RTM GROUP

ОУД4 – коротко о сложном

RTM TECHNOLOGIES — первая экспертная компания, специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

СОДЕРЖАНИЕ

ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

ТРЕБУЕТСЯ

- Анализ уязвимостей по ОУД4 в соответствии с ГОСТ 15408 (382-П, 683-П и т.д.)

РЕКОМЕНДУЕТСЯ

- Использовать профиль защиты
- Применять ГОСТ 57628

ПРОФИЛЬ ЗАЩИТЫ

РАЗРАБОТАН

- ТК-122 рекомендовал принять ПЗ **с учетом правок**

ВВЕДЕН

- Банком России как **рекомендуемый и без учета правок от ТК-122**

ЦИТАТА

- Элементы действий разработчика
- **AVA_VAN.5**.1DОценщик должен представить ОО для тестирования

СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

Анализ уязвимостей

- 382-П, 683-П (684-П)

Соответствие

- 719-П, проект 683-П (684-П)

СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

Анализ уязвимостей

Анализ уязвимостей по ОУД4 в соответствии с ГОСТ 15408 (382-П, 683-П и т.д.) представляет собой исследование программного продукта на наличие недостатков и уязвимостей, а также возможности использования этих уязвимостей.

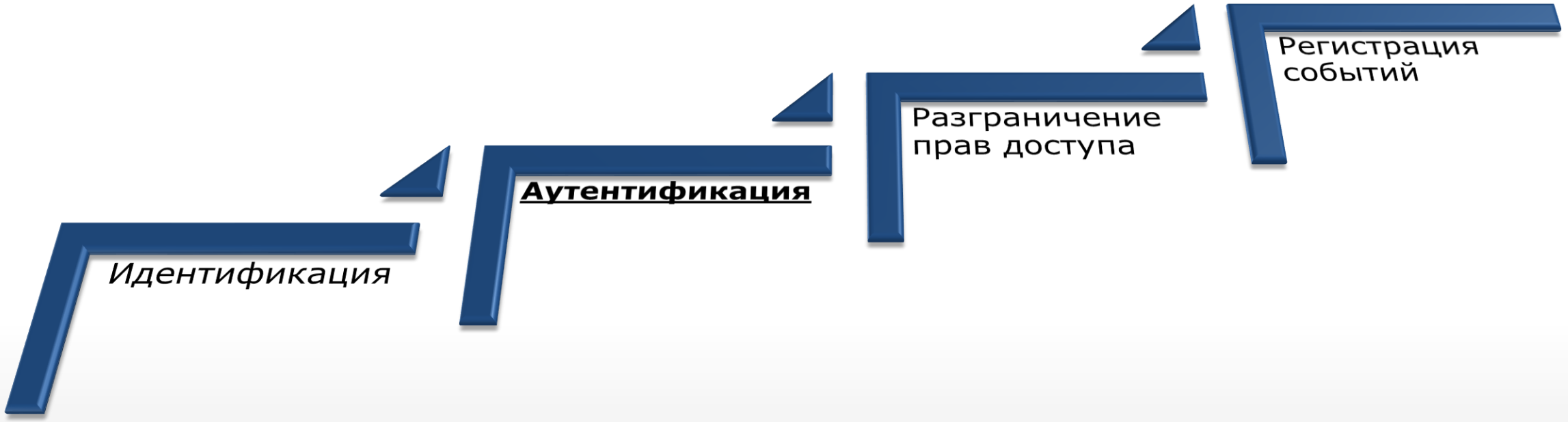
При анализе уязвимостей рассматриваются угрозы потенциальных действий нарушителя, способного обнаружить недостатки безопасности, которые позволят осуществить несанкционированный доступ к данным и функциональным возможностям, а также ограничивать санкционированные возможности других пользователей.

Результатом исследования является заключение, которое основывается на результатах анализа, выполненного оценщиком, и поддерживается тестированием, проведенным оценщиком.

СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

Анализ уязвимостей

В ходе анализа уязвимостей по ОУД4 эксперты RTM Group делают акцент на исследовании функций безопасности, а не на программном продукте в целом:

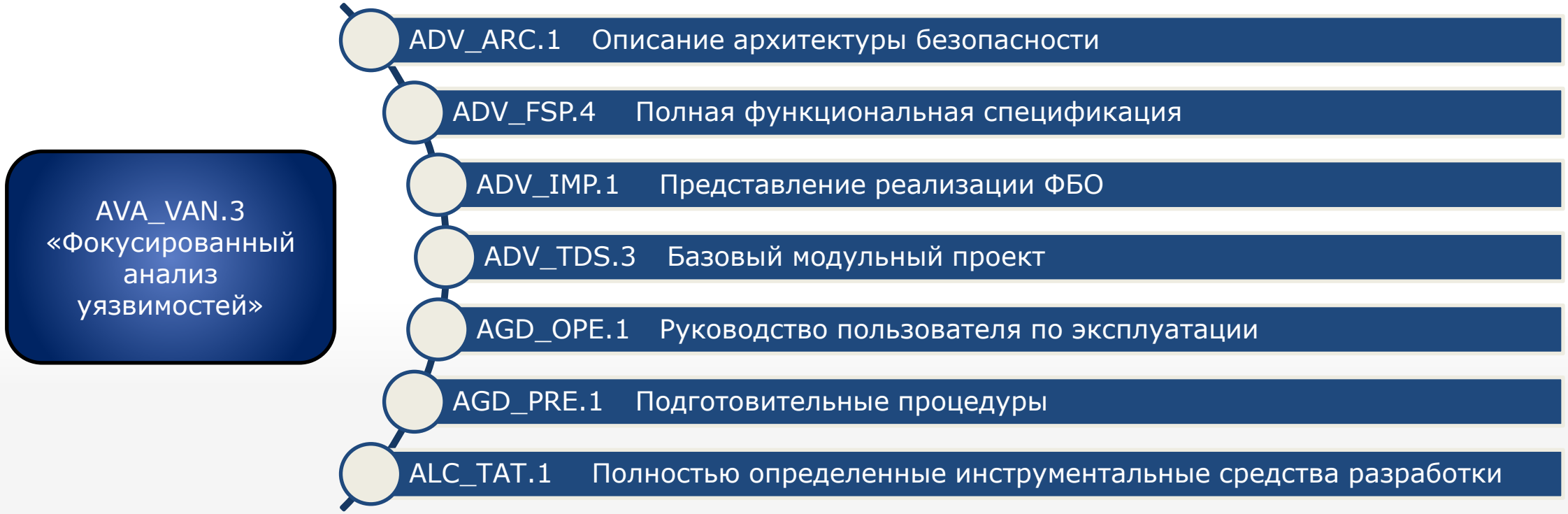


СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Оценка задания по безопасности	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_VAN	1	2	2	3	4	5	5

АНАЛИЗ УЯЗВИМОСТЕЙ

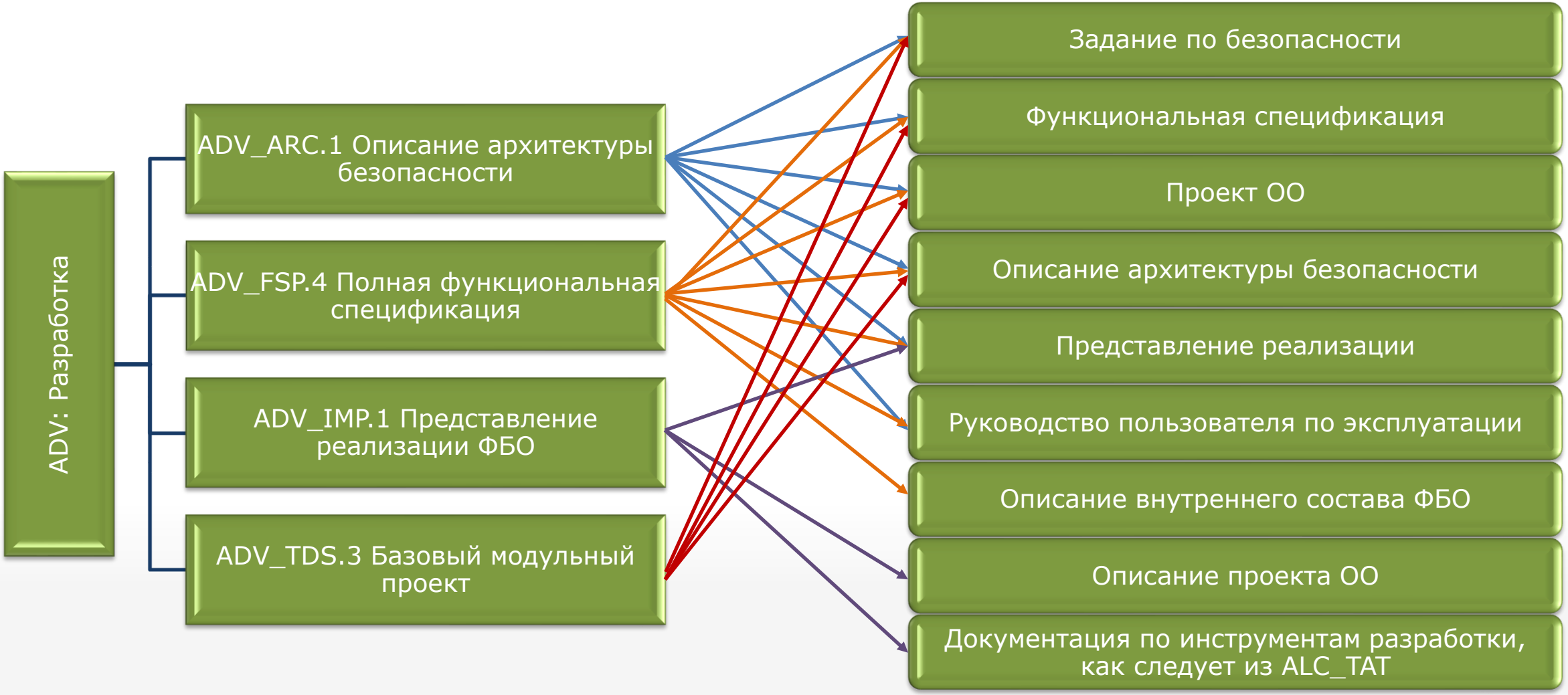
Анализ уязвимостей по требованиям к четвёртому оценочному уровню доверия (ОУД 4) – анализ на соответствие компоненту доверия AVA_VAN.3 «Фокусированный анализ уязвимостей» и полной совокупности компонентов доверия-зависимостей:



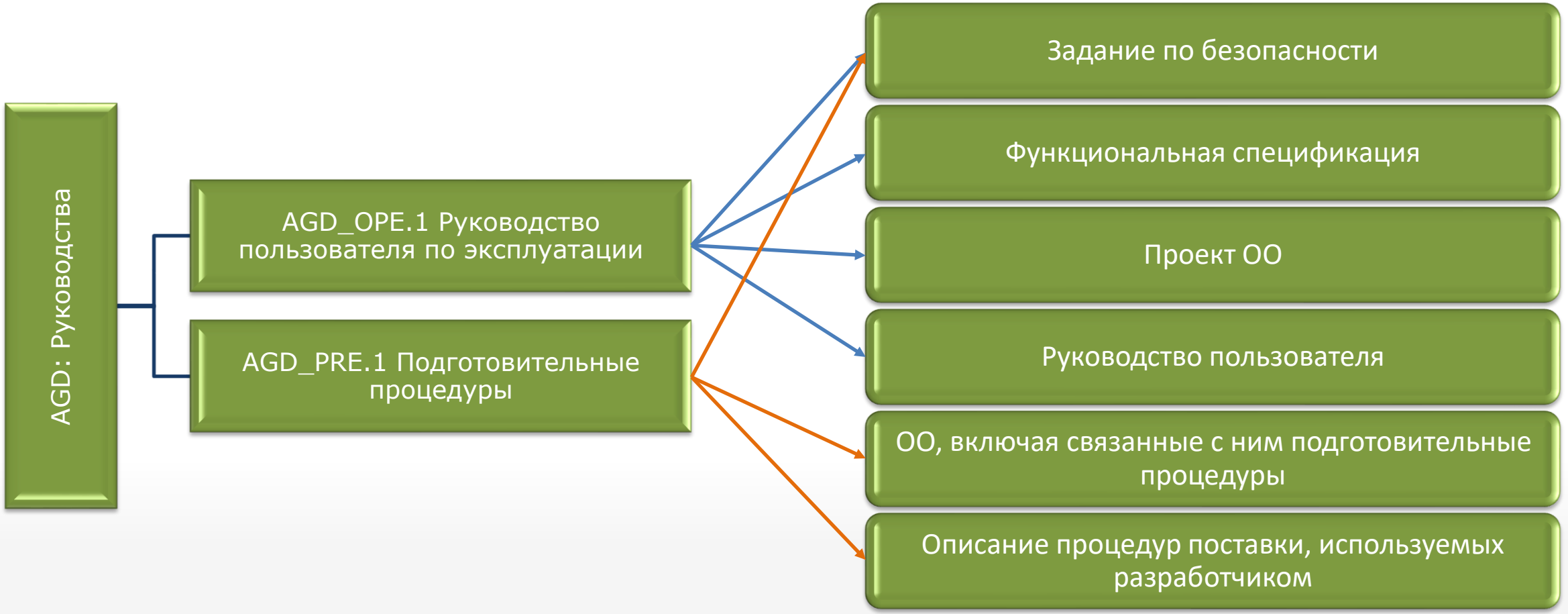
АНАЛИЗ УЯЗВИМОСТЕЙ

Цель анализа уязвимостей - сделать заключение, имеет ли программный продукт, находящийся в своей среде функционирования, уязвимости, пригодные для использования нарушителями, обладающими Усиленным базовым потенциалом нападения.

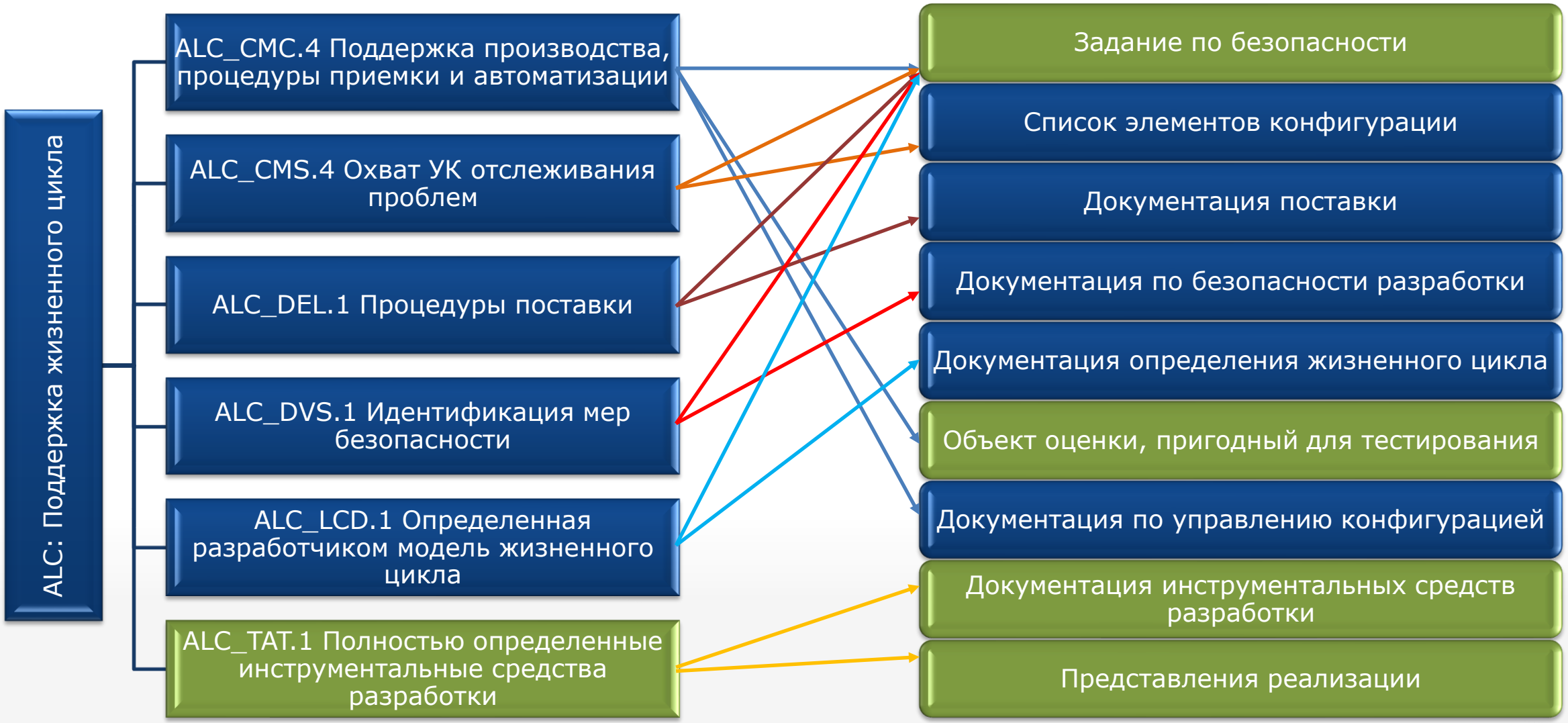
СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ



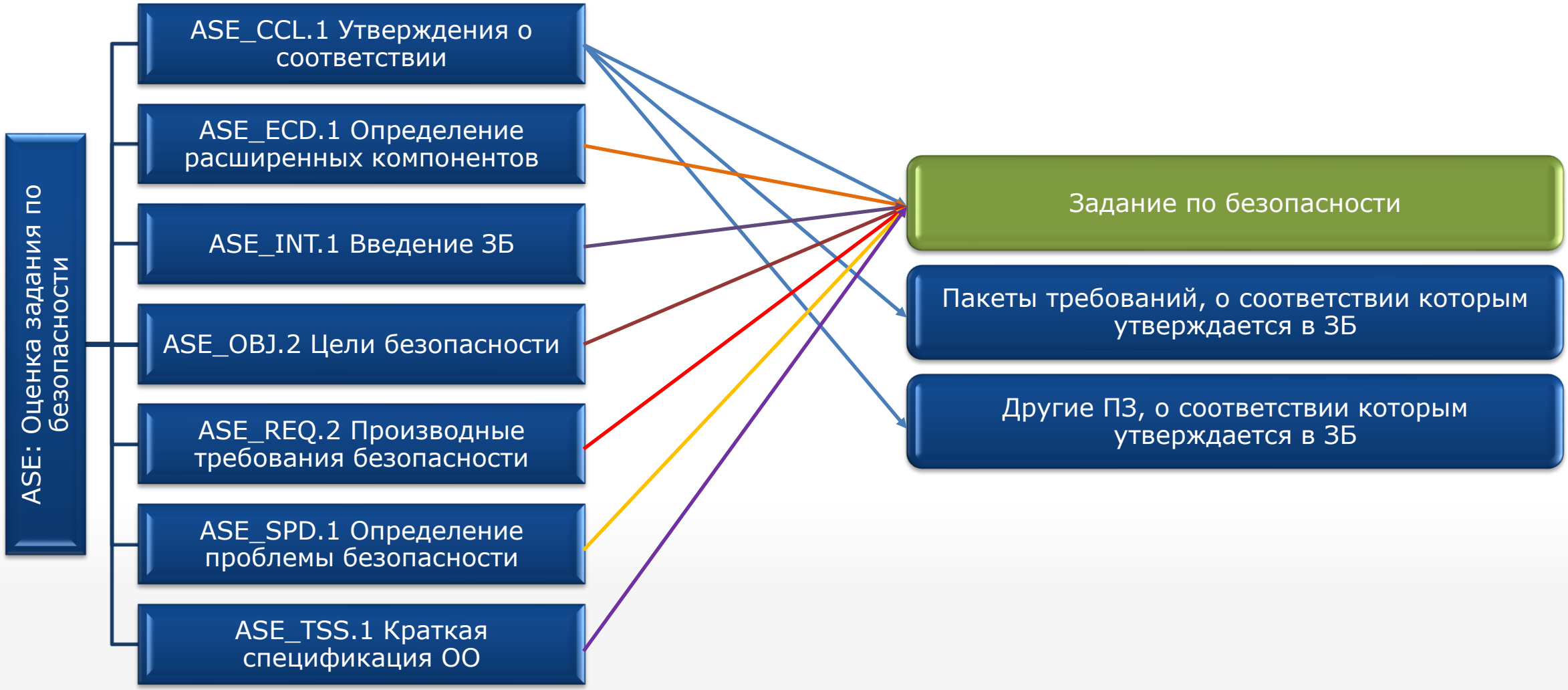
СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ



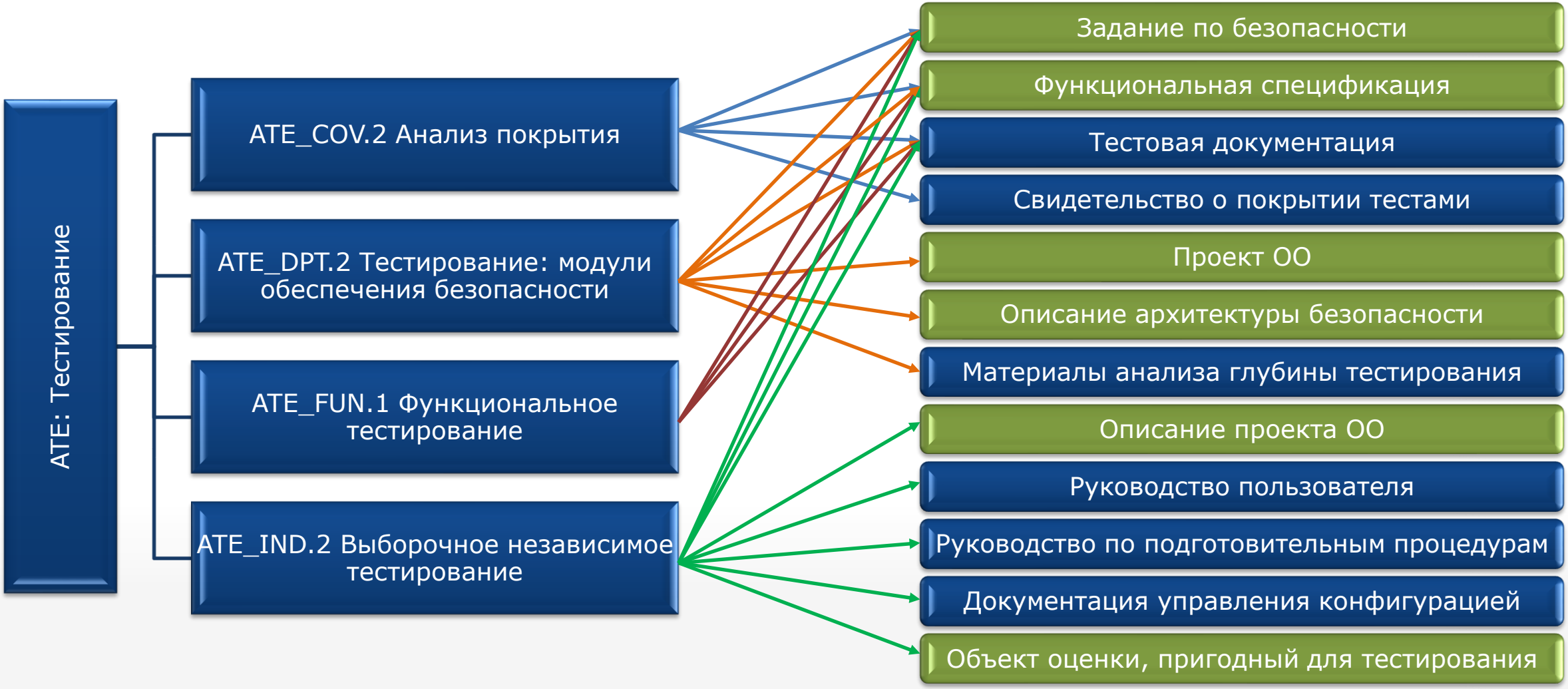
СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ



СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ



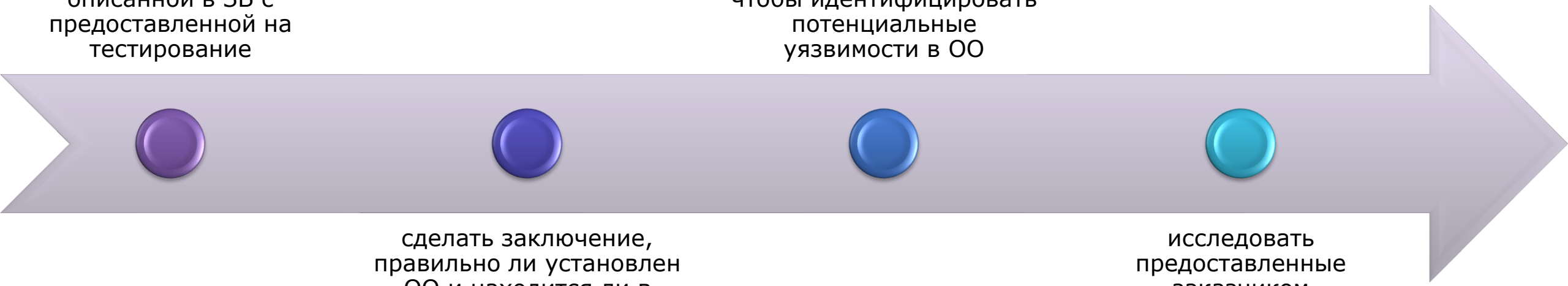
СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ



АНАЛИЗ УЯЗВИМОСТЕЙ

АНАЛИЗ УЯЗВИМОСТЕЙ

исследовать предоставленный заказчиком ОО на предмет соответствия конфигурации, описанной в ЗБ с предоставленной на тестирование



сделать заключение, правильно ли установлен ОО и находится ли в состоянии, которое известно

исследовать общедоступные источники информации, чтобы идентифицировать потенциальные уязвимости в ОО

исследовать предоставленные заказчиком свидетельства, чтобы идентифицировать возможные потенциальные уязвимости в ОО

АНАЛИЗ УЯЗВИМОСТЕЙ

задокументировать в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к данному ОО в среде его функционирования

на основе полученного списка потенциальных уязвимостей оценщик должен разработать тесты проникновения

разработать документацию для тестов проникновения

провести тестирование (статический и динамический анализ)* проникновения, и описать ход его проведения

**Статический анализ – проверяются файлы исходных текстов модулей ОО (Vulners DB, Exploit-DB, Shodan, dnSpy, Roslynator).*

Динамический анализ – проверяется ОО, предоставленный заказчиком в виде веб-приложения (Shodan, Exploit-DB, Vulners DB, Rapid7 AppSpider, BurpSuite, nmap, sqlmap, wfuzz).

АНАЛИЗ УЯЗВИМОСТЕЙ

зафиксировать фактические результаты тестов проникновения

задокументировать в ТОО свои действия по тестированию проникновения, включая условия и обобщённые результаты анализа уязвимостей на этапе подготовки к проведению тестирования проникновения

на основе результатов тестирования проникновения и выводов по анализу уязвимостей, дать заключение, является ли ОО, находящийся в своей среде функционирования, стойким к нарушителю, обладающему Усиленным базовым потенциалом нападения

задокументировать в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях

СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

RTM TECHNOLOGIES

ООО «РТМ ТЕХНОЛОГИИ», 111398, город Москва, улица Плющева, дом 17, корпус 2, пом.I, ком.1, ОГРН 1167746366875, ИНН/КПП 7720337868/772001001, +7 (495) 309-31-25, https://www.rtmtech.ru/, info@rtmtech.ru

Управляющий
ООО «РТМ ТЕХНОЛОГИИ»
_____ ИП Царев Е.О.
« » октября 2020 г.

Технический отчёт

по результатам проведения анализа уязвимостей
в соответствии с требованиями национального стандарта Российской Федерации
ГОСТ Р ИСО/МЭК 15408-3-2013

Цели анализа

Дата и номер отчёта	05 октября 2020 года, № 2020-78
Заказчик работ по анализу	ООО «СэйфТек»
Собственник объекта анализа	ООО «СэйфТек»
Название объекта анализа	Программный комплекс «PayControl»
Версия объекта анализа	v5
Уровень соответствия	Требования к анализу уязвимостей по четвёртому оценочному уровню доверия (ОУД 4)
Разработчик объекта анализа	ООО «СэйфТек»

Результаты анализа: Положительные, соответствие подтверждено

В отношении Программного комплекса «PayControl» версии v5 успешно проведены и получены положительные результаты анализа уязвимостей по требованиям к четвёртому оценочному уровню доверия (ОУД 4) в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013.

СПАСИБО ЗА ВНИМАНИЕ!

Фёдор Музалевский

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

+79081472741

f.muzalevsky@rtmtech.ru

https://rtmtech.ru

GroupRTM

rtm.group

@GroupRtm

rtm.group.Russia

t.me/kurilka_ib