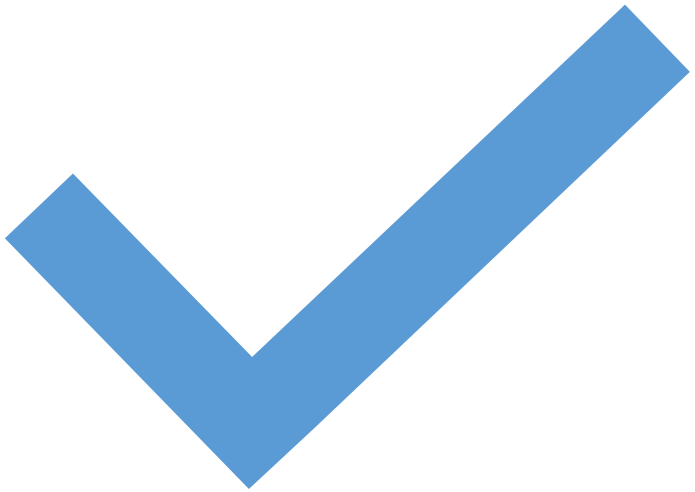


Развитие практик стандартизации Secure SDL: от международных лучших практик к «импортозамещенным» требованиям

Рустам Гусейнов, Председатель кооператива «РАД КОП»

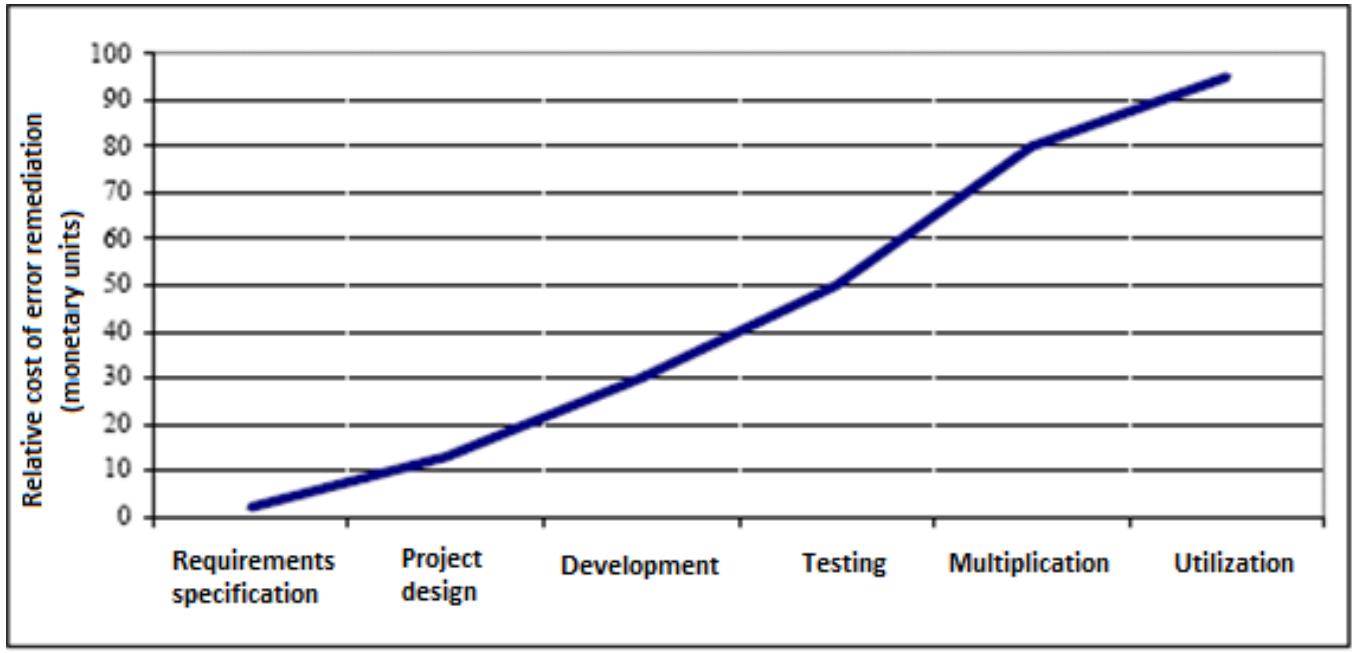
Кто я?

RAD COP

Гусейнов Рустам Мехтиевич

Консультант в области информационной безопасности, сооснователь производственного кооператива РАД КОП, https://radcop.online/

- Комплексный анализ защищенности компаний, включая технические и правовые аспекты защиты информации (в том числе пентесты и аудиты исходного кода);
- Оценка соответствия требованиям законодательства в области безопасности персональных данных и выстраивание системы защиты «под ключ» (включая разработку пакета внутренней нормативной документации и внедрение средств защиты информации);
- Аутсорсинг информационной безопасности для МСП.



Источник: Cost of an error correction in the case of a software product Source: Parker, G.W., Costurile calităţii, Editura Codecs, Bucureşti, 1998

RAD COP

NEW RESEARCH: THE COST OF POOR SOFTWARE QUALITY IN THE US: A 2022 REPORT.

Our 2022 update report estimates that the cost of poor software quality in the US has grown to at least $2.41 trillion, but not in similar proportions as seen in 2020. The accumulated software Technical Debt (TD) has grown to ~$1.52 trillion.

The key US economic conditions that frame the context for this biennial report are:

- A projected GDP for 2022 of $23.35 trillion, a roughly 2% rise since 2020
- An inflation rate of 15% over the two-year period
- A small 4% growth in the IT labor base over those 2 years to $1.51 trillion
- The number of unfilled IT jobs sits at ~300,000 as of the end of August

The 3 main problem areas that we focus on in this year's report are:

- Cybercrime losses due to existing software vulnerabilities jumped way up
- Software supply chain problems with underlying 3rd party components (especially Open Source Software, aka OSS) have risen significantly
- The growing impact of Technical Debt (TD) has become the biggest obstacle to making any changes to existing code bases

In this 2022 report we turn our attention to recent developments and emerging solutions to help improve the poor software quality situation as it now exists and stabilize/reduce the growth rate of CPSQ in the near future.

Источник: https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/

RAD COP

Направления требований

Требования к приложению

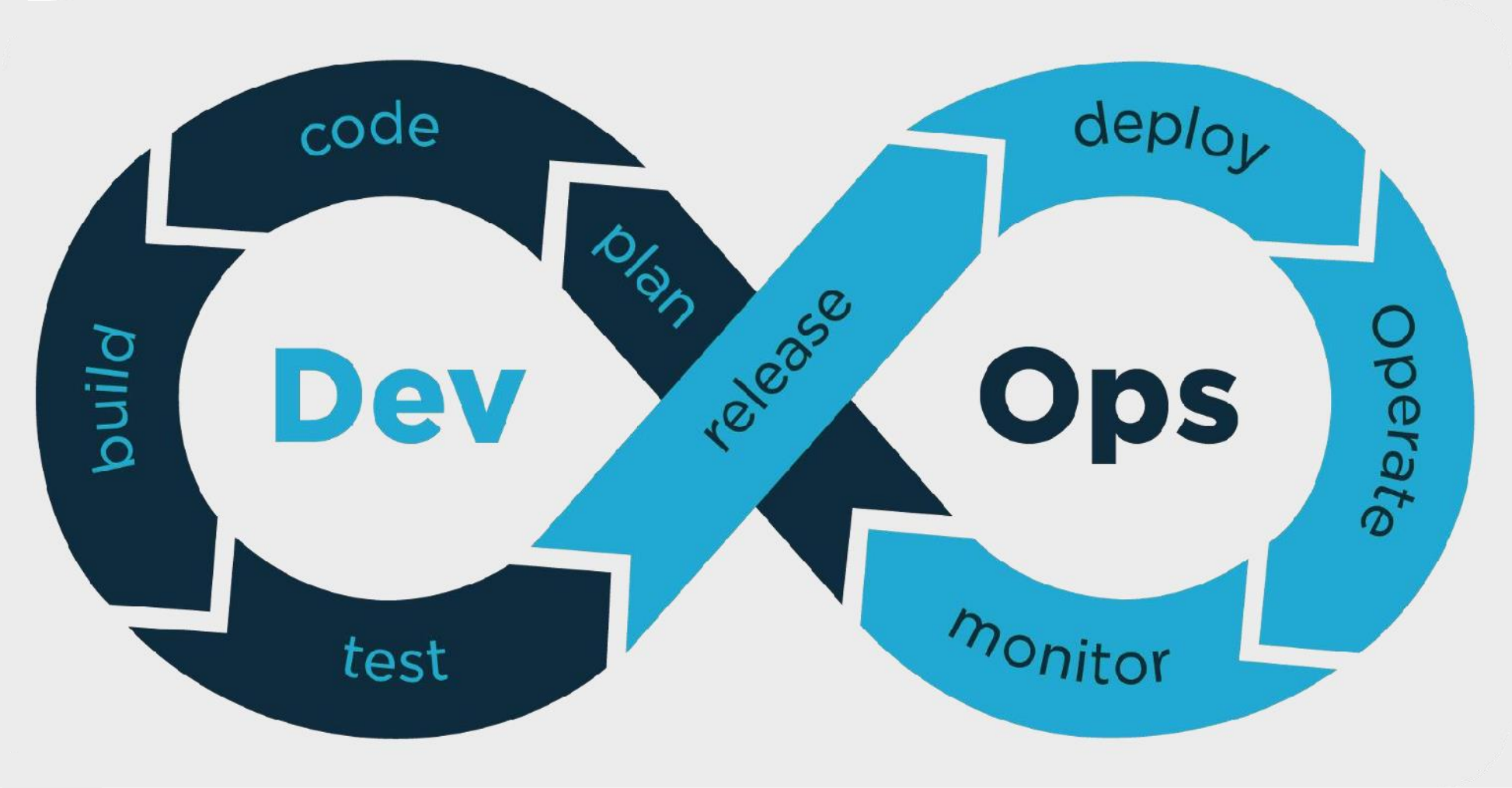
Требования к жизненному циклу

Люди
Процессы
Технологии

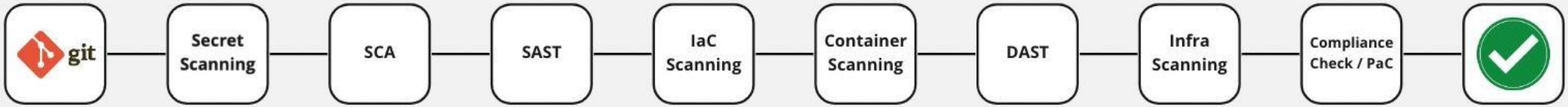
Некоторые исторические тезисы

- Цикличность «глобализации» и «регионализации»;
- Приход к Common Criteria (ИСО/МЭК 15408) и отход от них в пользу собственных стандартов и требований к определенным классам СрЗИ или ТУ на ПАК;
- Возникновение большого числа нишевых, отраслевых стандартов, рекомендаций и т.д. (PCI DSS, РС БР, ФСТЭК России, NIST.....);
- Появление процессных подходов, адекватных парадигме Agile и привязанных к уровням зрелости (OWASP, CIS и т.д.).

Банальности о DevOps / DevSecOps



Что должно получиться?



План на все случаи жизни

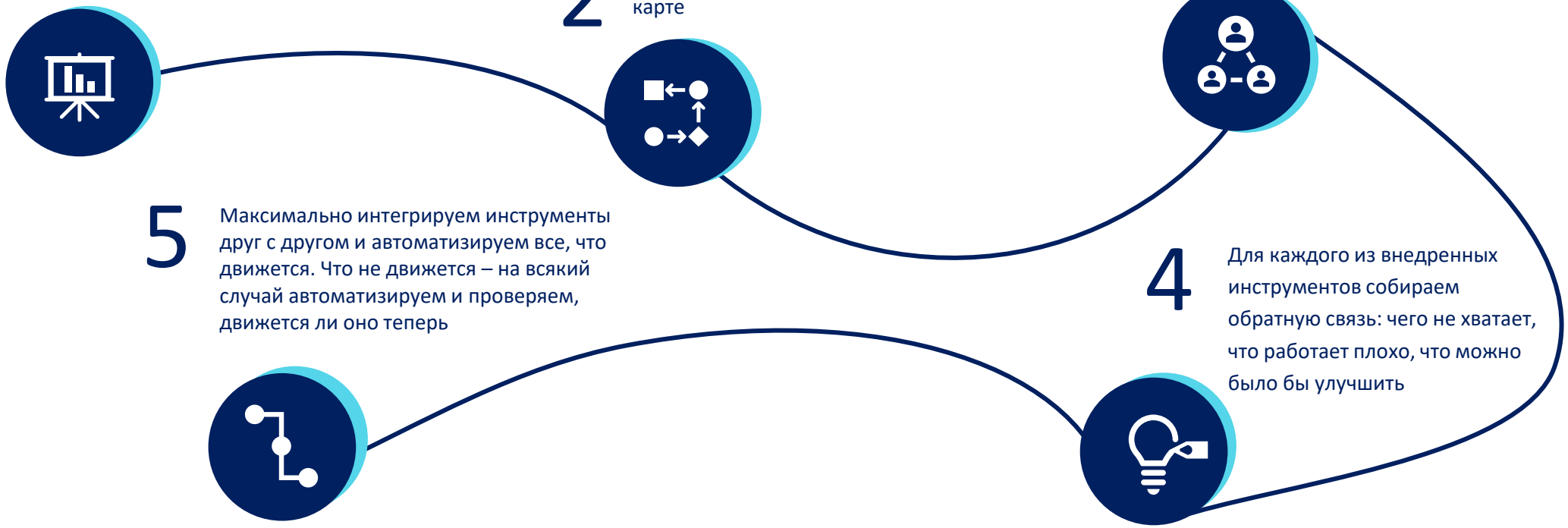
1 Глубоко анализируем BSIMM/DSOMM, строим дорожную карту, определяем метрики

2 Двигаемся по дорожной карте

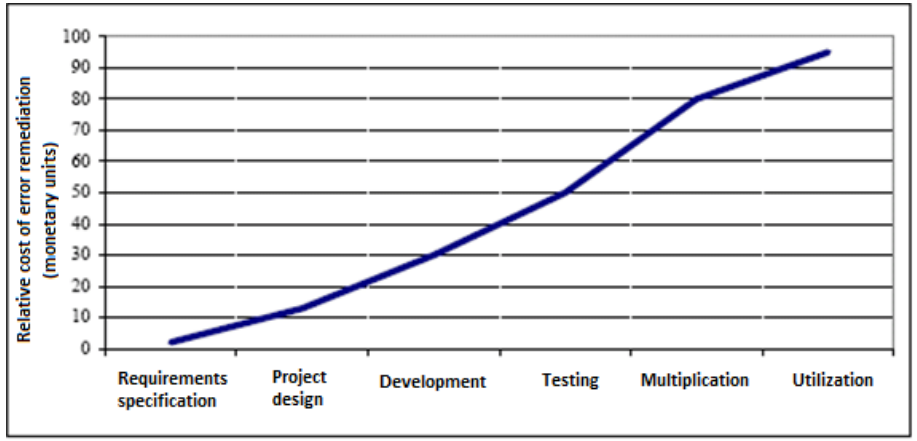
3 Выстраиваем процесс взаимодействия с командами разработки и поддержки

4 Для каждого из внедренных инструментов собираем обратную связь: чего не хватает, что работает плохо, что можно было бы улучшить

5 Максимально интегрируем инструменты друг с другом и автоматизируем все, что движется. Что не движется – на всякий случай автоматизируем и проверяем, движется ли оно теперь



Кто виноват и что делать?



1998 год!

NEW RESEARCH: THE COST OF POOR SOFTWARE QUALITY IN THE US: A 2022 REPORT.

Our 2022 update report estimates that the cost of poor software quality in the US has grown to at least $2.41 trillion, but not in similar proportions as seen in 2020. The accumulated software Technical Debt (TD) has grown to ~$1.52 trillion.

The key US economic conditions that frame the context for this biennial report are:

- A projected GDP for 2022 of $23.35 trillion, a roughly 2% rise since 2020
- An inflation rate of 15% over the two-year period
- A small 4% growth in the IT labor base over those 2 years to $1.51 trillion
- The number of unfilled IT jobs sits at ~300,000 as of the end of August

The 3 main problem areas that we focus on in this year's report are:

- Cybercrime losses due to existing software vulnerabilities jumped way up
- Software supply chain problems with underlying 3rd party components (especially Open Source Software, aka OSS) have risen significantly
- The growing impact of Technical Debt (TD) has become the biggest obstacle to making any changes to existing code bases

In this 2022 report we turn our attention to recent developments and emerging solutions to help improve the poor software quality situation as it now exists and stabilize/reduce the growth rate of CPSQ in the near future.

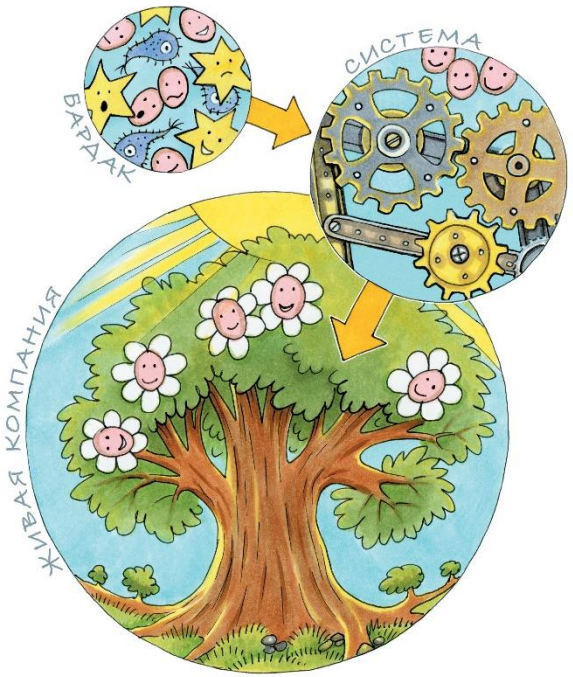
2022 год!

Михаил Рыбаков

Бизнес-процессы:

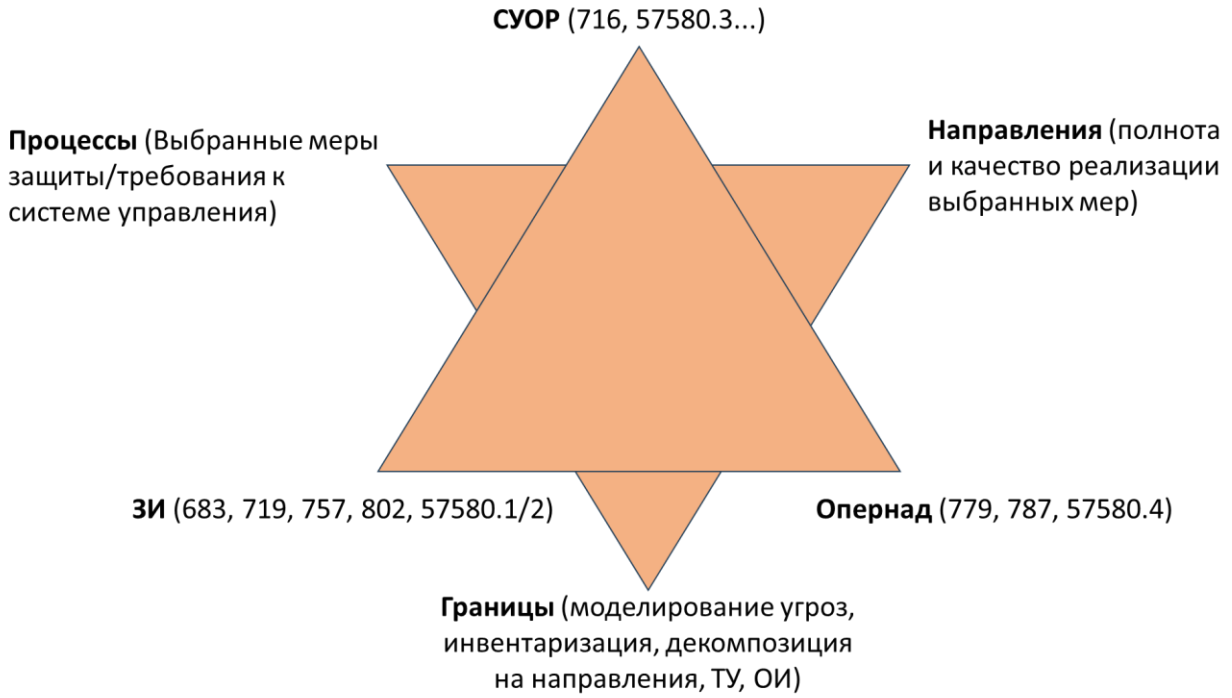
как их описать, отладить и внедрить

ПРАКТИКУМ

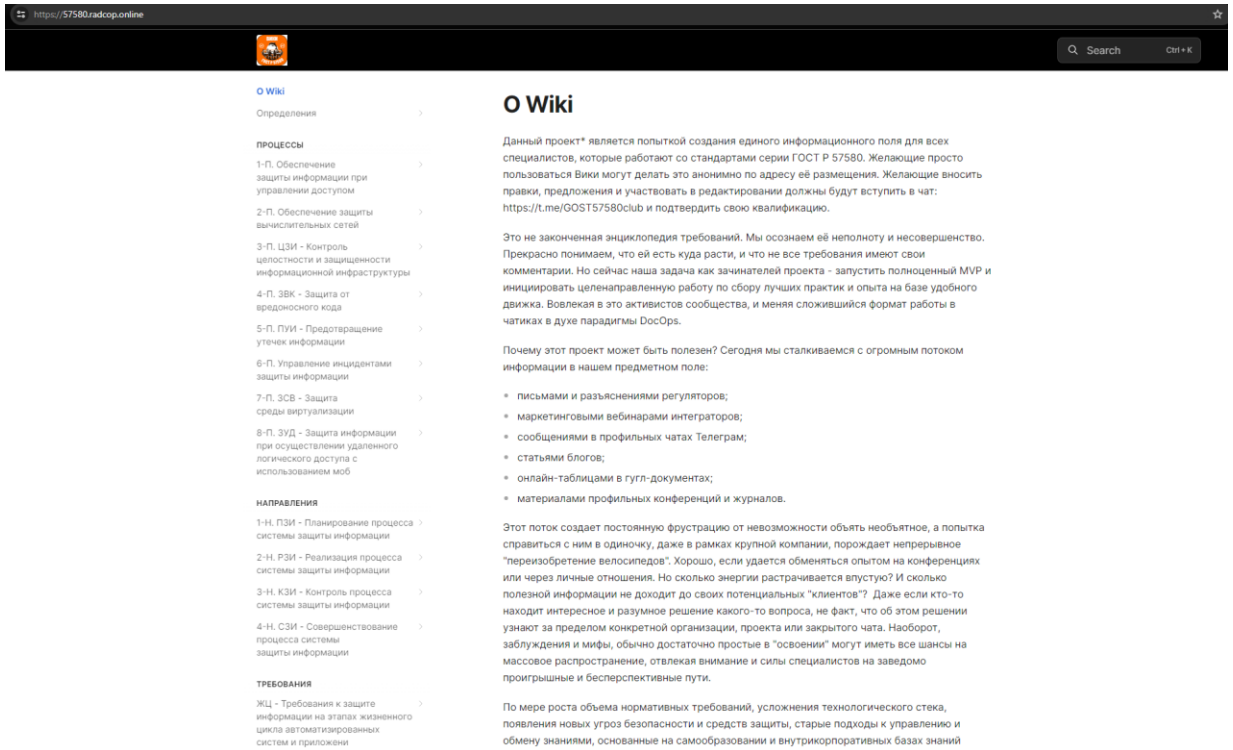


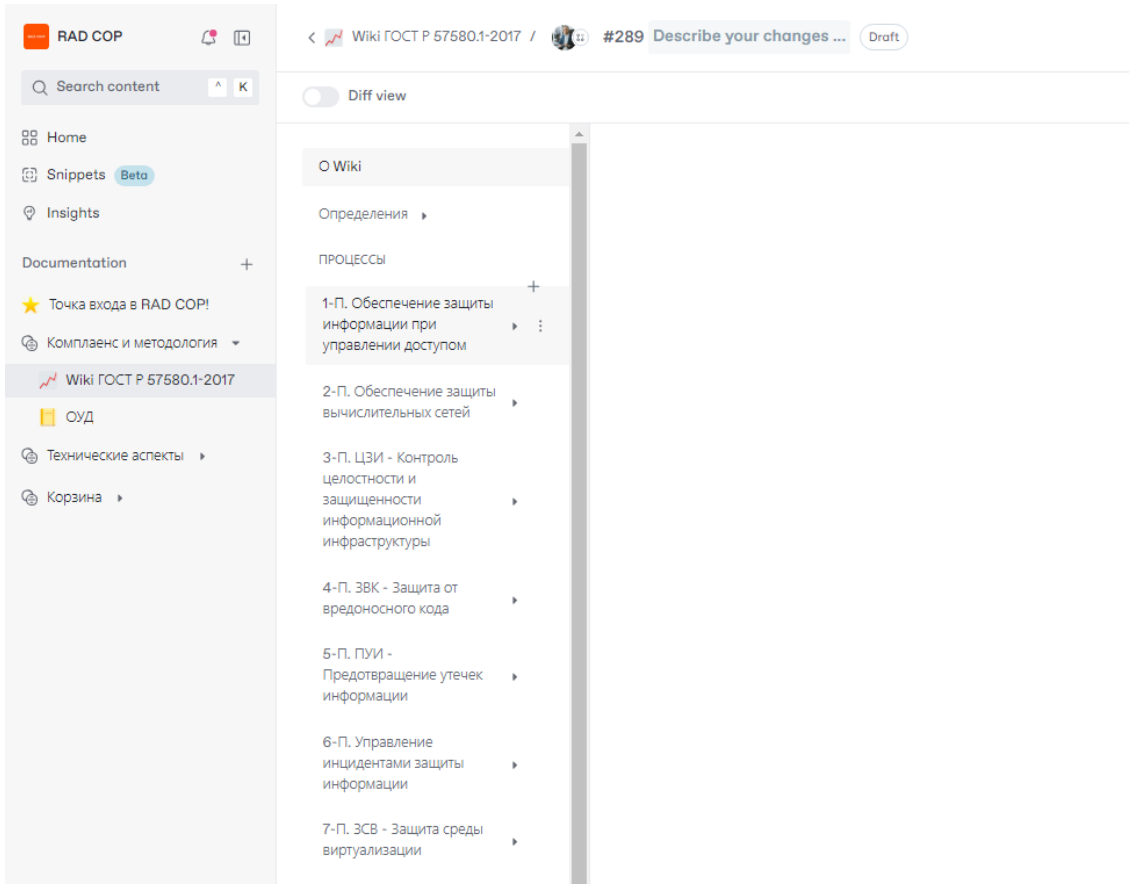
СЕРИЯ «ПОРЯДОК В БИЗНЕСЕ»

Ситуационный подход к ИБ



Ценность сообщества и обмен адаптированными лучшими практиками





Некий план и выводы

1. Начать работать с тем, что:

   А. обязательно для вас;

   Б. вам известно/может быть освоено с учетом ресурсов.

2. На берегу решить, как практика SecureSDL интегрирована в систему управления ИБ, а система управления ИБ интегрирована в систему менеджмента компании;

3. Провести GAP-анализ по выбранному набору требований и разработать актуальный именно для вас сценарий базового внедрения (приоритеты, ресурсы, ответственные);

4. Избежать ошибки «технократа» (слепой веры в технологии и автоматизацию, которая всех спасет сама по себе);

…… (итерировать, итерировать, итерировать)

N. Продолжать итерировать, сохраняя комплексное видение ситуации и помня о ситуационных моделях управления, потому что у них нетконечной точки эволюции, и их смысл в бесконечной адаптации.

inbox@radcop.online