Практика внедрения процедур разработки безопасного программного обеспечения

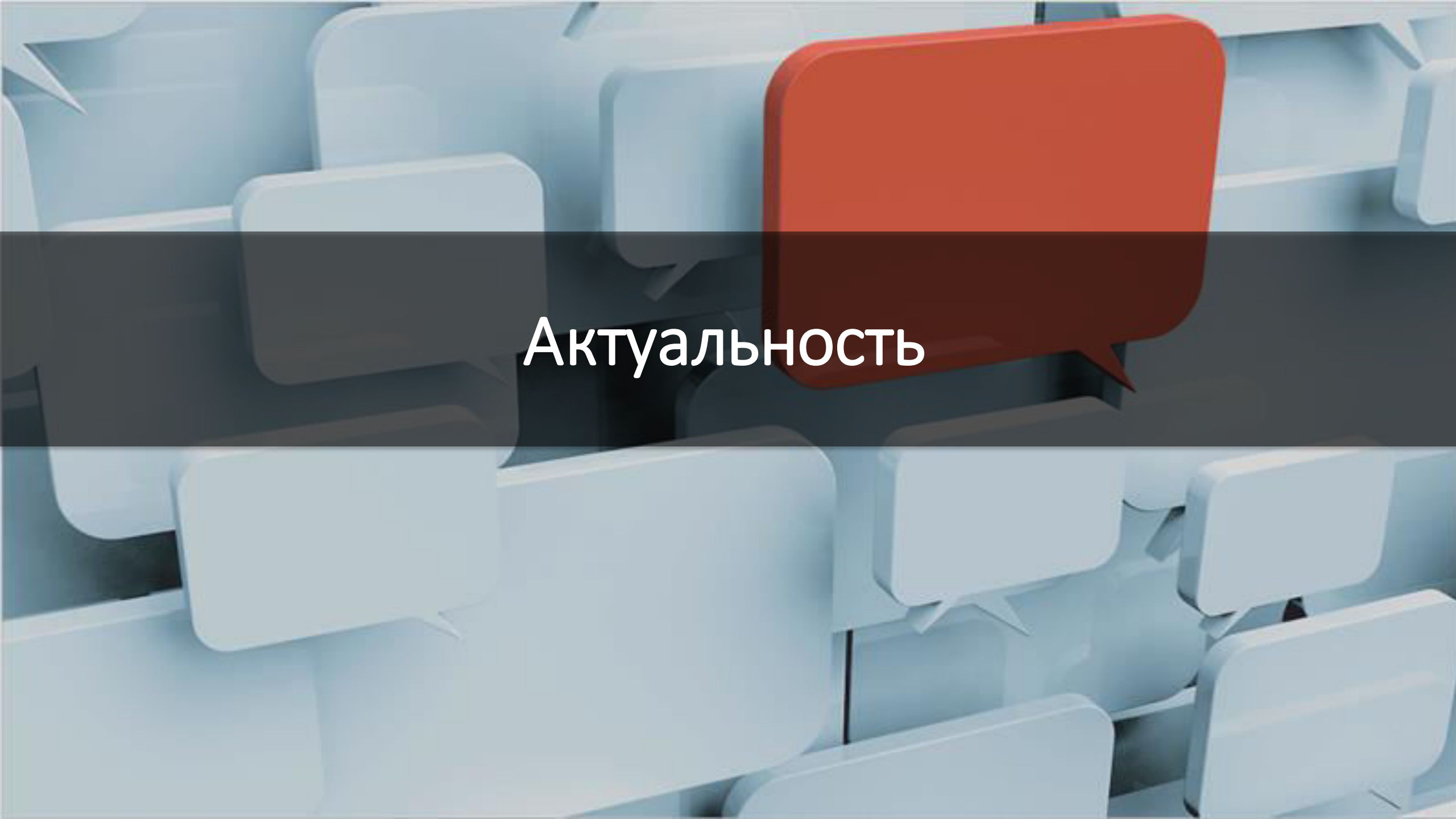
Максим Гришин, Алексей Марков

НПО «Эшелон»

IX Конференция "Актуальные вопросы защиты информации ", 13 февраля 2019 г., Москва, ТБ-Форум

План доклада

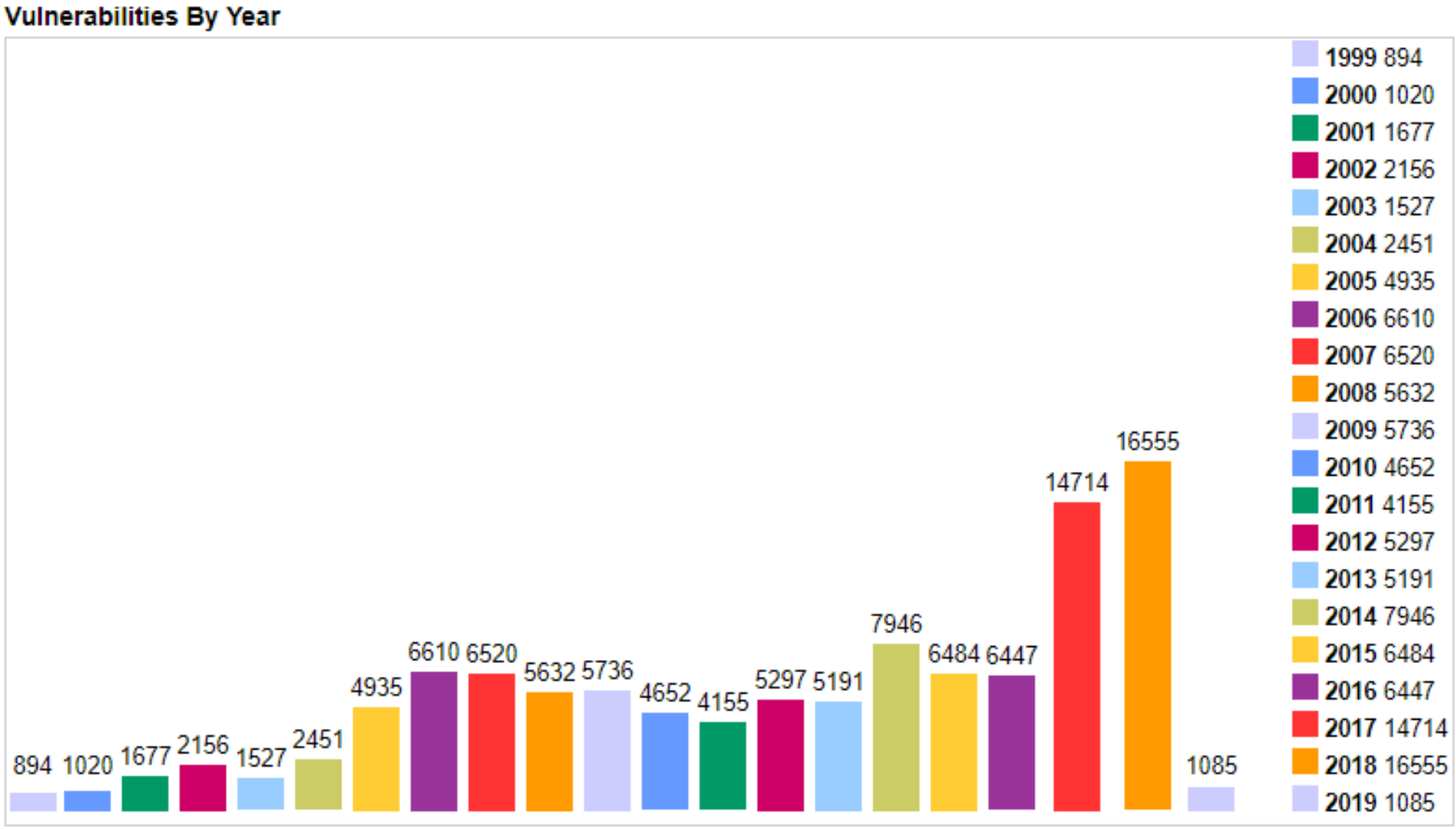
1. Актуальность
2. Линейка стандартов по разработке безопасного ПО
3. Проект стандарта «Руководство по разработке безопасного ПО..»
4. Требования и рекомендации
5. Типовые вопросы при внедрении
6. Примеры


Актуальность

Актуальность линейки стандартов по разработке БПО

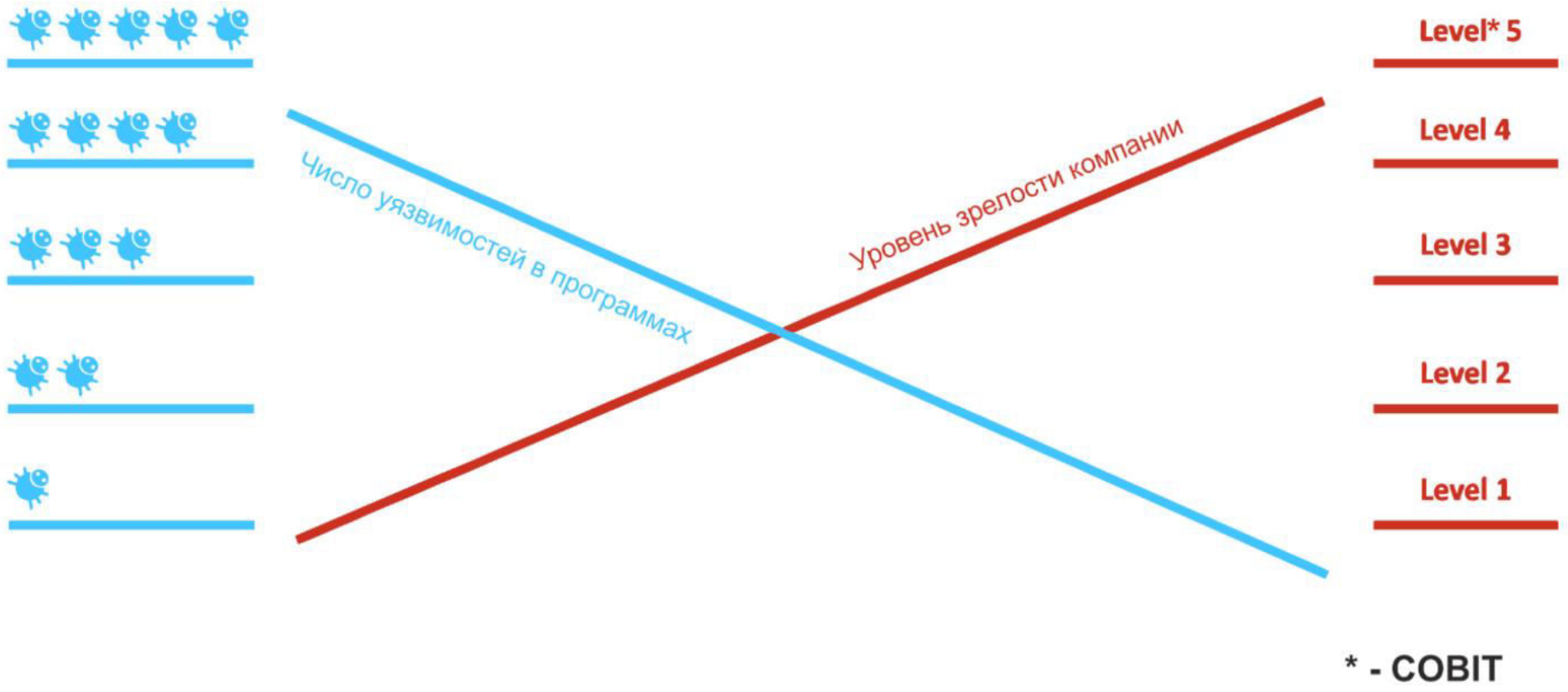
- Высокий уровень ошибок в ПО, которое разработано предприятиями «низкого уровня зрелости»
- Международные стандарты и «лучшие практики» не охватывают все процессы разработки ПО с учетом всевозможных требований по безопасности информации

Число уязвимостей не уменьшается



Данные CVEDetails

Зависимость уязвимостей в ПО от зрелости компании



Международная и зарубежная база не покрывает все возможные ситуации (меры, угрозы)

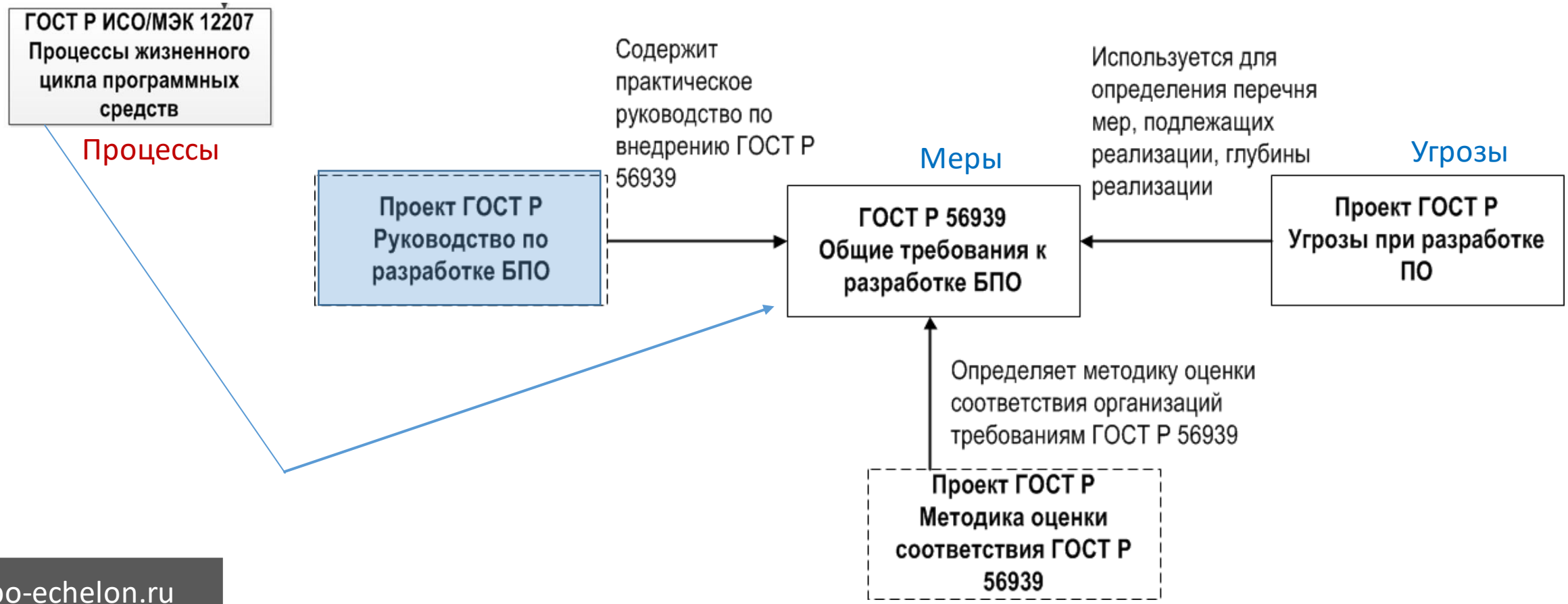
Мера и механизм	Стандарт						
	ISO 15408	Microsoft SDL	Cisco SDL	Open SAMM	OWASP CLASP	ISO TR 24772	ISO 27034-1
Обучение сотрудников организации-разработчика разработке безопасного ПО	-	+	+	+	-	-	-
Обеспечение безопасности инфраструктуры разработки ПО	+	-	-	-	-	-	-
Управление конфигурацией разрабатываемого ПО	+	-	-	-	-	-	-
Моделирование угроз безопасности информации, источником которых является ПО	+	+	+	+	+	-	-
Определение требования по разработке безопасного ПО	+	+	+	+	+	-	-
Использование стандарта на оформление исходного кода программы (правил и рекомендаций, направленных на минимизацию количества потенциально уязвимых конструкций в исходном коде программы)	-	+	+	+	+	+	-
Проведение статического анализа исходного кода программы	-	+	+	+	+	-	-
Проведение динамического анализа динамического кода программы	-	+	+	+	+	-	-
Проведение экспертизы исходного кода программ в ручном режиме	-	+	+	+	+	-	-
Проведение анализа уязвимостей	-	+	+	+	+	-	-
Обеспечение безопасности поставки ПО пользователю	+	+	+	+	-	-	-
Устранение уязвимостей ПО, выявляемых в процессе функционирования ПО	+	+	+	+	+	-	-
Возможность использования документа при оценке соответствия ПО требованиям, предъявляемым к разработке безопасного ПО	+	-	-	-	-	-	-
Наличие методики выбора подмножества мер разработки безопасного ПО	+	+	+	+	-	-	+
Согласованность с процессами жизненного цикла ПО, определенными ISO 12207	-	-	-	-	-	-	+

Каталог угроз	Учет угроз безопасности информации, специфичных для среды разработки	Учет непреднамеренных угроз безопасности информации
Supply Chain Attack Patterns: Framework and Catalog, Melinda Reed, John F. Miller, and Paul Popick	+	-
NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments	-	-
NIST IR 8144 Assessing Threats to Mobile Devices & Infrastructure	+	-
Common Attack Pattern Enumeration and Classification	+	-
Банк данных угроз безопасности информации» ФСТЭК России	-	+

Линейка стандартов по разработке безопасного ПО

Идея линейки стандартов

- Процессы – Меры - Угрозы
- ГОСТ 12207 – линейка ГОСТ 56939



Утвержденные, направленные на утверждение национальные стандарты

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

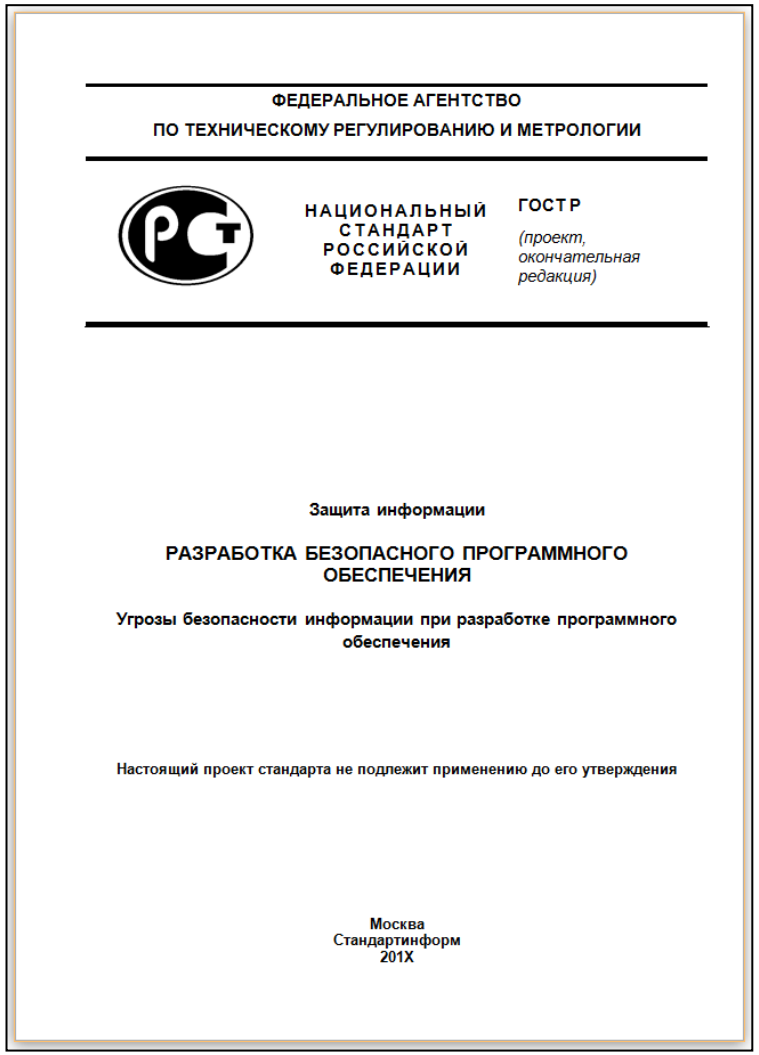
Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2016



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, окончательная редакция)

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Угрозы безопасности информации при разработке программного обеспечения

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

Взаимосвязь с другими национальными стандартами

Разработка безопасного ПО в нормативных документах

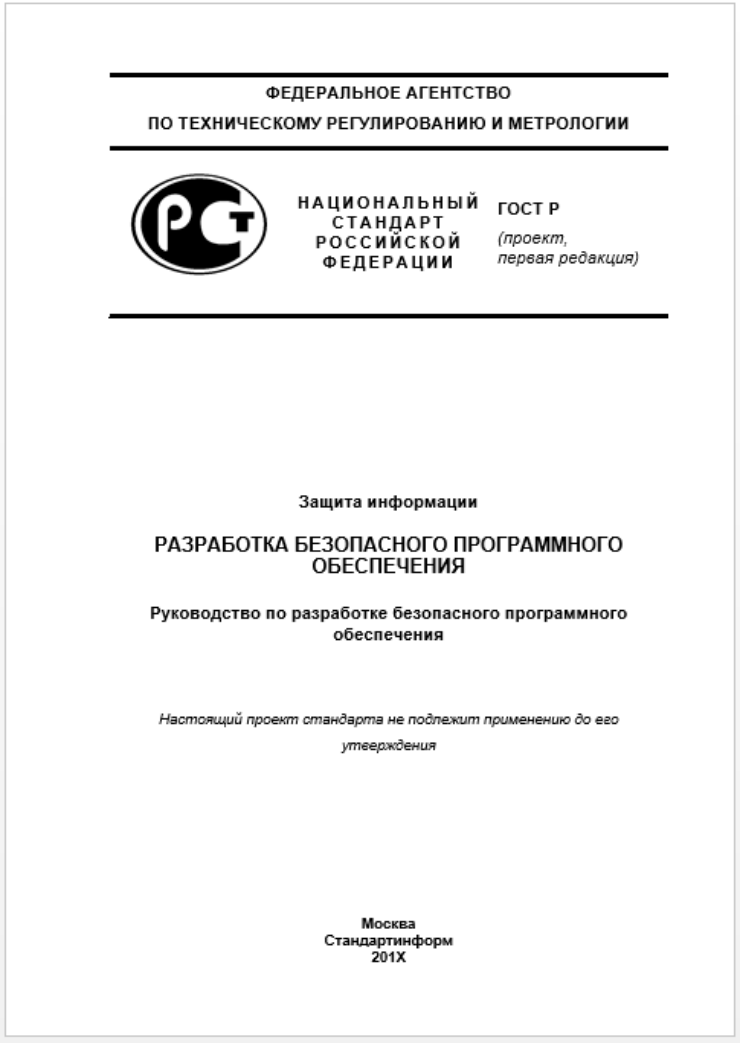
- Компенсационная мера (Приказы ФСТЭК России)
- Мера требований доверия (НПА ФСТЭК России)
- Мера (проекты документов ФСТЭК России)
- Нормативные документы при проверке производства и лицензировании

Проект стандарта «Руководство по разработке безопасного ПО..»

Цель

- Настоящий стандарт входит в комплекс стандартов, направленных на достижение целей, связанных с предотвращением появления и/или устранением уязвимостей программ, и содержит рекомендации по реализации мер по разработке безопасного программного обеспечения, установленных ГОСТ Р 56939.
- Ориентирован на разработчиков и производителей ПО, может быть использован ОС&ИЛ

Проект стандарта ГОСТ Р «… руководство по разработке безопасного программного обеспечения»



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, первая редакция)

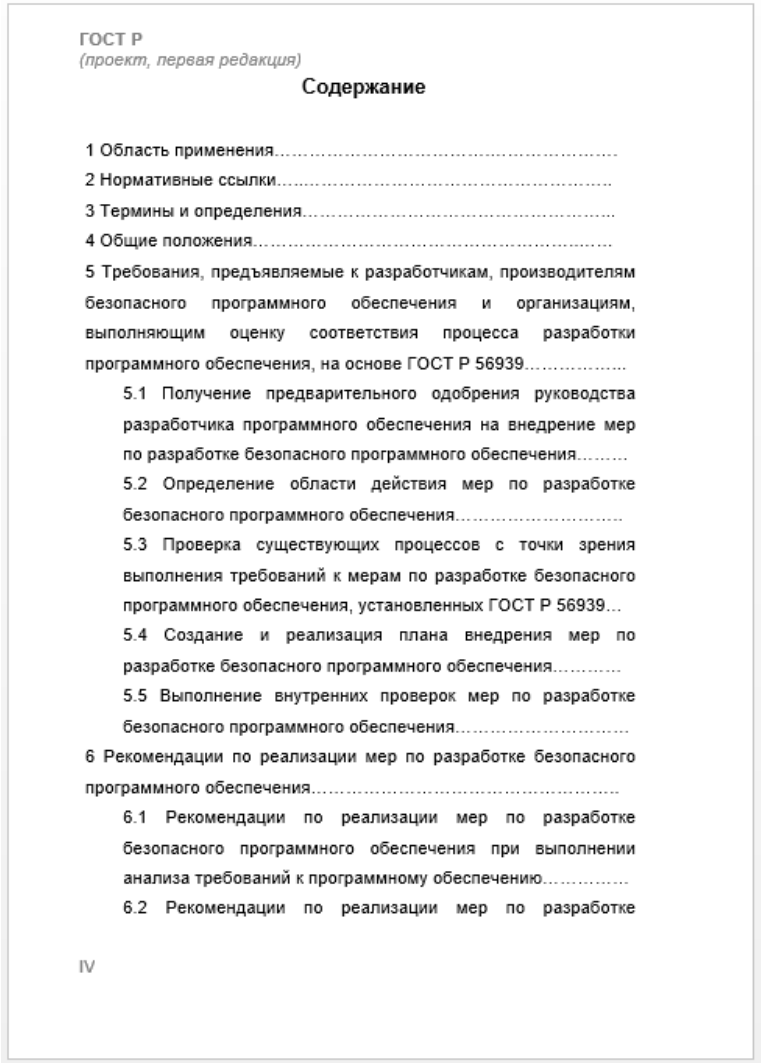
Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Руководство по разработке безопасного программного обеспечения

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X



ГОСТ Р
(проект, первая редакция)

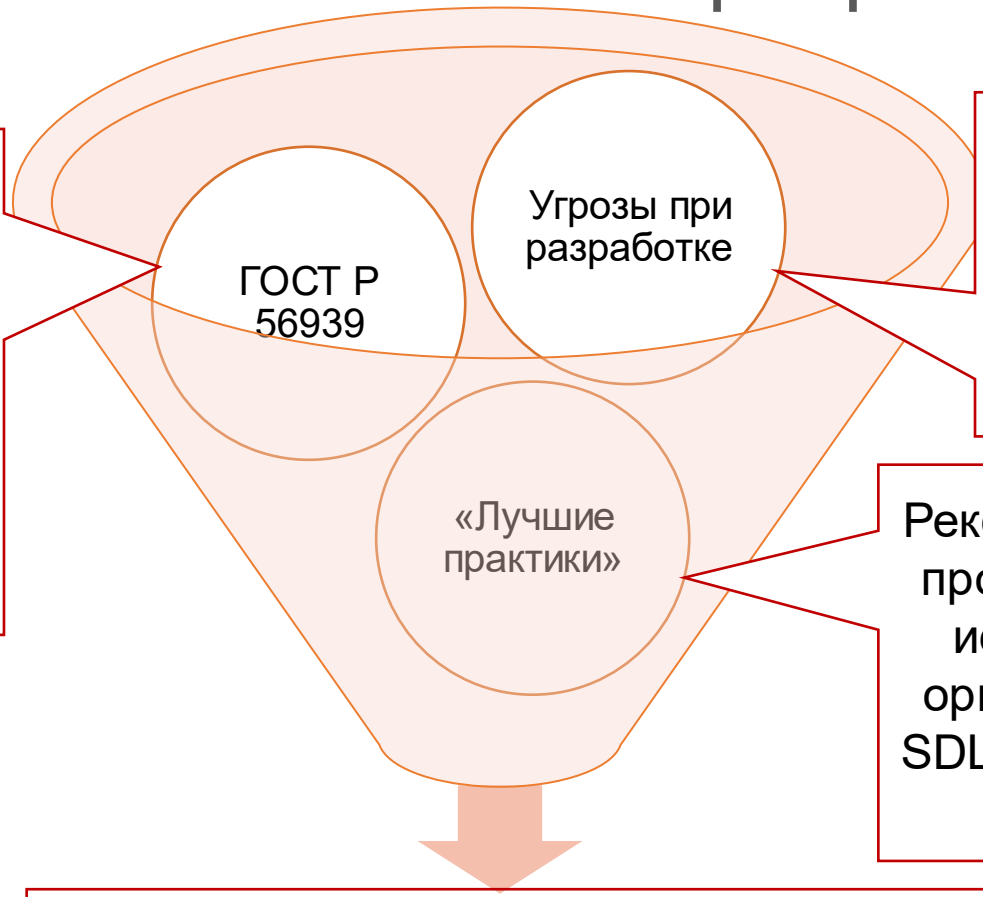
Содержание

1 Область применения……
2 Нормативные ссылки……
3 Термины и определения……
4 Общие положения……
5 Требования, предъявляемые к разработчикам, производителям безопасного программного обеспечения и организациям, выполняющим оценку соответствия процесса разработки программного обеспечения, на основе ГОСТ Р 56939……
5.1 Получение предварительного одобрения руководства разработчика программного обеспечения на внедрение мер по разработке безопасного программного обеспечения……
5.2 Определение области действия мер по разработке безопасного программного обеспечения……
5.3 Проверка существующих процессов с точки зрения выполнения требований к мерам по разработке безопасного программного обеспечения, установленных ГОСТ Р 56939…
5.4 Создание и реализация плана внедрения мер по разработке безопасного программного обеспечения……
5.5 Выполнение внутренних проверок мер по разработке безопасного программного обеспечения……
6 Рекомендации по реализации мер по разработке безопасного программного обеспечения……
6.1 Рекомендации по реализации мер по разработке безопасного программного обеспечения при выполнении анализа требований к программному обеспечению……
6.2 Рекомендации по реализации мер по разработке

IV

Проект стандарта: особенности разработки

Перечень и описание мер по разработке безопасного ПО, подлежащих реализации в среде разработки ПО

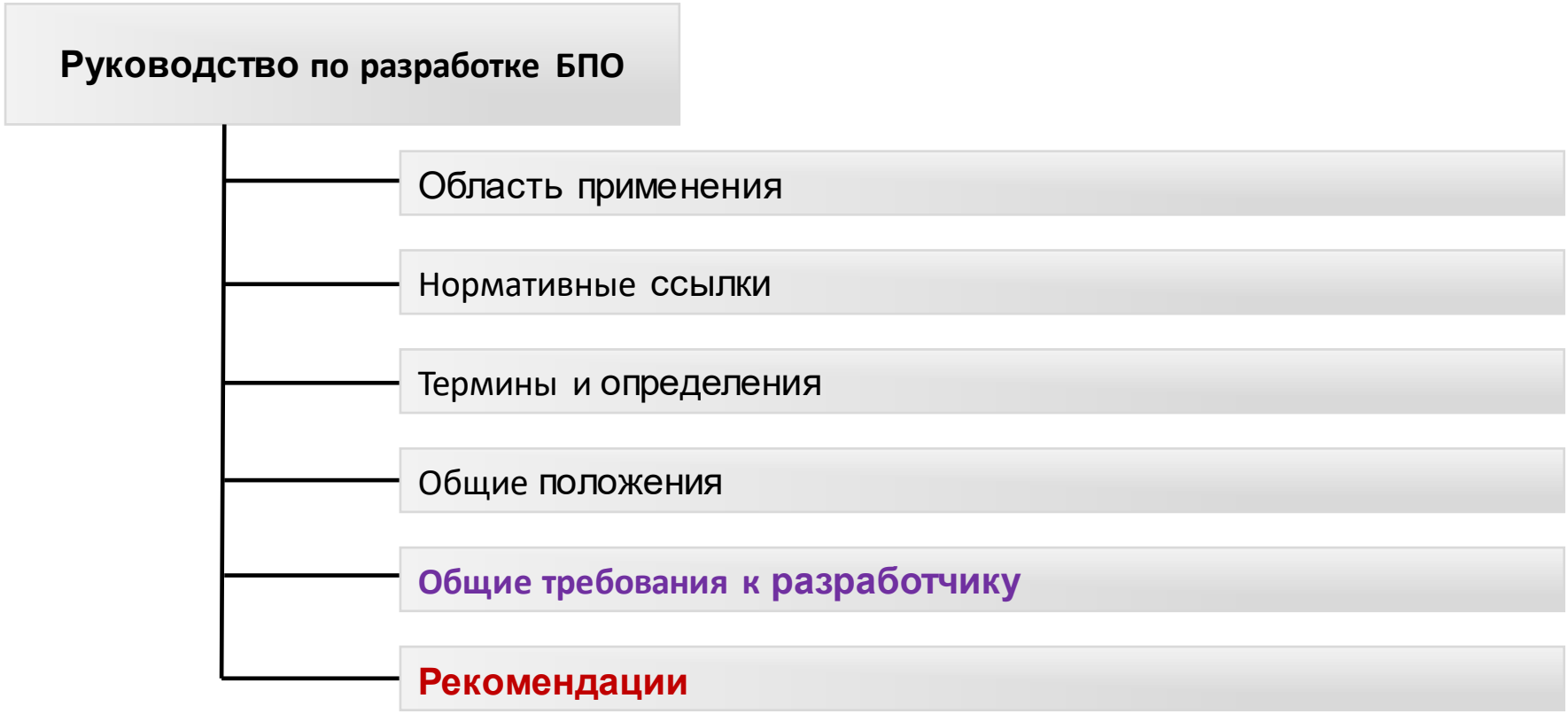


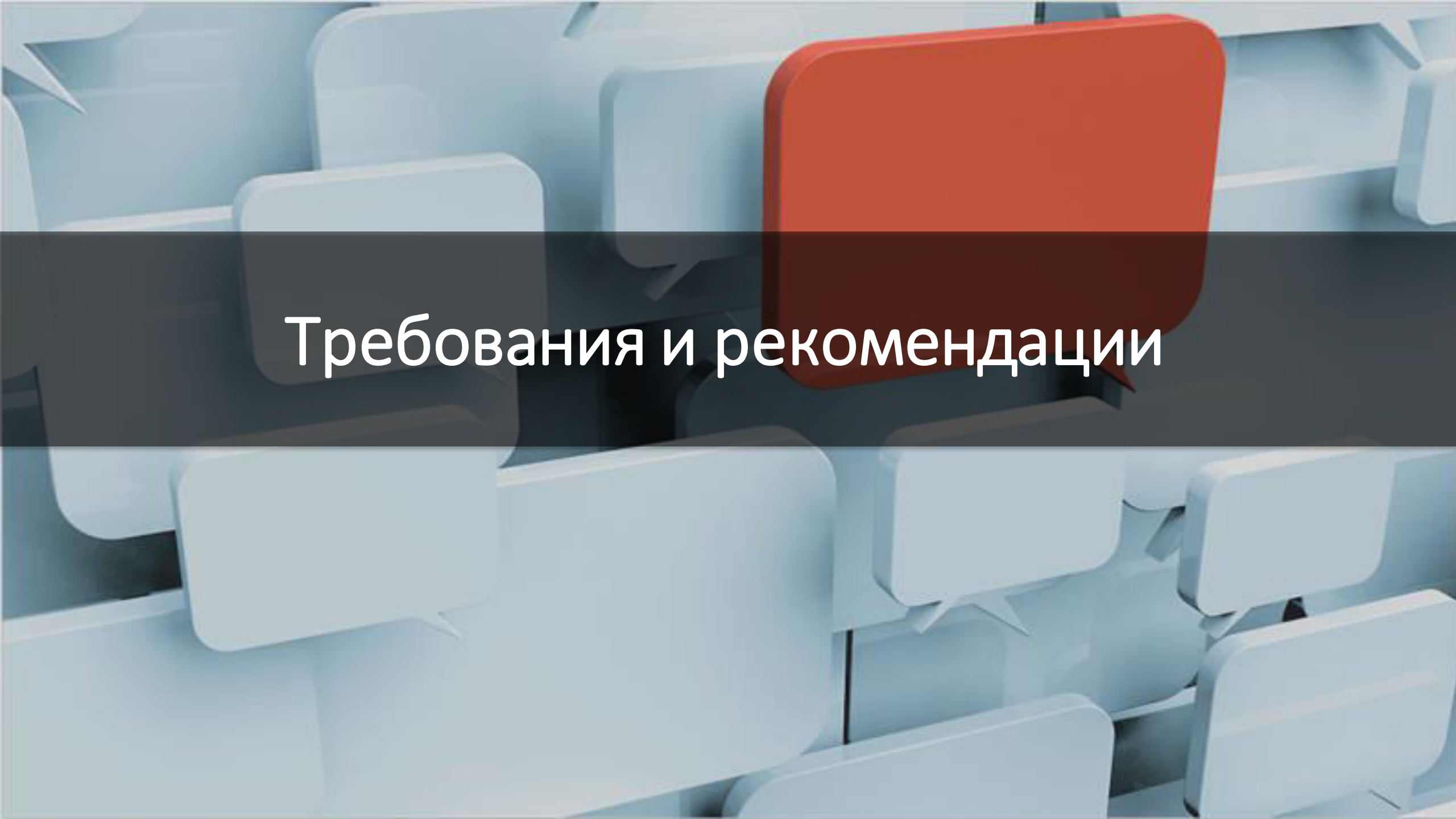
Перечень и описание угроз из готовящегося к публикации стандарта

Рекомендации крупных производителей ПО и исследовательских организаций Microsoft SDL, Veracode, OWASP SAMM

Проект национального стандарта ГОСТ Р XXXXX-201X «Защита информации. Разработка безопасного программного обеспечения. Руководство по разработке безопасного программного обеспечения»

Проект стандарта: структура документа

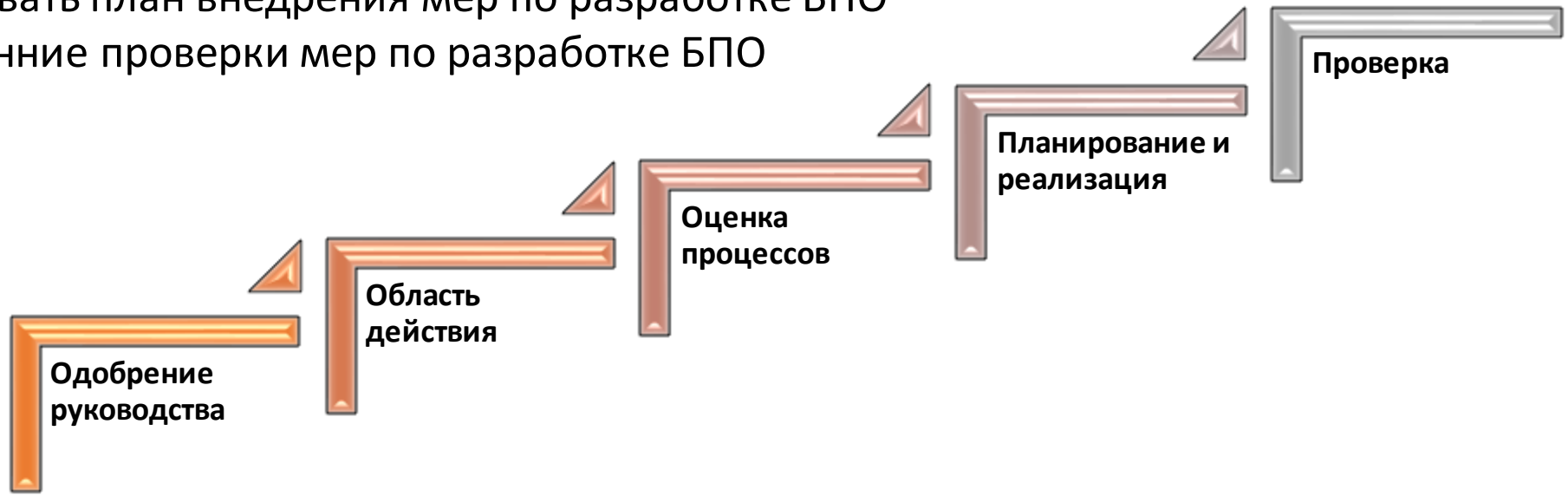




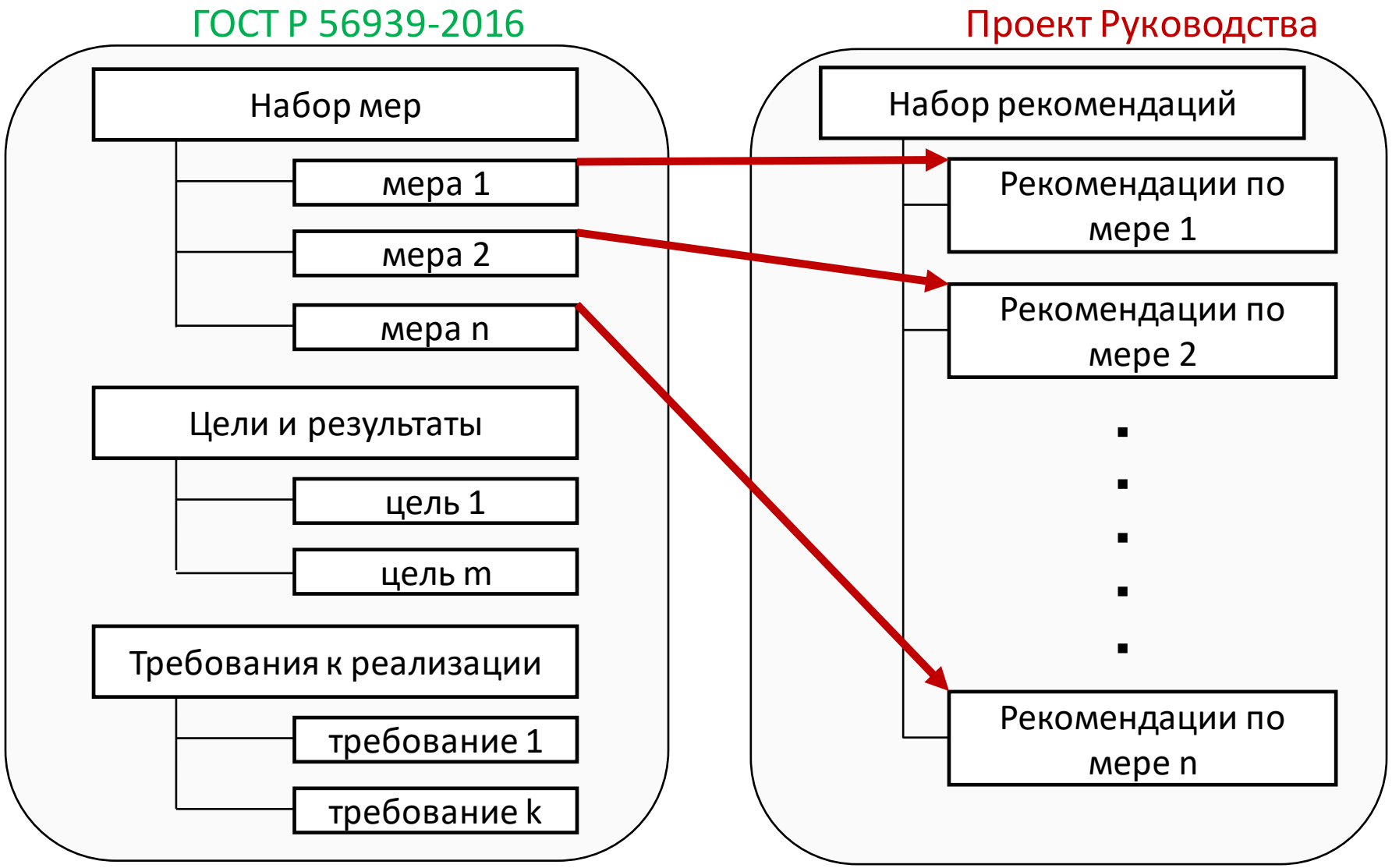
Требования и рекомендации

Требования как основные шаги по внедрению мер по разработке безопасного программного обеспечения

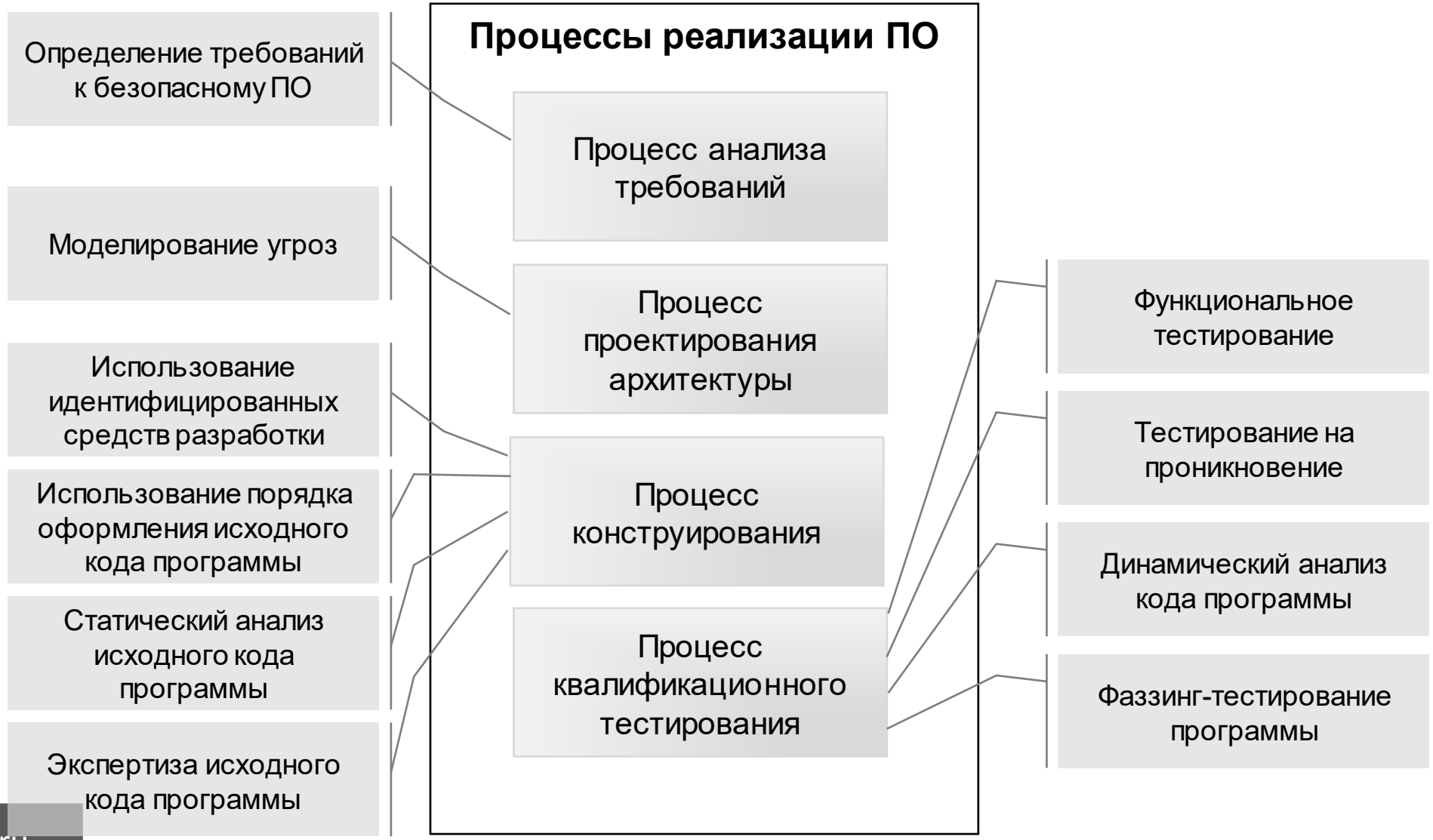
- получить предварительное одобрение руководства разработчика ПО на внедрение мер по разработке БПО
- определить область действия мер по разработке БПО
- оценить существующие процессы с точки зрения выполнения требований к мерам по разработке БПО, установленных ГОСТ Р 56939
- создать и реализовать план внедрения мер по разработке БПО
- выполнять внутренние проверки мер по разработке БПО



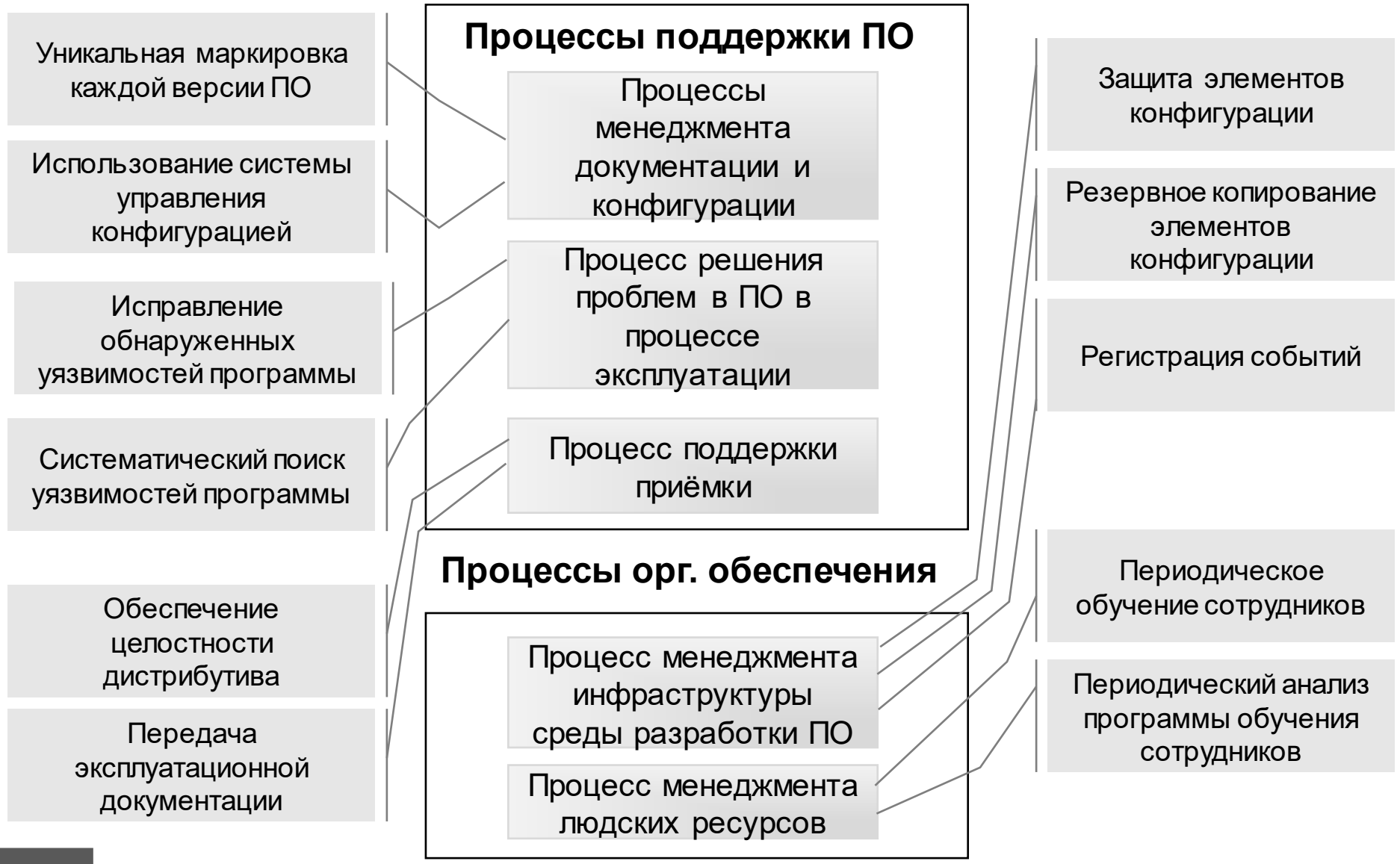
Рекомендации по внедрению и реализации



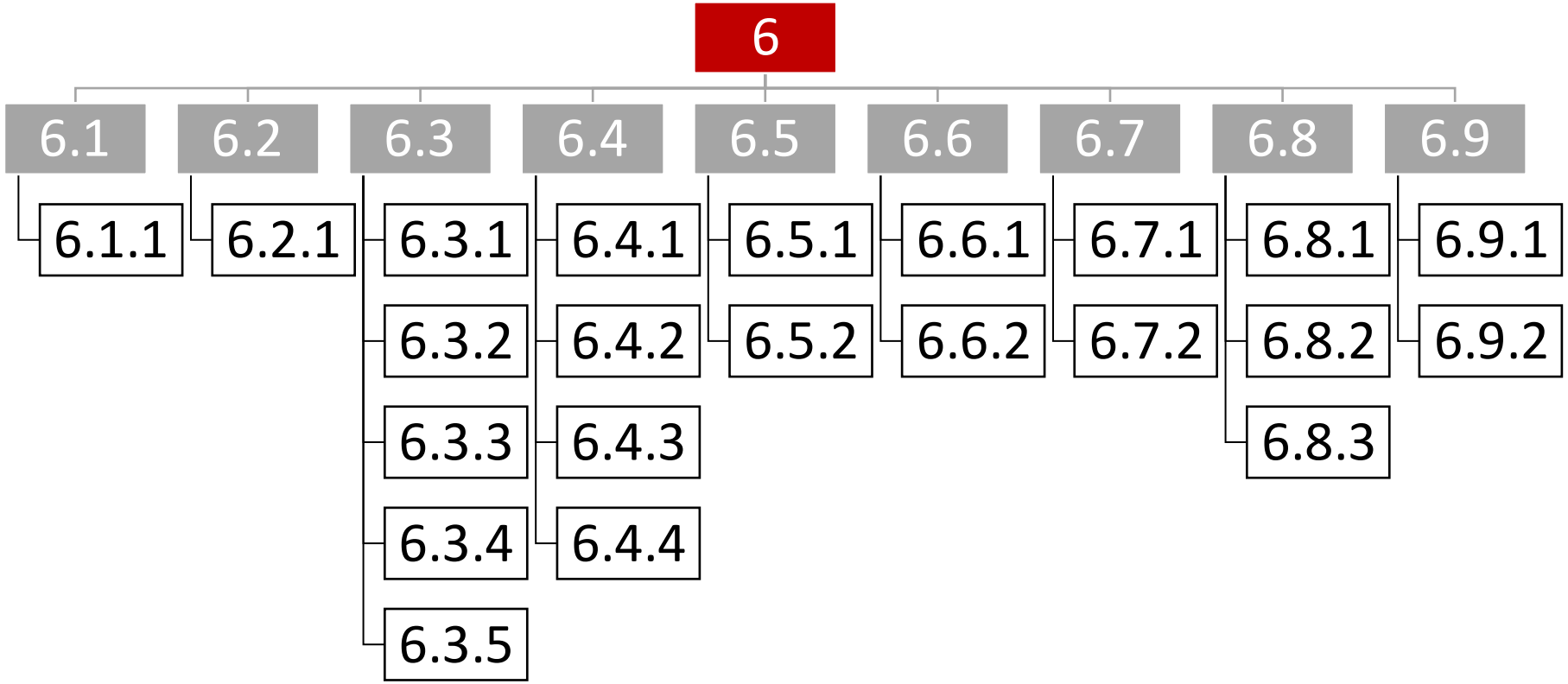
ВСПОМНИМ технические меры из ГОСТ Р 56939-2016 (1)



Далее: технические меры из ГОСТ Р 56939-2016 (2)



Разделение рекомендаций



Элементы описания

Мера по ГОСТ Р 56939

- Описание меры
- Рекомендации
- Перечень документации
- Распределение ролей и обязанностей

Формат представления рекомендаций

ГОСТ Р
(проект, первая редакция)

идентифицированные инструментальные средства. Разработчику ПО следует использовать последние доступные версии инструментальных средств и их возможности по проверке создаваемой программы на наличие проблем, имеющих отношение к разработке безопасного ПО.

6.3.1.2 Рекомендации по реализации меры

Использование идентифицированных инструментальных средств при разработке ПО позволяет получить непротиворечивые и предсказуемые результаты при выполнении процедур, относящихся к различным процессам жизненного цикла ПО.

В общем случае перечень задач, решаемых при реализации меры, выглядит следующим образом:

- идентификация инструментальных средств, которые используются при разработке ПО;
- определение версий инструментальных средств, которые используются при разработке ПО;
- выяснение настройки и параметров функционирования каждого используемого инструментального средства;
- документирование сведений об используемых инструментальных средствах разработки;
- предоставление информации об используемых инструментальных средствах работникам, участвующим в процессе разработки ПО.

Разработчику ПО следует провести исследование процессов разработки с целью определения инструментальных средств, которые используются в ходе реализации процедур безопасной

34

При внедрении меры по разработке безопасного ПО разработчиком ПО должны быть выполнены следующие действия (см. рисунок 1):

а) действие 1:

1) шаг 1.1

2) шаг 1.2

.....

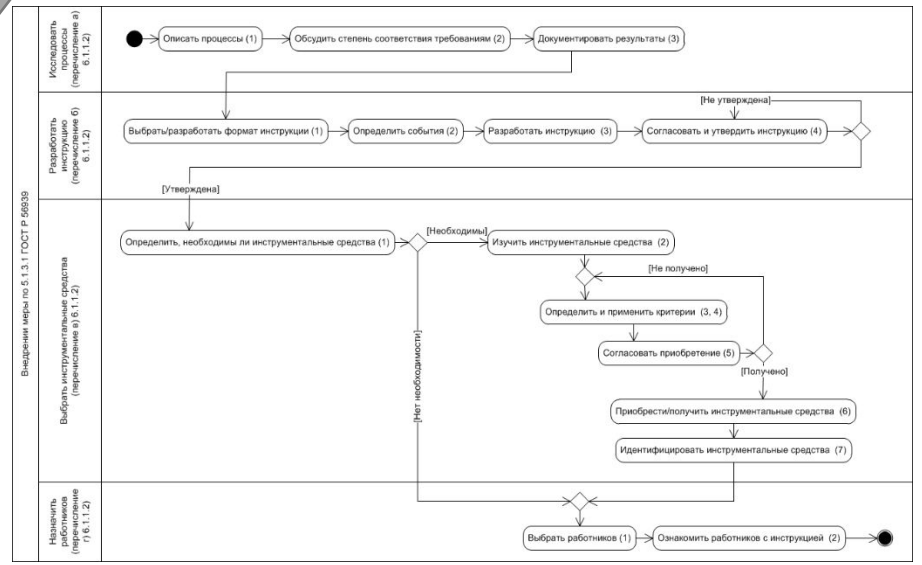
б) действие 2:

1) шаг 2.1

2) шаг 2.2

.....

+



Формат представления рекомендаций

ГОСТ Р
(проект, первая редакция)

6.2.1.4 Распределение ролей и обязанностей, связанных с реализацией меры, между работниками

Рекомендуемое распределение ролей и обязанностей, связанных с реализацией меры по разработке безопасного ПО, выглядит следующим образом:

- специалисты группы разработки безопасного ПО выявляют и формулирует потенциальные угрозы безопасности информации;
- архитектор ПО, специалисты группы разработки ПО проверяют формулировки потенциальные угрозы безопасности информации на адекватность разрабатываемому ПО;
- архитектор ПО, специалисты группы разработки безопасного ПО уточняют проект архитектуры программы.

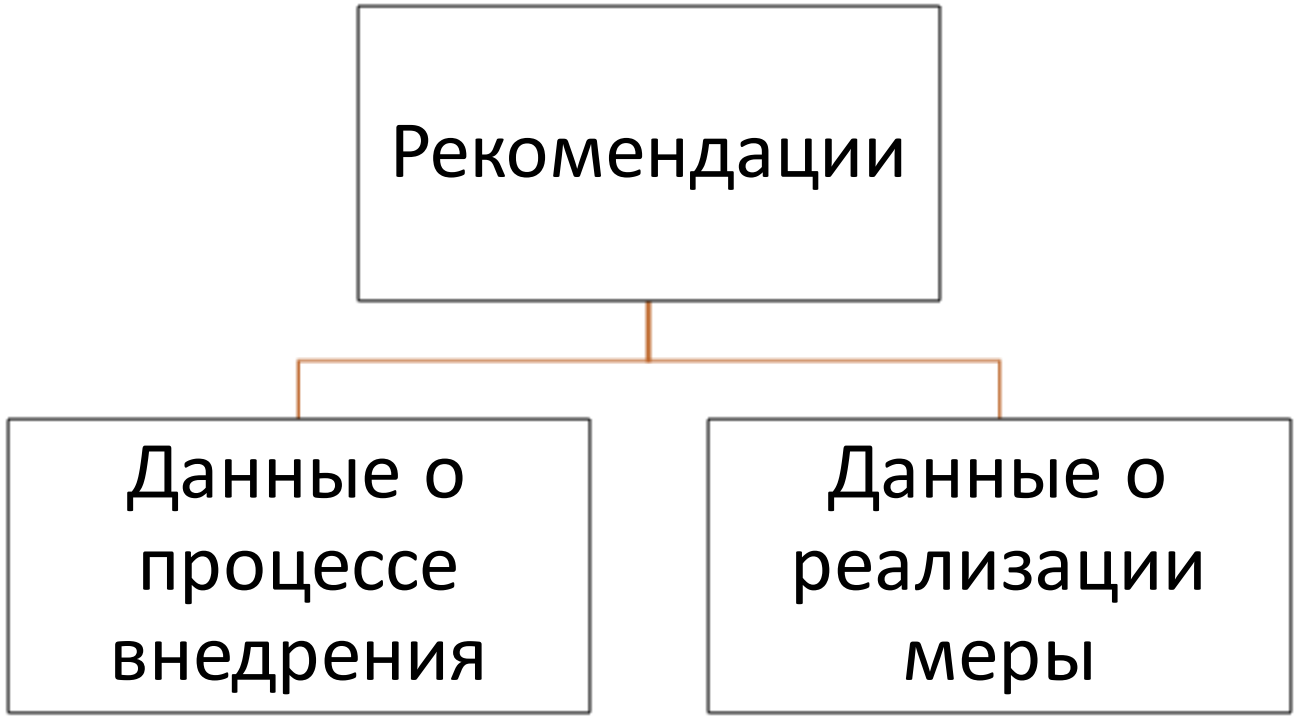
6.1.1.5 Распределение ролей и обязанностей, связанных с внедрением и реализацией меры по разработке безопасного программного обеспечения

Рекомендуемые распределения ролей и обязанностей, связанных с внедрением и реализацией меры по разработке безопасного ПО, представлены в таблицах 6.1 и 6.2.

Таблица 6.1 – Рекомендуемое распределение ролей и обязанностей, связанных с внедрением меры по разработке безопасного ПО

Выполняемое действие	Роль
Перечисление а) 6.1.1.2	Специалист по процессному управлению
Перечисления 1) - 3) перечисления б) 6.1.1.2	Специалист по процессному управлению
Перечисление 4) перечисления б) 6.1.1.2	Специалист группы разработки безопасного ПО Руководитель группы разработки безопасного ПО Руководитель разработки ПО
Перечисление в) 6.1.1.2	Специалист группы разработки безопасного ПО Руководитель группы разработки безопасного ПО
Перечисление г) 6.1.1.2	Руководитель группы разработки безопасного ПО Руководитель разработки ПО

Структура рекомендаций



Типовые вопросы при внедрении

Разработка инструкций и документации

- Выбор и разработка формата
- Определить условия применения процедур
- Разработка описаний
- Утверждение инструкций

Выбор инструментальных средств

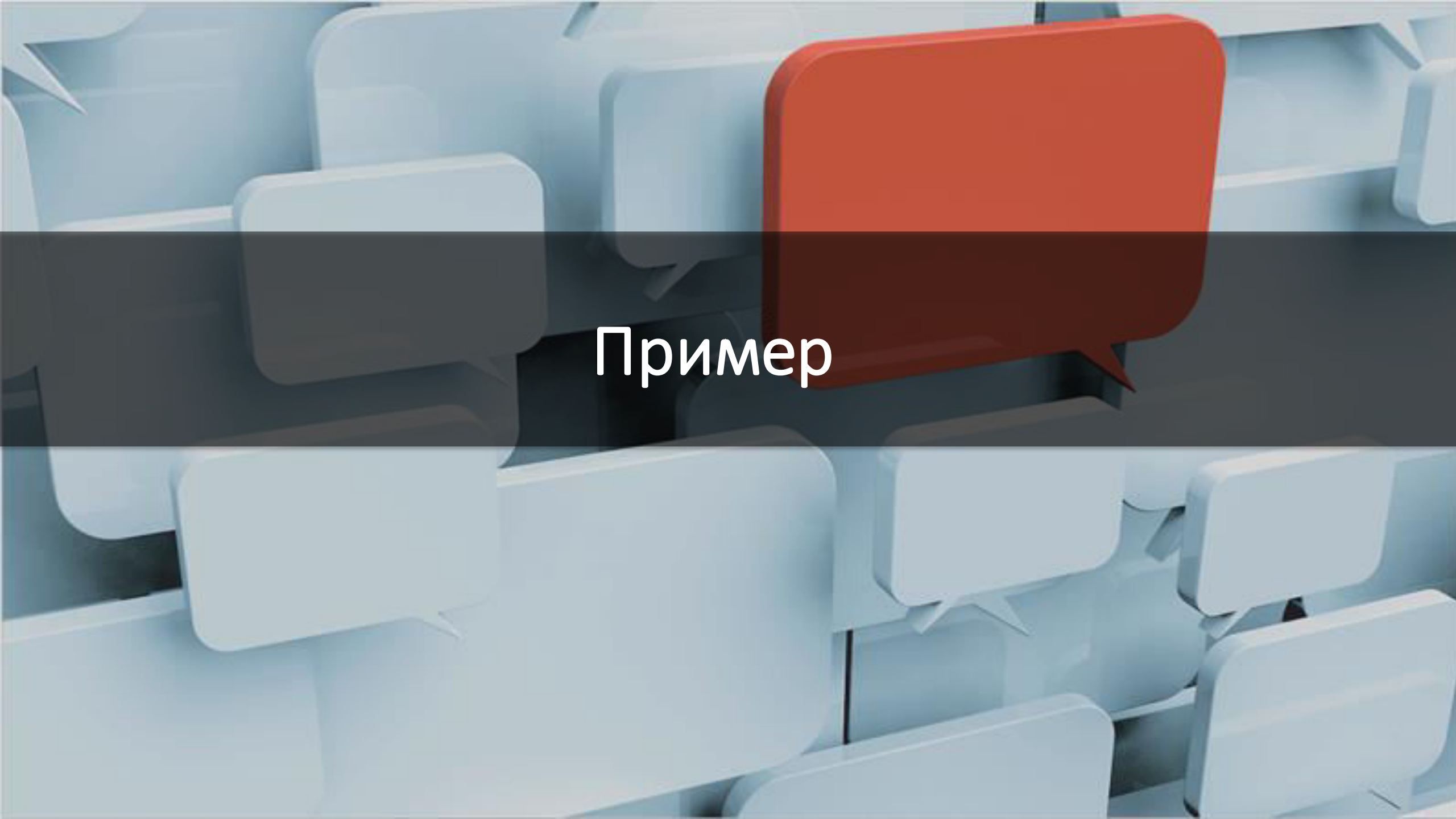
- Необходимость использования
- Исследование существующих средств
- Определение критериев
- Применение критериев
- Согласование приобретения
- Приобретение
- Идентификация инструментальных средств

Назначение ответственных

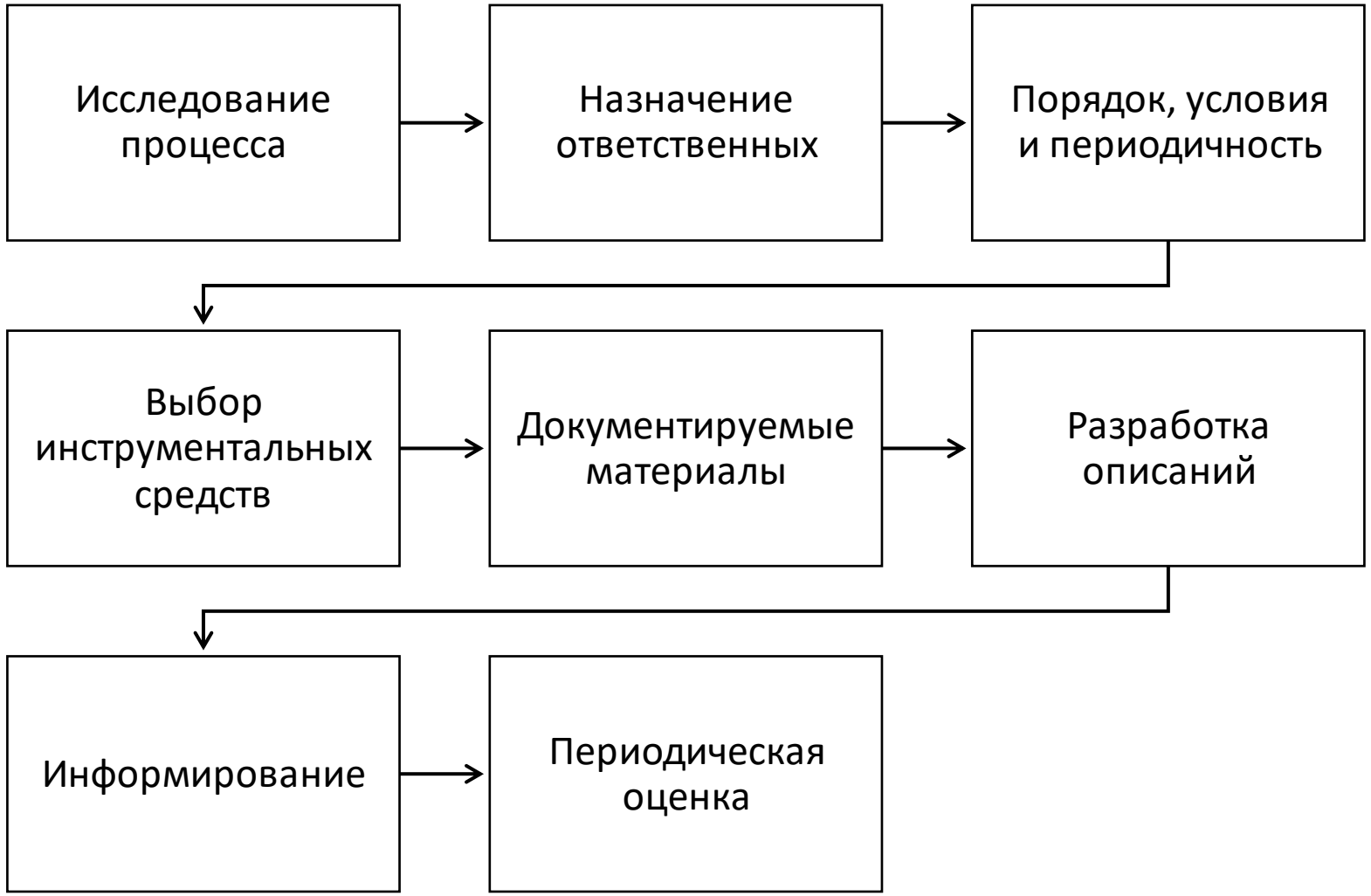
- Выбор работников
- Ознакомление с документацией по применению мер

Примеры инструментальных средств, используемых при реализации мер

Этап работы/задача	Средства автоматизации
Документирование (требования, архитектура)	- текстовые редакторы - средства для совместной работы (wiki, confluence)
Моделирование угроз	- средства автоматизации (MS Threat modeling tools) - Excel
Статический анализ исходного кода	- статический анализатор исходных текстов
Динамический анализ	- эмулятор/интерпретатор - средство выполнения фаззинга - сканер сетевых портов
Тестирование на проникновение	- тестовые программы - программы для создания эксплоитов - сканер уязвимостей
Управление конфигурацией и защита объектов среды разработки	- средства управления конфигурацией, версионирования


Пример

Пример: статический анализ



Статический анализ: ответственные

Разработчики, сборщики

- знание кода и процесса сборки (+)
- ущерб основным обязанностям (-)
- недостаточная осведомленность в ИБ (-)

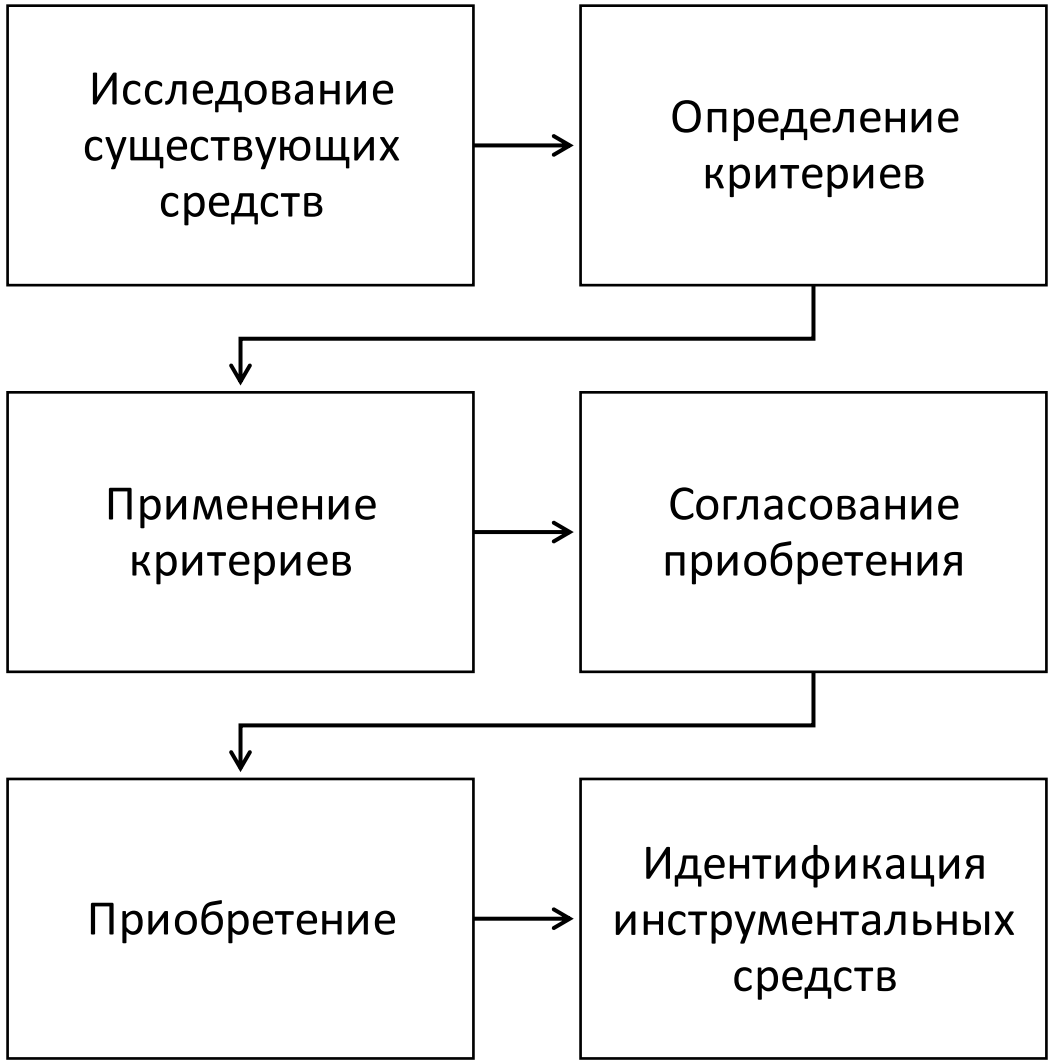
Группа ИБ

- знания и навыки в области ИБ (+)
- вовлечение специалистов в процесс разработки (+)
- недостаточное знание кода и процесса сборки (-)

Внешние исполнители

- = Группа ИБ

Выбор статического анализатора: общий алгоритм



Выбор статического анализатора: характеристики

Характеристики

- поддерживаемые языки программирования
- типы обнаруживаемых недостатков
- методы статического анализа
- возможность интеграции в среду разработки
- простота освоения, наличие документации
- отчеты
- производительность
- требуемые ресурсы
- стоимость лицензий

Статический анализ: когда и как запускать

Условия

- Добавление в репозиторий
- Любая сборка
- Промежуточные версии
- «Релиз»
- Расписание, переходы между фазами проекта

Способ запуска

- Вручную
- Автоматически при выполнении условий

Статический анализ: описание процедур

Инструкции, руководства

- ответственные и их обязанности
- порядок, условия и периодичность проведения статического анализа
- ссылки на руководства по использованию анализаторов
- объем и содержимое документируемых материалов
- порядок обработки результатов

Все в
процессе

Проект стандарта: этапы выполнения проекта

Обсуждения в рамках выполнения НИР:

- 7 организаций – разработчиков ПО
- ~ 150 замечаний и предложений

СПАСИБО ЗА ВНИМАНИЕ!

Максим Гришин, Алексей Марков, mail@cnpo.ru

Контактная информация

107023, Москва, ул. Электрозаводская, 24

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

http://www.npo-echelon.ru

mail@cnpo.ru