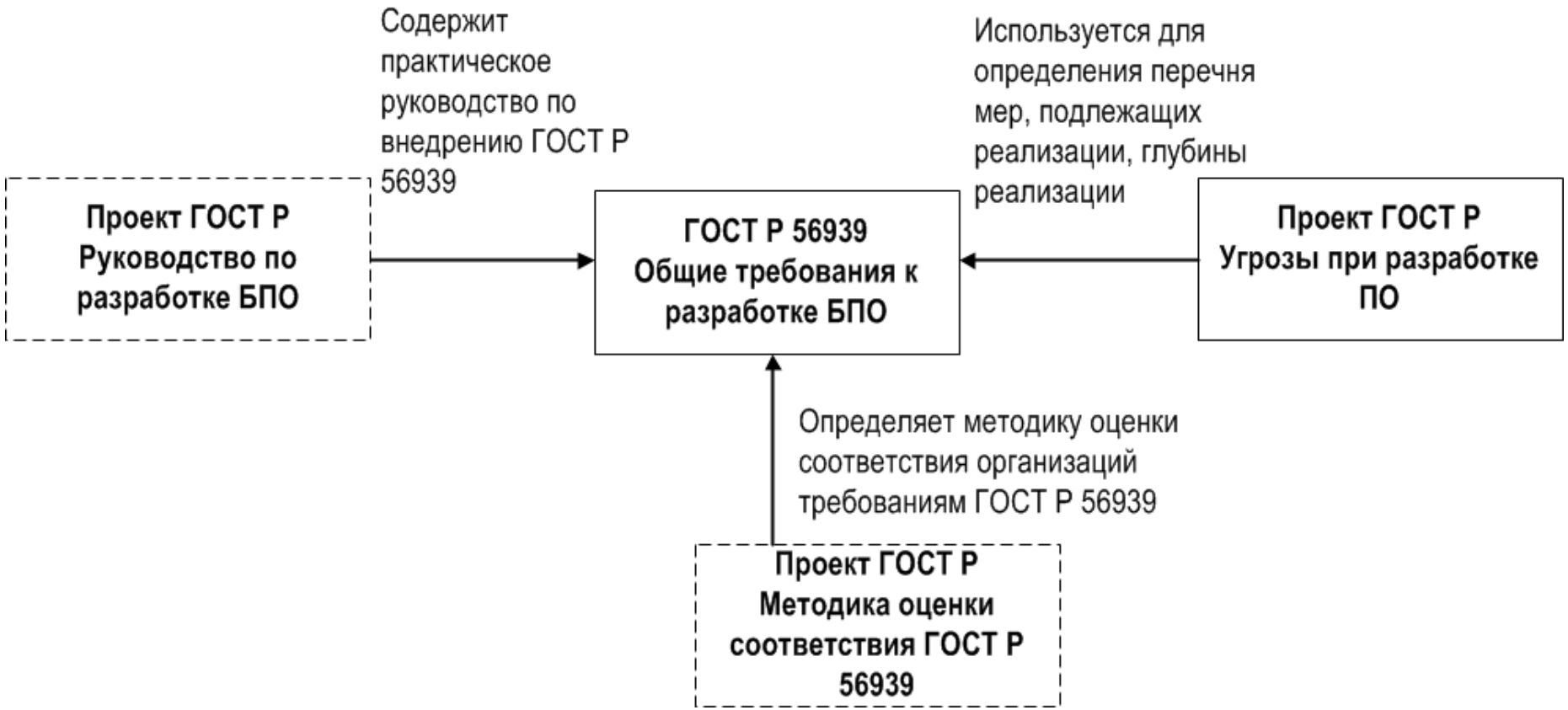
Эшелон
комплексная безопасность

ДЕЙСТВУЮЩИЕ И ПЕРСПЕКТИВНЫЕ НАЦИОНАЛЬНЫЕ СТАНДАРТЫ В ОБЛАСТИ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Александр Барабанов, к.т.н.,
заместитель генерального директора по НИР

СИСТЕМА НАЦИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



ГОСТ Р 56939-2016: ПРЕДПОСЫЛКИ СОЗДАНИЯ

Оценка программного обеспечения

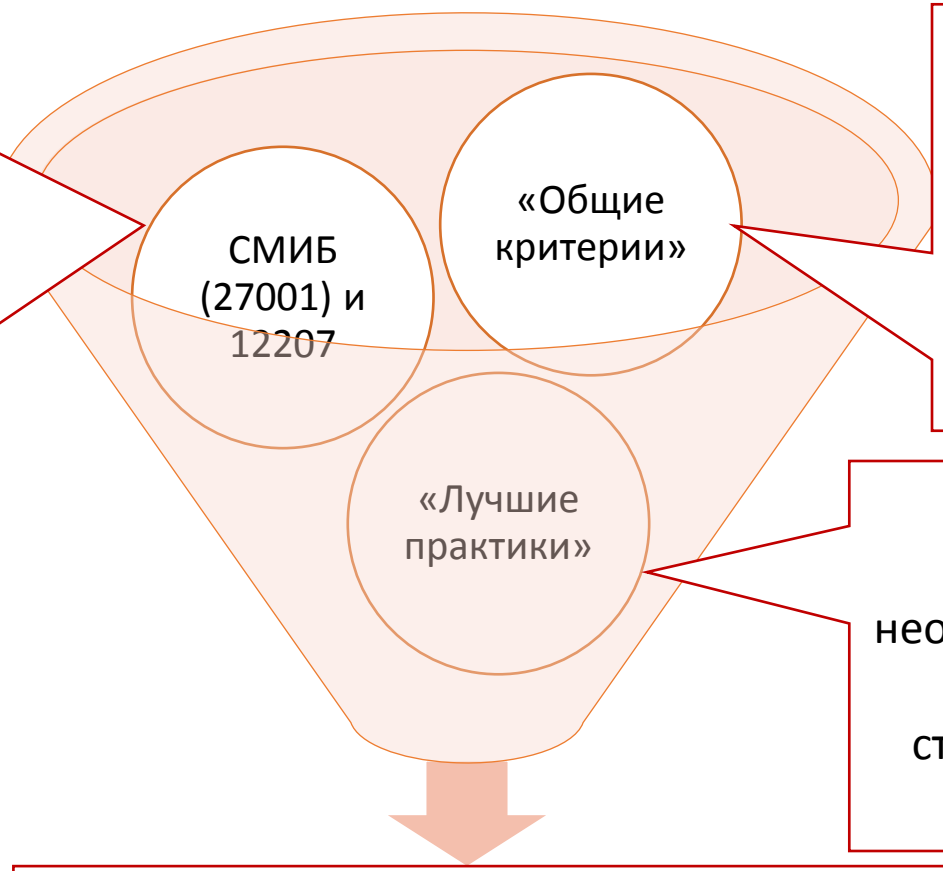
1. Создание и поддержка базы данных уязвимостей ПО
2. Проведение анализа уязвимостей в рамках сертификации (ISO/IEC TR 20004)
3. НПА нового поколения (AVA_VAN)
4. Создание ГОСТ Р по уязвимостям ИС

Оценка процесса разработки

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

ГОСТ Р 56939-2016:ОСОБЕННОСТИ РАЗРАБОТКИ

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

ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

ГОСТ Р 56939-2016: МЕРЫ ПО РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (1)

Меры по разработке безопасного программного обеспечения

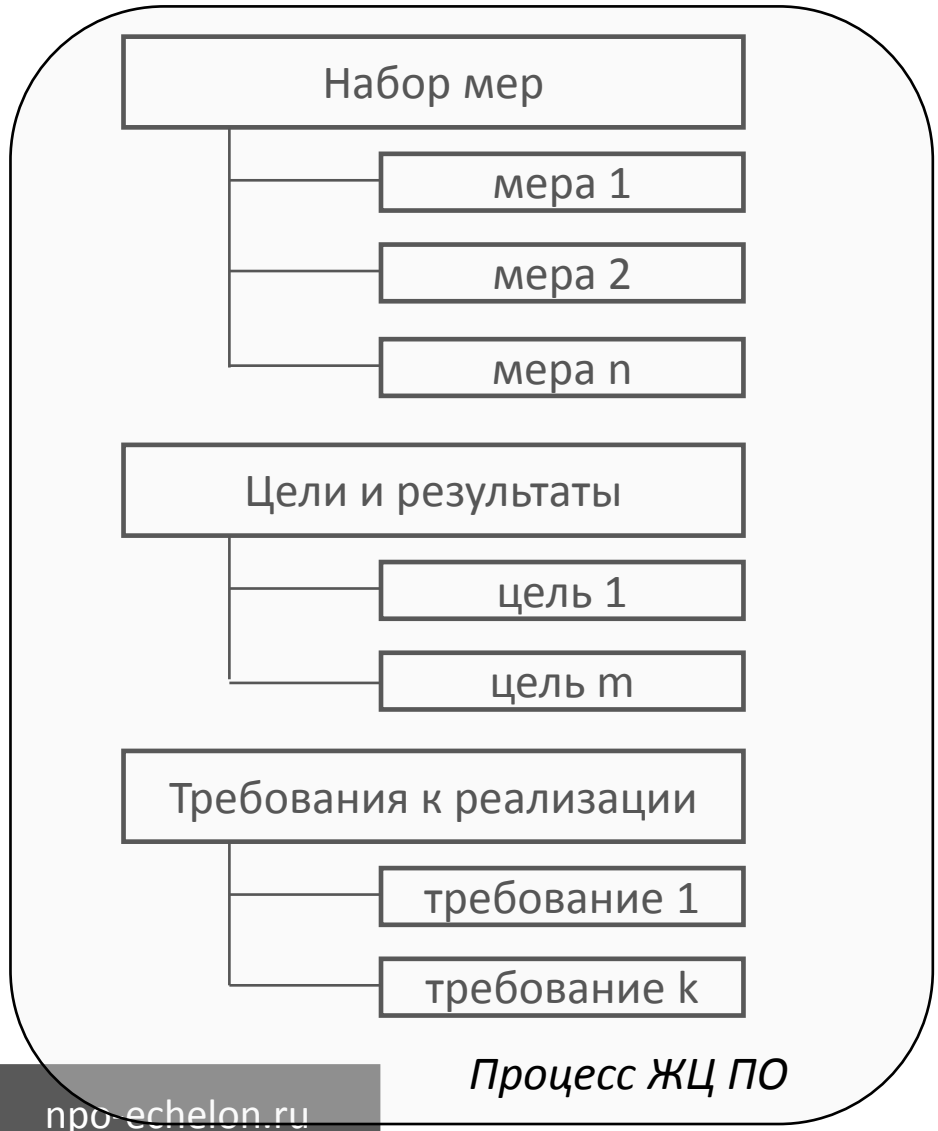
Общие меры:

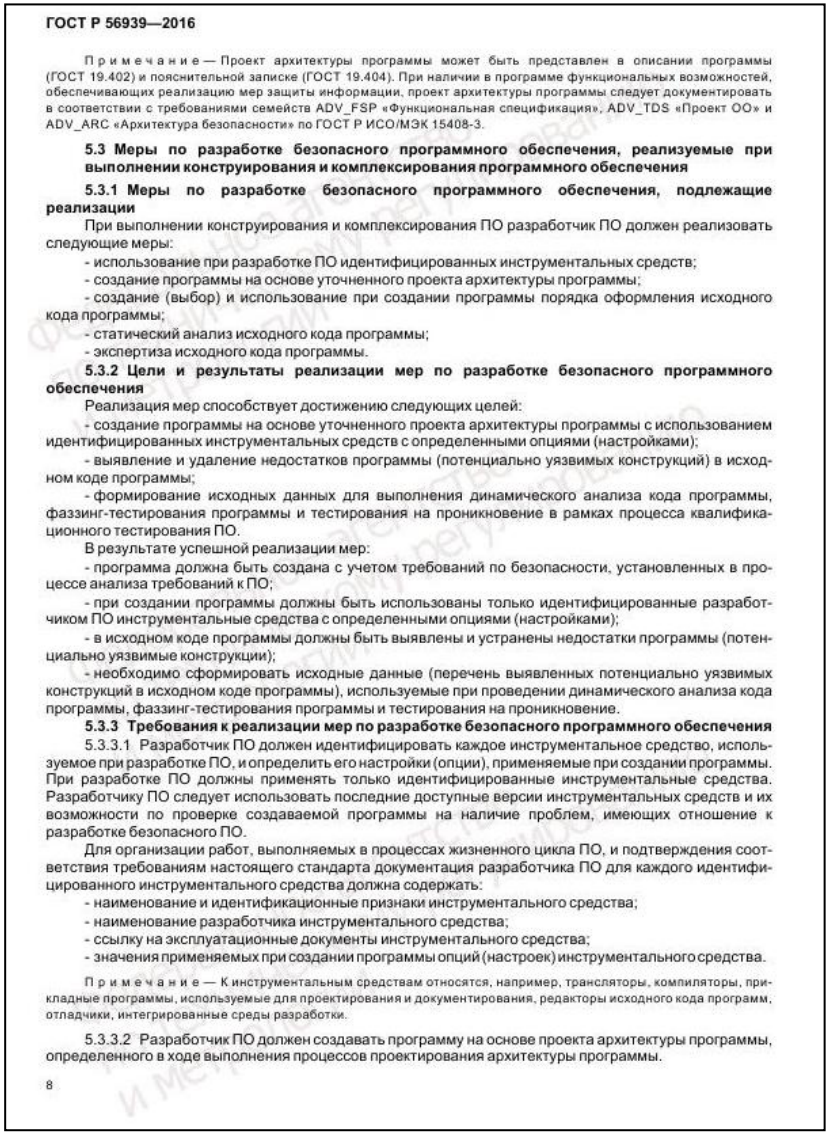
- содержатся в 4 разделе (аналог основной части ISO/IEC 27001)

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

ГОСТ Р 56939-2016: МЕРЫ ПО РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (2)





ГОСТ Р 56939—2016

Примечание — Проект архитектуры программы может быть представлен в описании программы (ГОСТ 19.402) и пояснительной записке (ГОСТ 19.404). При наличии в программе функциональных возможностей, обеспечивающих реализацию мер защиты информации, проект архитектуры программы следует документировать в соответствии с требованиями семейств ADV_FSP «Функциональная спецификация», ADV_TDS «Проект ОО» и ADV_ARC «Архитектура безопасности» по ГОСТ Р ИСО/МЭК 15408-3.

5.3 Меры по разработке безопасного программного обеспечения, реализуемые при выполнении конструирования и комплексирования программного обеспечения

5.3.1 Меры по разработке безопасного программного обеспечения, подлежащие реализации

При выполнении конструирования и комплексирования ПО разработчик ПО должен реализовать следующие меры:

- использование при разработке ПО идентифицированных инструментальных средств;
- создание программы на основе уточненного проекта архитектуры программы;
- создание (выбор) и использование при создании программы порядка оформления исходного кода программы;
- статический анализ исходного кода программы;
- экспертиза исходного кода программы.

5.3.2 Цели и результаты реализации мер по разработке безопасного программного обеспечения

Реализация мер способствует достижению следующих целей:

- создание программы на основе уточненного проекта архитектуры программы с использованием идентифицированных инструментальных средств с определенными опциями (настройками);
- выявление и удаление недостатков программы (потенциально уязвимых конструкций) в исходном коде программы;
- формирование исходных данных для выполнения динамического анализа кода программы, фаззинг-тестирования программы и тестирования на проникновение в рамках процесса квалификационного тестирования ПО.

В результате успешной реализации мер:

- программа должна быть создана с учетом требований по безопасности, установленных в процессе анализа требований к ПО;
- при создании программы должны быть использованы только идентифицированные разработчиком ПО инструментальные средства с определенными опциями (настройками);
- в исходном коде программы должны быть выявлены и устранены недостатки программы (потенциально уязвимые конструкции);
- необходимо сформировать исходные данные (перечень выявленных потенциально уязвимых конструкций в исходном коде программы), используемые при проведении динамического анализа кода программы, фаззинг-тестирования программы и тестирования на проникновение.

5.3.3 Требования к реализации мер по разработке безопасного программного обеспечения

5.3.3.1 Разработчик ПО должен идентифицировать каждое инструментальное средство, используемое при разработке ПО, и определить его настройки (опции), применяемые при создании программы. При разработке ПО должны применять только 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.

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

- наименование и идентификационные признаки инструментального средства;
- наименование разработчика инструментального средства;
- ссылку на эксплуатационные документы инструментального средства;
- значения применяемых при создании программы опций (настроек) инструментального средства.

Примечание — К инструментальным средствам относятся, например, трансляторы, компиляторы, прикладные программы, используемые для проектирования и документирования, редакторы исходного кода программ, отладчики, интегрированные среды разработки.

5.3.3.2 Разработчик ПО должен создавать программу на основе проекта архитектуры программы, определенного в ходе выполнения процессов проектирования архитектуры программы.

8

ВЗАИМОСВЯЗЬ РАЗРАБОТАННОГО СТАНДАРТА С ДРУГИМИ НАЦИОНАЛЬНЫМИ СТАНДАРТАМИ

ПРОЕКТ ГОСТ Р «…УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

УГРОЗЫ БЕЗОПАСНОСТИ: ПРИМЕР ОПИСАНИЯ УГРОЗЫ

Параметр	Описание параметра
Описание угрозы	Данная угроза заключается в преднамеренном внедрении в разрабатываемую программу заимствованных у сторонних разработчиков ПО компонентов, содержащих уязвимости программы. Уязвимости программы, появившиеся из-за применения уязвимых компонентов, в дальнейшем могут быть использованы с целью выполнения компьютерных атак на информационные системы пользователей, применяющих ПО. Реализация данной угрозы внутренним нарушителем может осуществляться путем внесения изменений в программные модули или исходный код программ сторонних разработчиков ПО, используемые при разработке программы в среде разработки ПО или в процессе их передачи из среды разработки стороннего разработчика ПО. Изменения могут вноситься путем санкционированного или несанкционированного доступа к указанным модулям. Внешний нарушитель может реализовывать данную угрозу путем удаленного доступа (из внешних сетей связи общего пользования и (или) сетей международного информационного обмена) к программным модулям или исходному коду программ сторонних разработчиков ПО, используемым при разработке программы. Реализация данной угрозы внешним нарушителем возможна при условии подключения среды разработки ПО к внешним сетям связи общего пользования и (или) сетям международного информационного обмена. Угроза обусловлена недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и мерах по разработке безопасного ПО, связанных с управлением конфигурацией ПО и с проведением систематического поиска уязвимостей программы.
Источники угрозы	Источниками угрозы являются: - внутренний нарушитель, обладающий низким потенциалом, при реализации угрозы безопасности информации путем внесения изменений в программные модули или исходный код программ сторонних разработчиков ПО, осуществляя санкционированный доступ; - внутренний нарушитель, обладающий средним потенциалом, при реализации угрозы безопасности информации путем внесения изменений в программные модули или исходный код программ сторонних разработчиков ПО, осуществляя несанкционированный доступ; - внешний нарушитель, обладающий высоким потенциалом.
Объект воздействия	Объектами воздействия данной угрозы являются программные модули или исходный код программ сторонних разработчиков ПО, используемые при разработке программы.
Последствия реализации угрозы	Последствиями реализации угрозы являются: - нарушение целостности программных модулей или исходного кода программ сторонних разработчиков ПО, используемых при разработке программы; - внедрение в программу уязвимостей, которые могут быть использованы для выполнения компьютерных атак на информационные системы пользователей, применяющих ПО.

СПАСИБО ЗА ВНИМАНИЕ!

Александр Барабанов
к.т.н, CISSP, CSSLP
Заместитель генерального директора по НИР
a.barabanov@npo-echelon.ru


Эшелон
комплексная безопасность