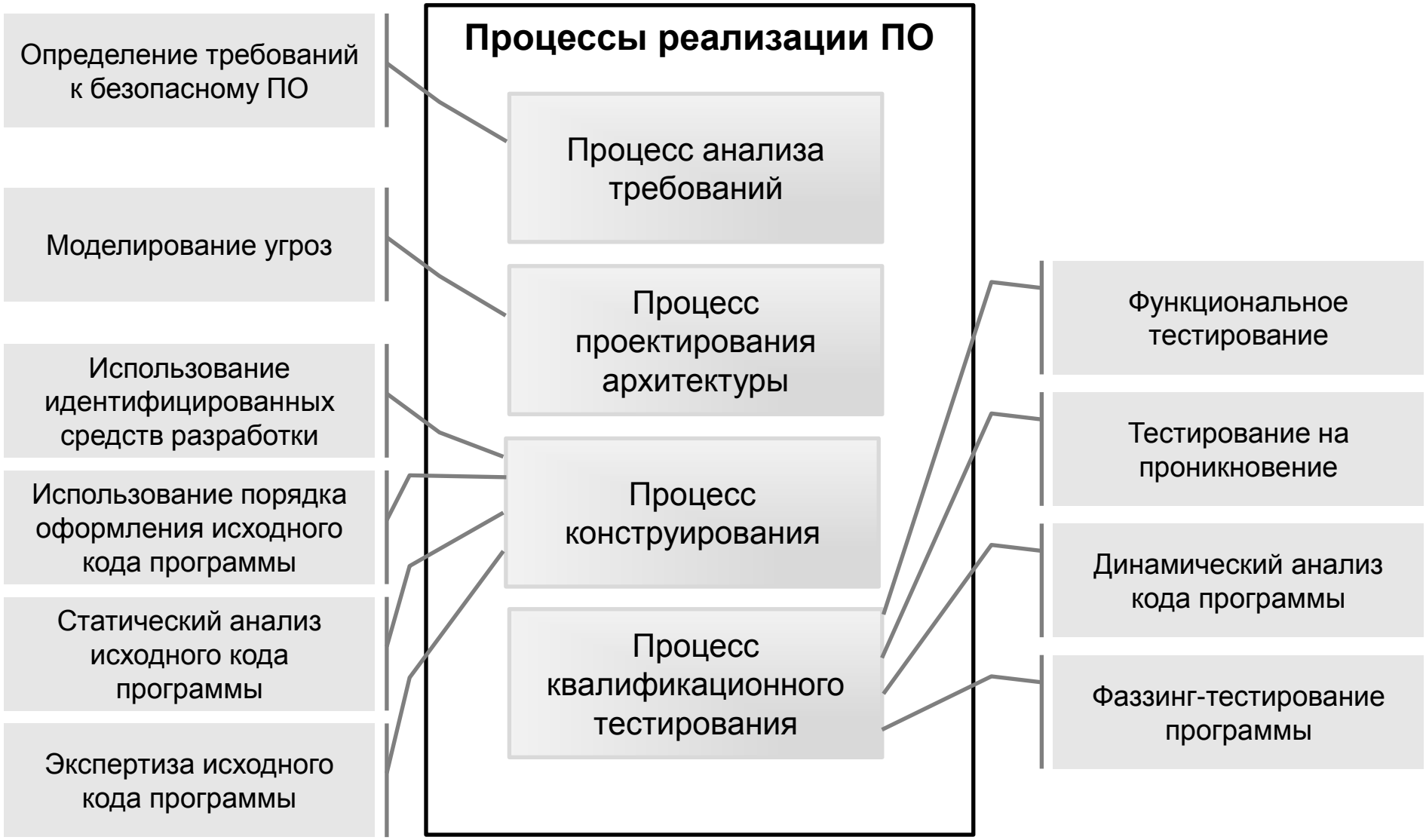
Технические меры

- содержатся в 5 разделе (аналог приложения А к ISO/IEC 27001)
- для соответствия ГОСТ **должны быть реализованы все меры из раздела 5**
- предусмотрена возможность использования компенсирующих мер

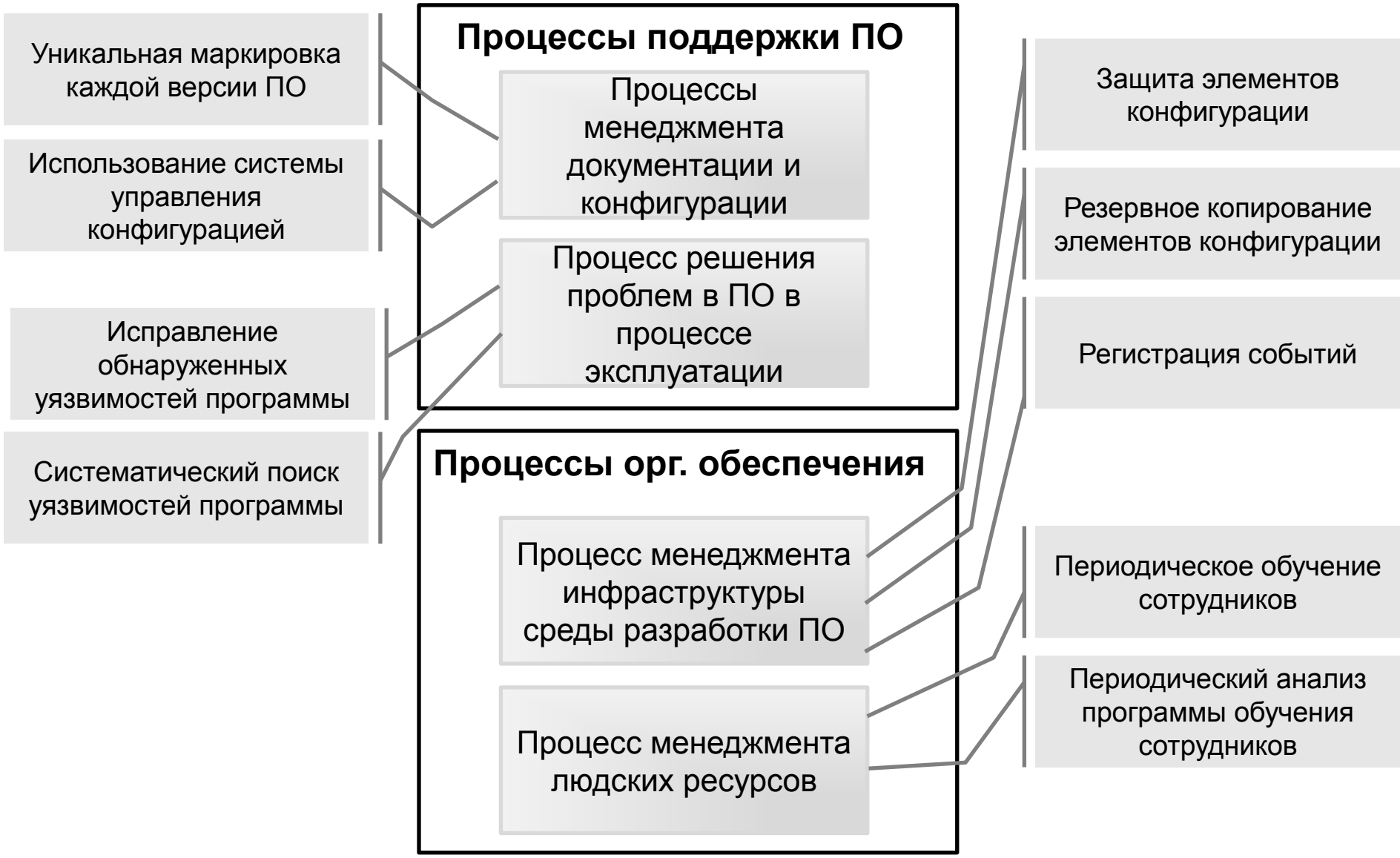
Технические меры по разработке безопасного программного обеспечения (1)



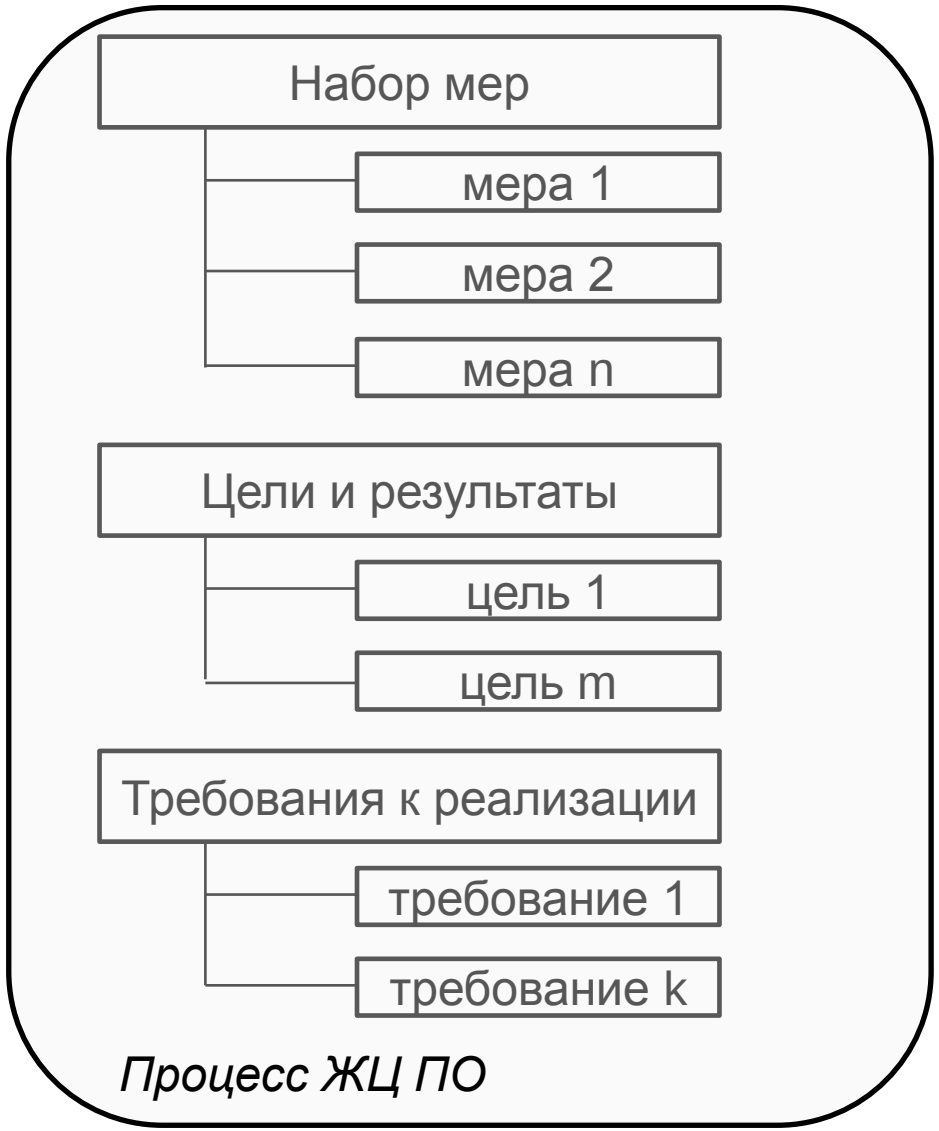
Технические меры по разработке безопасного программного обеспечения (2)



Технические меры по разработке безопасного программного обеспечения (3)



Технические меры по разработке безопасного программного обеспечения (4)



ГОСТ Р XXXXX-20XX
(проект, окончательная редакция)

5.6 Меры по разработке безопасного программного обеспечения, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации

5.6.1 Меры по разработке безопасного программного обеспечения, подлежащие реализации

При выполнении решения проблем в ПО разработчик ПО должен реализовать следующие меры:

- реализация и использование процедуры отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы;
- систематический поиск уязвимостей программы.

5.6.2 Цели и результаты реализации мер по разработке безопасного программного обеспечения

Реализация мер способствует достижению цели устранения ошибок ПО и уязвимостей программы, выявляемых в процессе эксплуатации ПО.

В результате успешной реализации мер ошибки ПО и уязвимости программы, обнаруженные в процессе эксплуатации ПО, регистрируются, анализируются и устраняются.

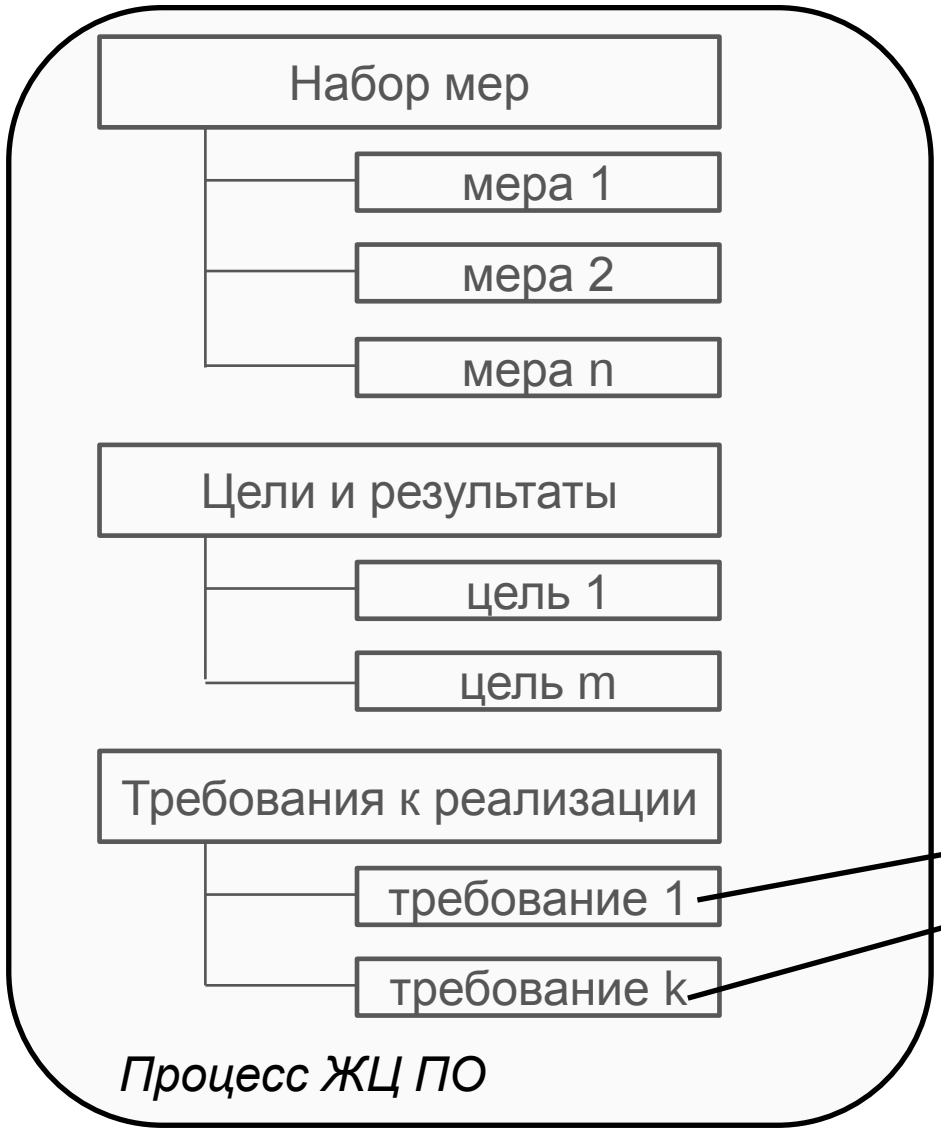
5.6.3 Требования к реализации мер по разработке безопасного программного обеспечения

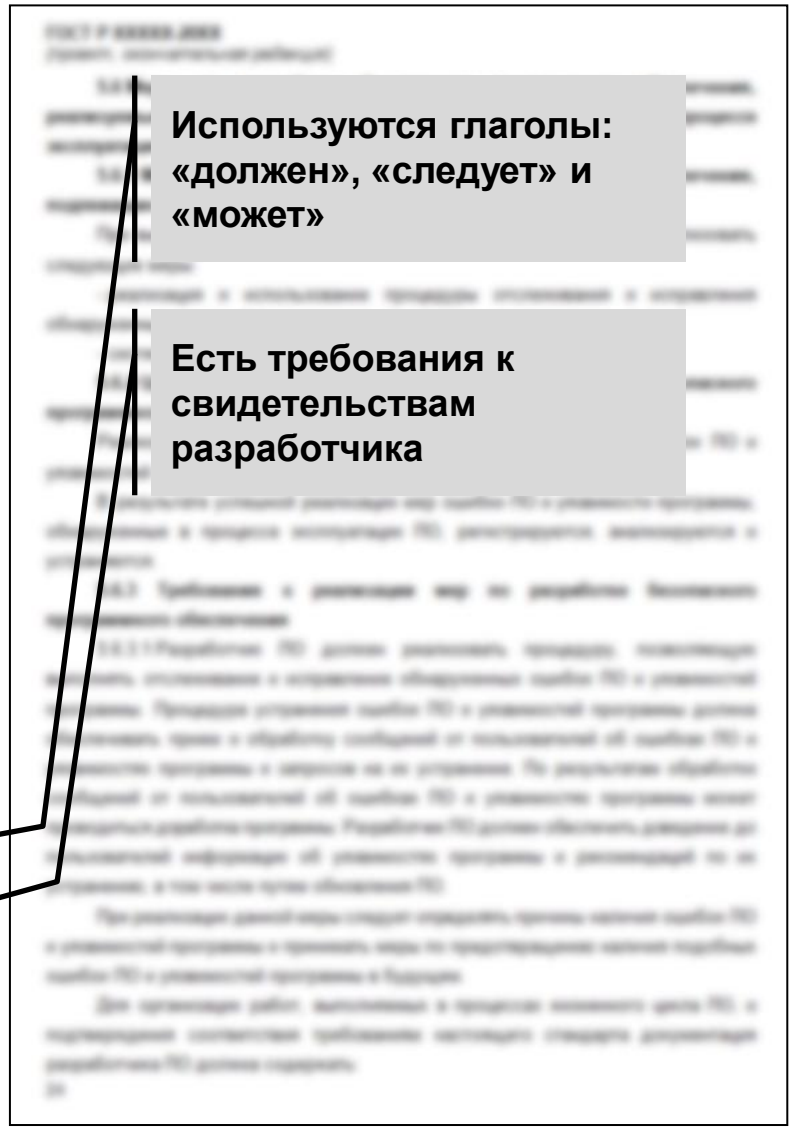
5.6.3.1 Разработчик ПО должен реализовать процедуру, позволяющую выполнять отслеживание и исправление обнаруженных ошибок ПО и уязвимостей программы. Процедура устранения ошибок ПО и уязвимостей программы должна обеспечивать прием и обработку сообщений от пользователей об ошибках ПО и уязвимостях программы и запросов на их устранение. По результатам обработки сообщений от пользователей об ошибках ПО и уязвимостях программы может проводиться доработка программы. Разработчик ПО должен обеспечить доведение до пользователей информации об уязвимостях программы и рекомендаций по их устранению, в том числе путем обновления ПО.

При реализации данной меры следует определять причины наличия ошибок ПО и уязвимостей программы и принимать меры по предотвращению наличия подобных ошибок ПО и уязвимостей программы в будущем.

Для организации работ, выполняемых в процессах жизненного цикла ПО, и подтверждения соответствия требованиям настоящего стандарта документация разработчика ПО должна содержать:

Технические меры по разработке безопасного программного обеспечения (4)





Перспективы развития

1. Использование ГОСТ при сертификации (в рамках проверки производства).
2. Планируется разработка документов, развивающих положения созданного документа:
   - перечень типовых угроз БИ
   - рекомендации по реализации мер
   - рекомендации по проведению оценки соответствия

Контактная информация

107023, Москва, ул. Электрозаводская, 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.npo-echelon.ru

ab@cnpo.ru