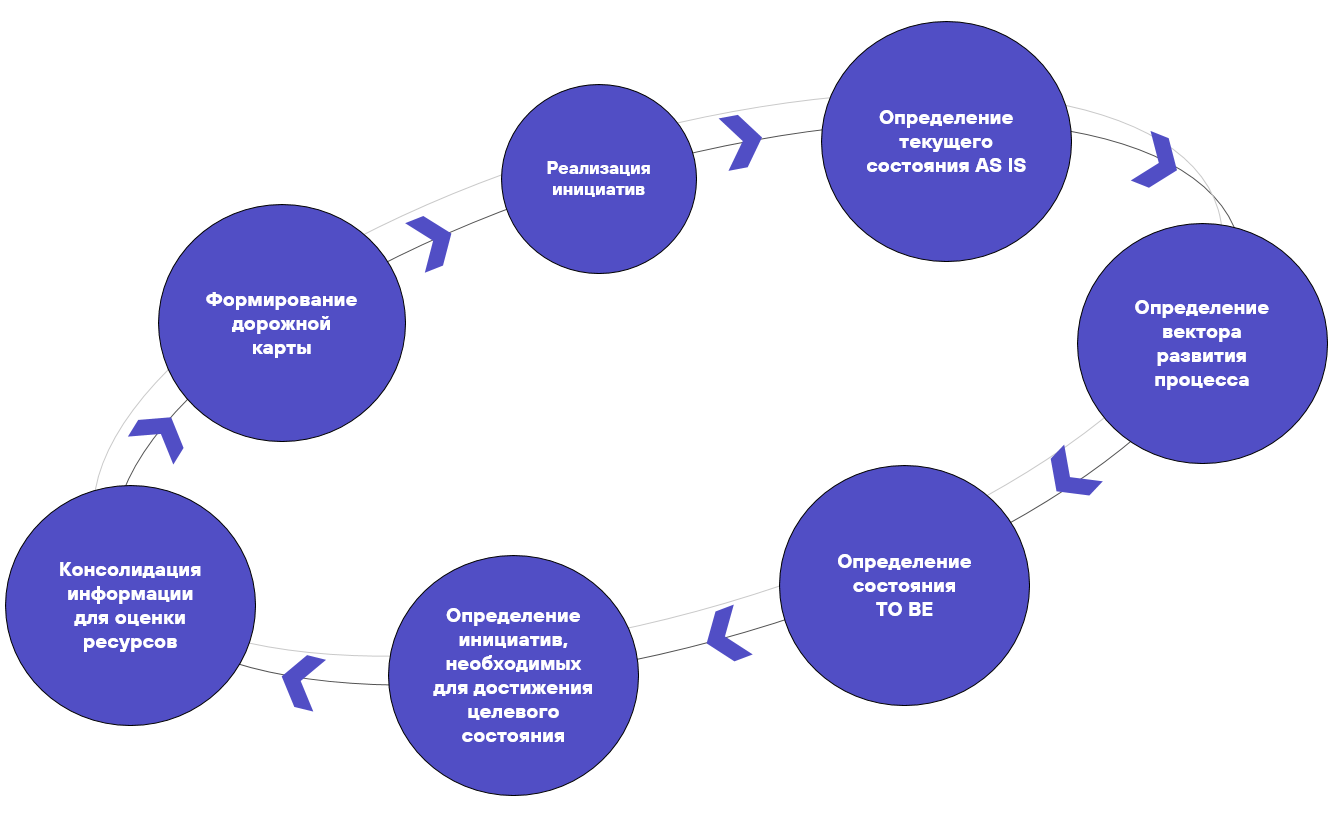
# Framework безопасной разработки DAF

## Общее описание

При внедрении практик и процесса безопасной разработки ПО первый и самый главный вопрос, с которым сталкиваются компании – **«С чего начать?».** Для того, чтобы ответить на этот вопрос, необходимо преодолеть следующий путь:

1. Определить, где вы находитесь сейчас;
2. Определить, в какую сторону хотите развиваться;
3. Зафиксировать целевое состояние;
4. Определить инициативы, реализация которых поможет достичь целевого состояния;
5. Проанализировать всю собранную информацию для оценки необходимых ресурсов;
6. Сформировать дорожную карту реализации инициатив;
7. Реализовать инициативы.



Для того, чтобы минимизировать ресурсы на прохождение этого пути и упростить подход к формированию дальнейшей стратегии развития процесса безопасной разработки ПО в компании, нашей командой было принято решение разработать собственный фреймворк.

DevSecOps Assessment Framework (DAF) – это фреймворк оценки зрелости процесса безопасной разработки ПО. В данном случае под словом фреймворк мы понимаем набор инструментов, принципов, правил, инструментов, руководств и процессов, которые помогают создавать безопасное ПО.

Основные задачи, которые ставились при создании фреймворка:

* сформировать набор практик, который будет охватывать весь процесс безопасной разработки с детализацией;
* сформировать набор практик, которые будут актуальны только для рынка РФ;
* сделать максимально простой процесс оценки зрелости;
* сформировать подход к определению текущего уровня зрелости организации и практик, которые к этому уровню относятся;
* создать визуализацию результатов для удобства восприятия результатов;
* сформировать инкрементальный подход к уровням зрелости.

DAF состоит из трех основных компонентов:

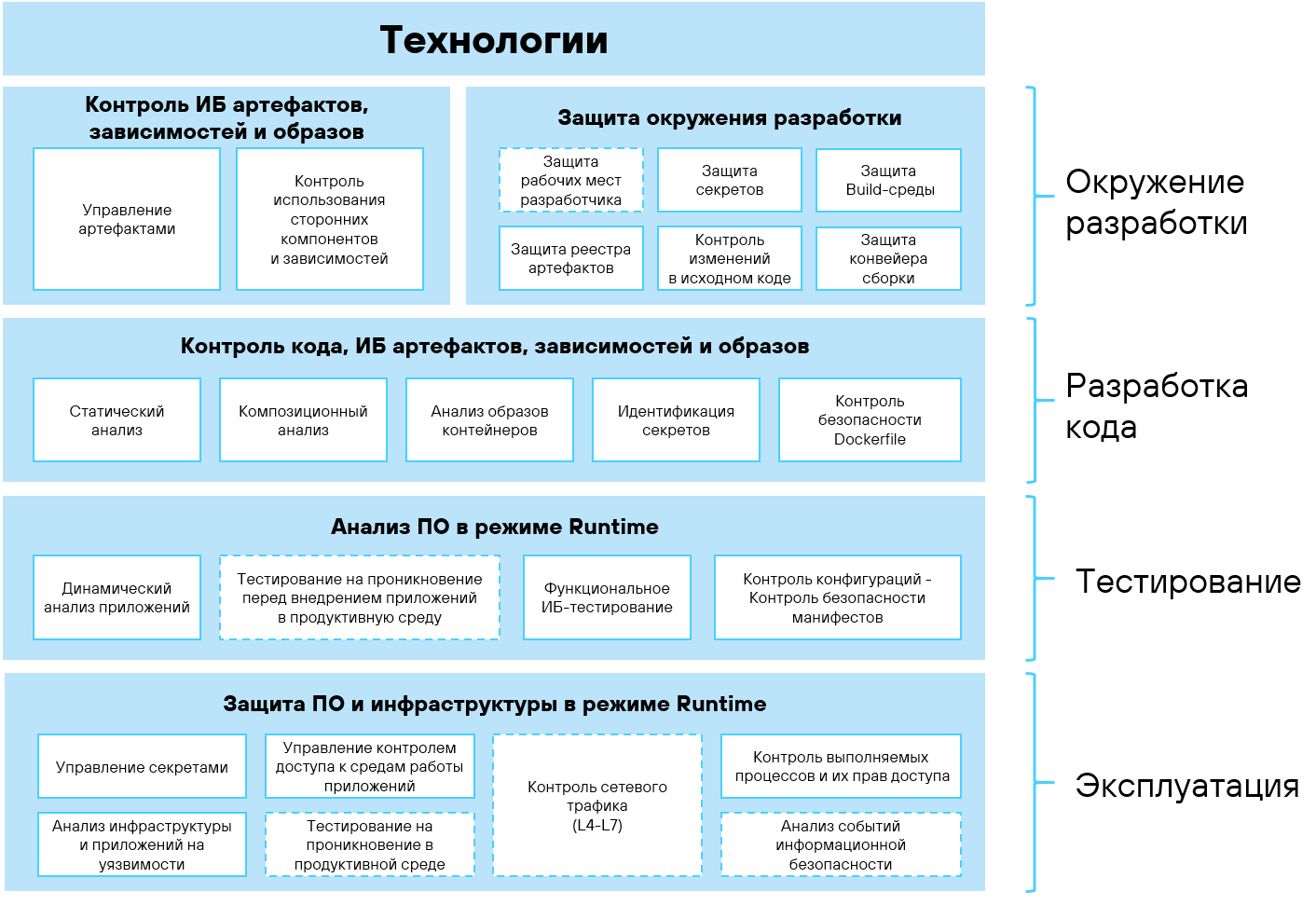


Ниже мы расскажем про них более подробно

## Пиратская карта

Пиратская карта – это верхнеуровневый взгляд на весь фреймворк. Она включает в себя все аспекты процесса безопасной разработки с этапа планирования до перевода ПО в промышленную эксплуатацию. Карта делится на два блока: Технологии и Процессы.

Блок Технологий включает в себя наборы практик, которые делятся по средам разработки.





## Таблица оценки и тепловая матрица



Таблица оценки содержит различные параметры и метрики, которые позволят компании определить уровень зрелости для конкретного поддомена безопасной разработки (процессов или инструментов). Для определения соответствия поддомена конкретному уровню, необходимо выполнение одного или нескольких практик, определенных для данного уровня.

Тепловая матрица показывает степень выполнения практик в рамках определенного уровня в процентах. Например, если для полного выполнения уровня, требуется соблюдение 4 условий, а выполняется только 2 – в таблицу заносится значение 50% для данного уровня.

Основная цель таблицы оценки и тепловой матрицы – визуализация

Оценка развития каждой из практик делится на следующие уровни:

**Уровень 0: Uninitiated**

На этом уровне компания не имеет никаких формализованных процессов или инструментов. Практики могут использоваться случайным образом по инициативе отдельных работников.

**Уровень 1: Beginners**

На этом уровне зрелости практик .

**Уровень 2: Intermediate**

Процессы на этом уровне становятся повторяемыми и управляемыми. Компания начинает применять методики для планирования, выполнения и отслеживания активностей. Однако эти методики могут быть не всегда последовательными или полностью документированными.

**Уровень 3: Advanced**

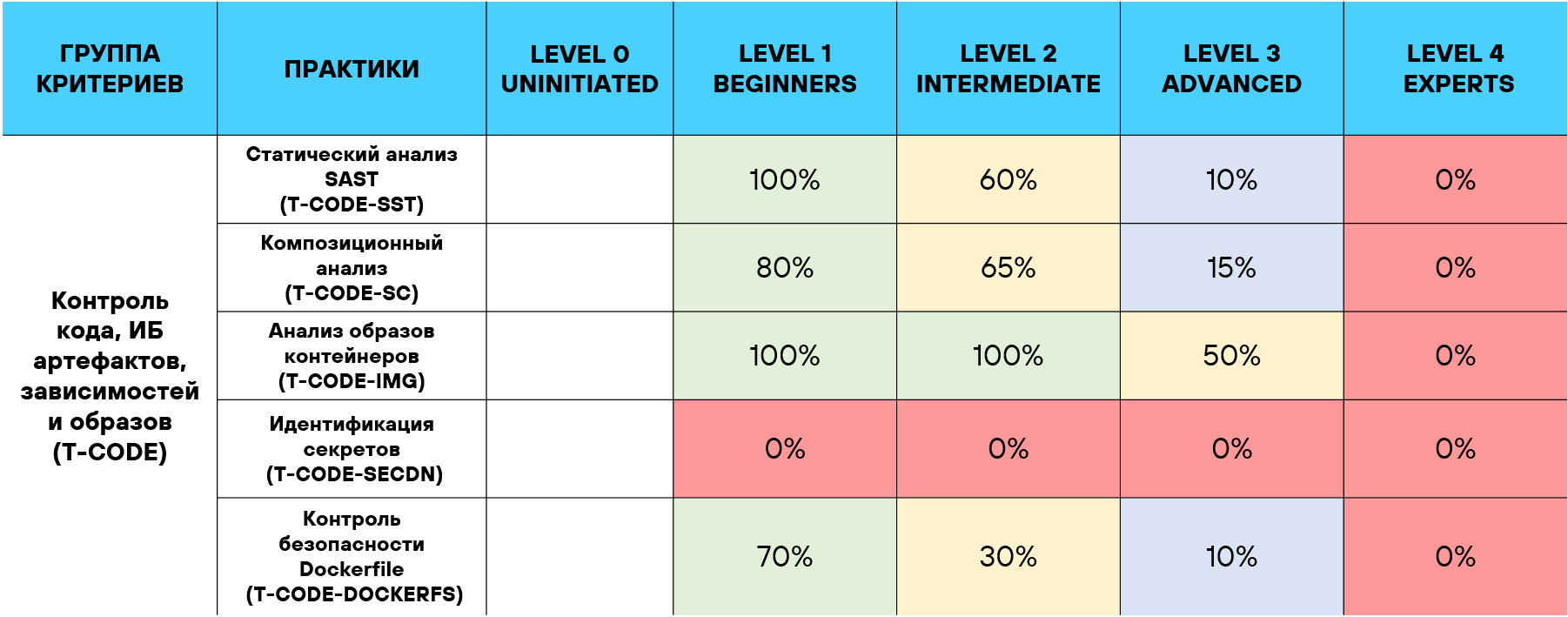
Процессы становятся более структурированными и документированными. Компания применяет стандартные процедуры, которые поддерживаются набором инструментов и обучения. Этот уровень обычно включает в себя систематическую оценку эффективности процессов.

**Уровень 4: Experts**

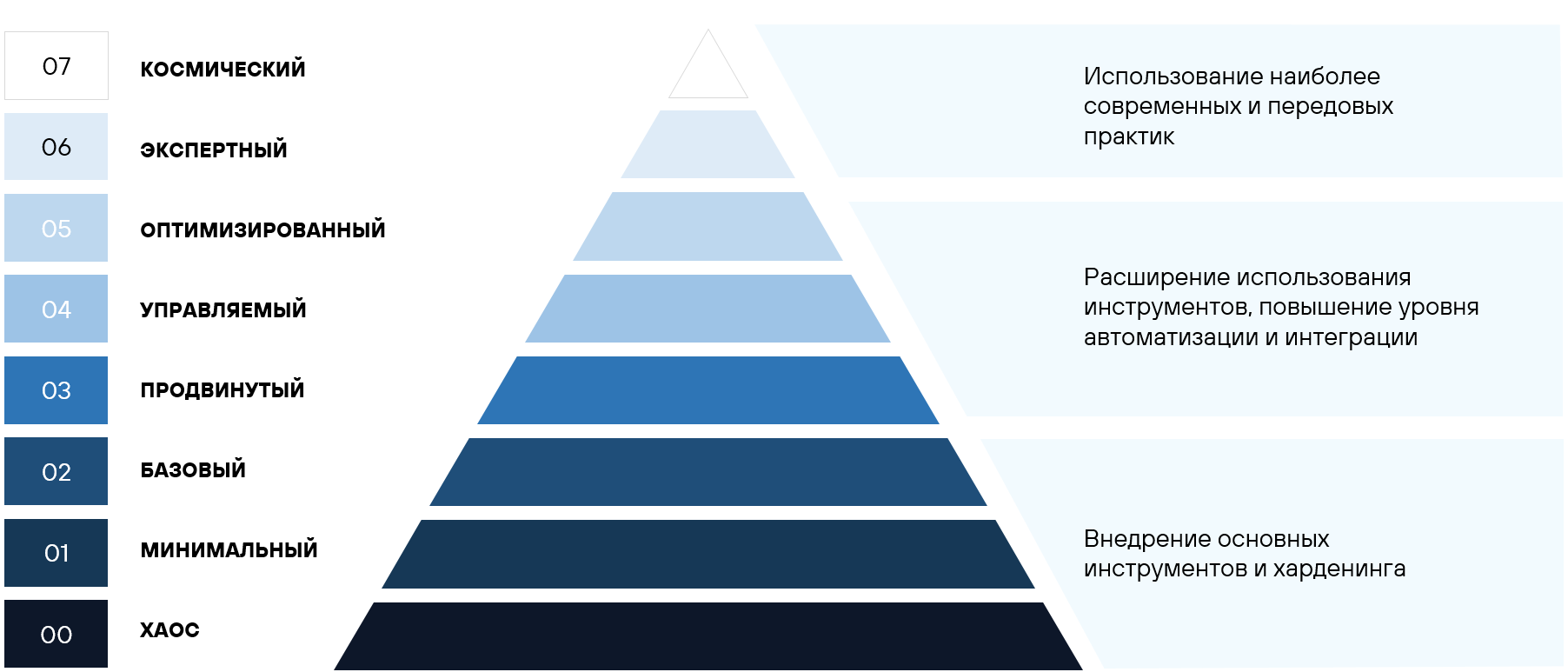
На этом уровне компания применяет метрики для измерения эффективности процессов и их улучшения. Процессы анализируются и оптимизируются на основе этих метрик. Уровень предсказуемости и эффективности значительно увеличивается.

Уровень 5: Наивысшая степень развития

Это уровень непрерывного улучшения. Компания не только применяет метрики, но и систематически анализирует результаты для последующего улучшения процессов. Подход к управлению и улучшению является принципиальным и интегрированным в корпоративную культуру.



## Пирамида зрелости



Пирамида зрелости безопасной разработки представляет собой иерархическую структуру, отражающую прогрессивное внедрение практик и методологий безопасности в процесс разработки программного обеспечения. Она служит руководством для компаний, показывая, какие практики и технологии следует внедрять на различных этапах развития программного обеспечения, чтобы повысить его безопасность.

**Зачем она нужна:**

* **Понимание текущего положения:** Организации могут определить, на каком уровне безопасности они находятся в данный момент, а также увидеть, какие улучшения они уже достигли.
* **Планирование:** Пирамида позволяет компаниям планировать следующие шаги в улучшении безопасности их процессов разработки.
* **Мотивация:** Отображая прогресс в виде пирамиды, команды могут видеть, как они двигаются вверх, что может служить мотивацией для дальнейших улучшений.
* **Стандартизация:** Пирамида зрелости может служить основой для внутренних стандартов и правил, устанавливаемых компаниями для повышения качества и безопасности разработки.

В целом, пирамида зрелости безопасной разработки служит инструментом для оценки, планирования и улучшения безопасности программного обеспечения на протяжении всего его жизненного цикла.

Пирамида зрелости безопасной разработки состоит из 3 основных частей:

* Уровни 0 - 2. В рамках данных уровней основная цель компании – добиться внедрения основных инструментов и процессов, используемых при безопасной разработки и обеспечить базового уровня их покрытия
* Уровни 3 - 5. В рамках данных уровней происходит расширение зоны покрытия использования инструментов до максимального, развитие основных процессов, а также дополнительное внедрение инструментов безопасной разработки, которые не входят в базовый комплект
* Уровни 6 - 7. Когда внедрены все основные инструменты и процессы безопасной разработки, компания занимается внедрением наиболее современных, сложных и труд затратных практик.

## Материалы, используемые при создании

Для создания фреймворка были проанализированы и использованы следующие материалы:

* Международные лучшие практики:
  + The Building Security In Maturity Model (BSIMM);
  + OWASP Software Assurance Maturity Model (OWASP SAMM);
  + DevSecOps Maturity Model (DSOMM);
  + Microsoft Security Development Lifecycle (SDL);
* Практики от Center for Internet Security (CIS):
  + CIS Software Supply Chain Security Guide;
  + CIS GitHub benchmark.
* Best practices от вендоров (Aqua, GitGuardian и другие)
* Наш опыт, а также наших заказчиков.

