

Формирование правил кодирования

В чем подвох?



Static analyses are a collective term which includes analysis such as searching the source code text or the model for patterns matching known faults or compliance with modelling or **coding guidelines**.

Вводные для создания правил

Лучшие практики и опыт экспертов

Вопросы на ревью

RCA для багов и реп-багов

Стандарты: MISRA, AUTOSAR

Гайды: SEI CERT, CppCoreGuidelines

Правила стат анализаторов



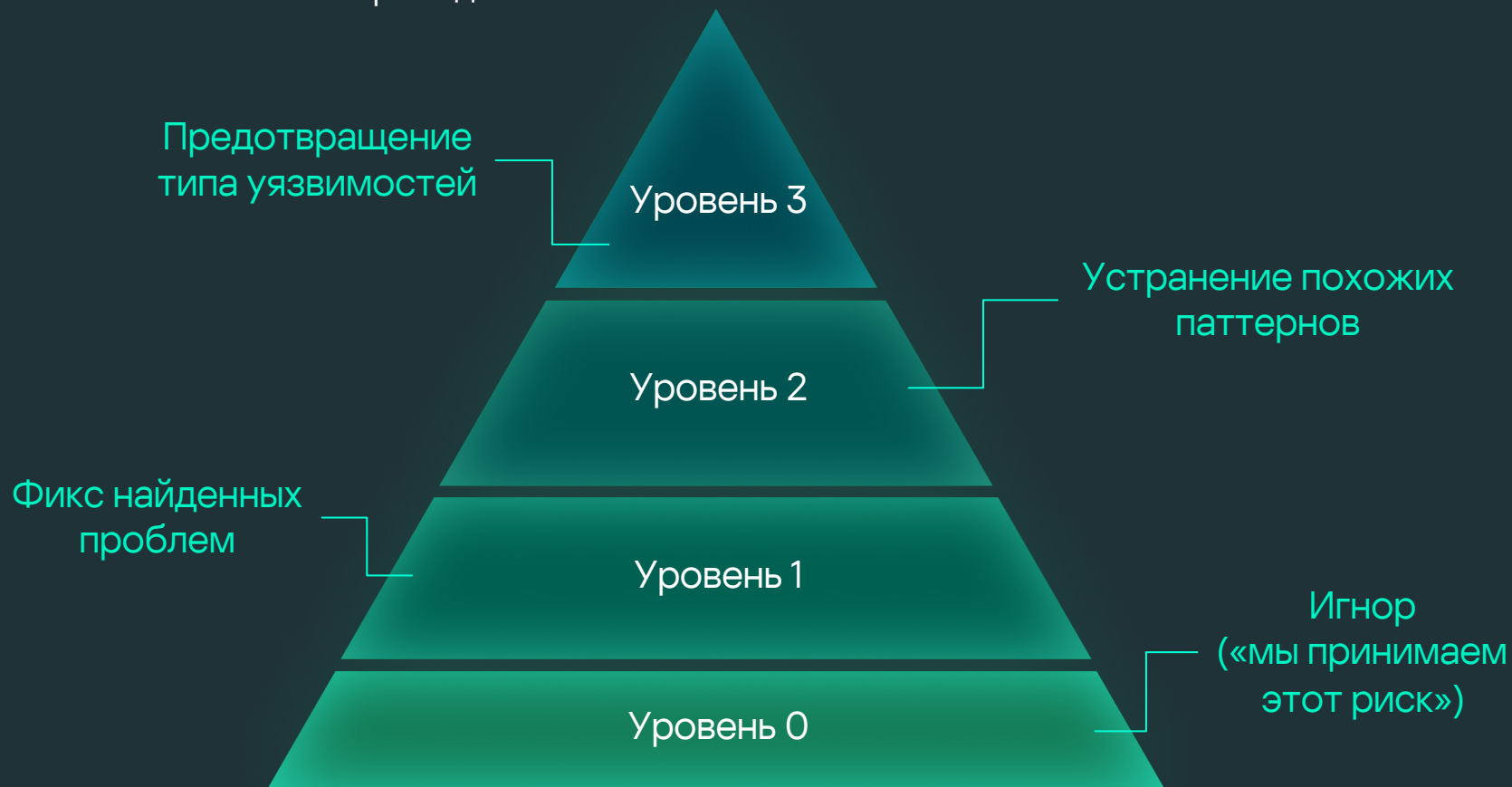
Лучший гайд — это тот, который используют разработчики и который они сами хотят поддерживать в актуальном состоянии

(с) капитан очевидность

Задача этого гайда - оформить в письменном виде существующие в компании лучшие практики безопасной разработки. Оригинально запрос на гайд возник от задач стандарта ISO26262, однако было решено, что гайд должен был рабочей частью процесса, а не документом для сертификации. Поэтому гайд должен включать SDL практики компании (для сертификации на ФСТЭК) и не противоречить требованиям AUTOSAR.

Гайд призван быть минималистичным и сфокусированным на практиках безопасного кодирования. Есть широкие стандарты, которые покрывают все экзотические конструкции языка. Но мы обмениваем полноту на читаемость. Пусть гайд покрывает самый минимум, но тот минимум, который действительно релевантен для нашего проекта и несоблюдение которого вредит надежности и безопасности.

22 пункта для C, 22 для C++





22

пункта в гайде для C

26

правил статического
анализатора для C.

22

для C++

46

правил для C++.

Спасибо!

А мы — молодцы 😊

Анна Мелехова

Security Architect

Anna.Melekhova
@kaspersky.com



KasperskyOS