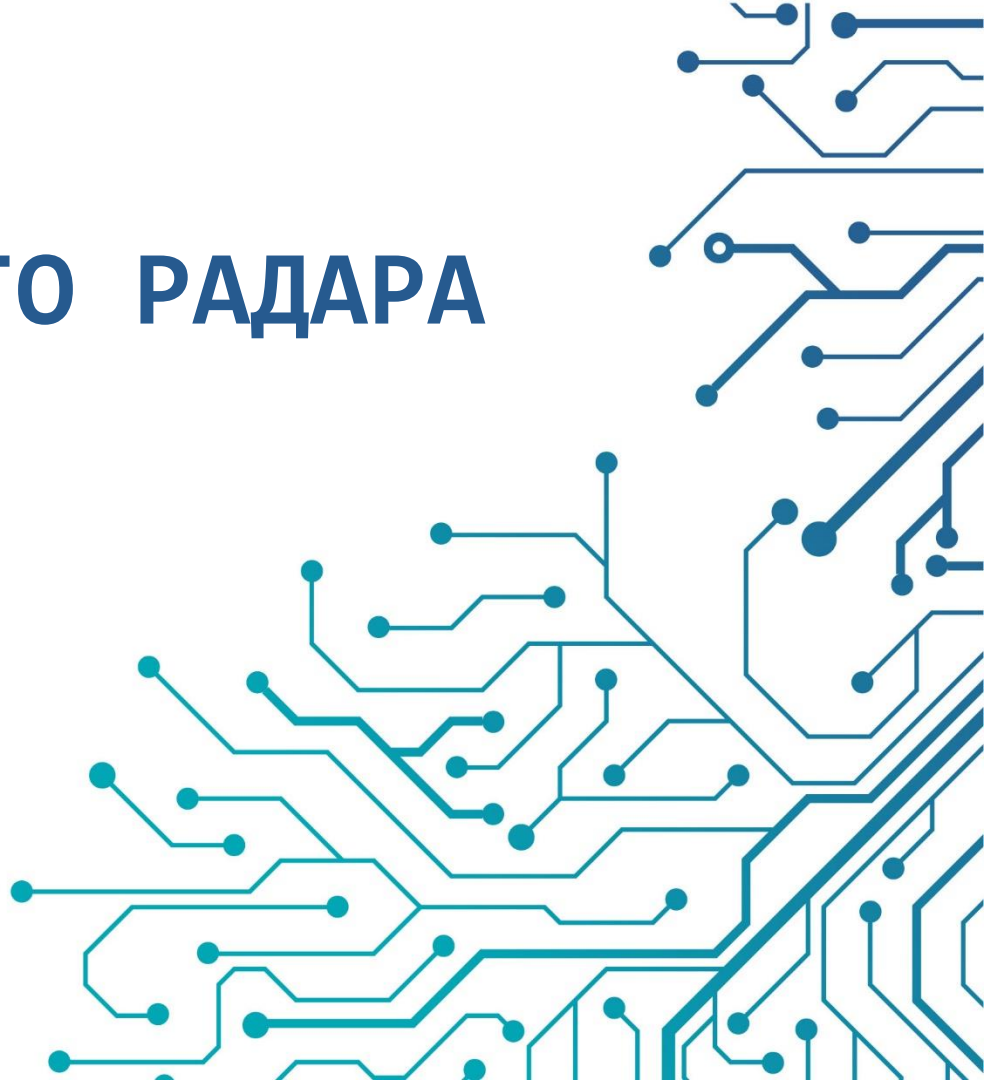
Опыт внедрения
ТЕХНОЛОГИЧЕСКОГО РАДАРА

Виталий Минко



infotecs
ARCHDAYS
2022

О себе

Виталий Минко

Руководитель архитектурного направления

Отдел Аналитики и Архитектуры

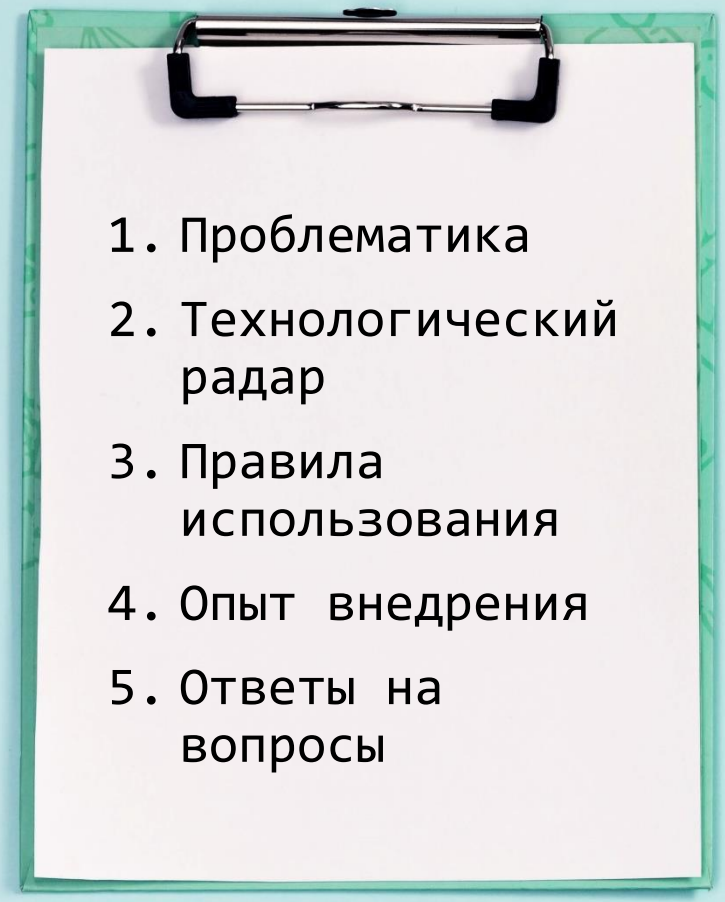
infotecs

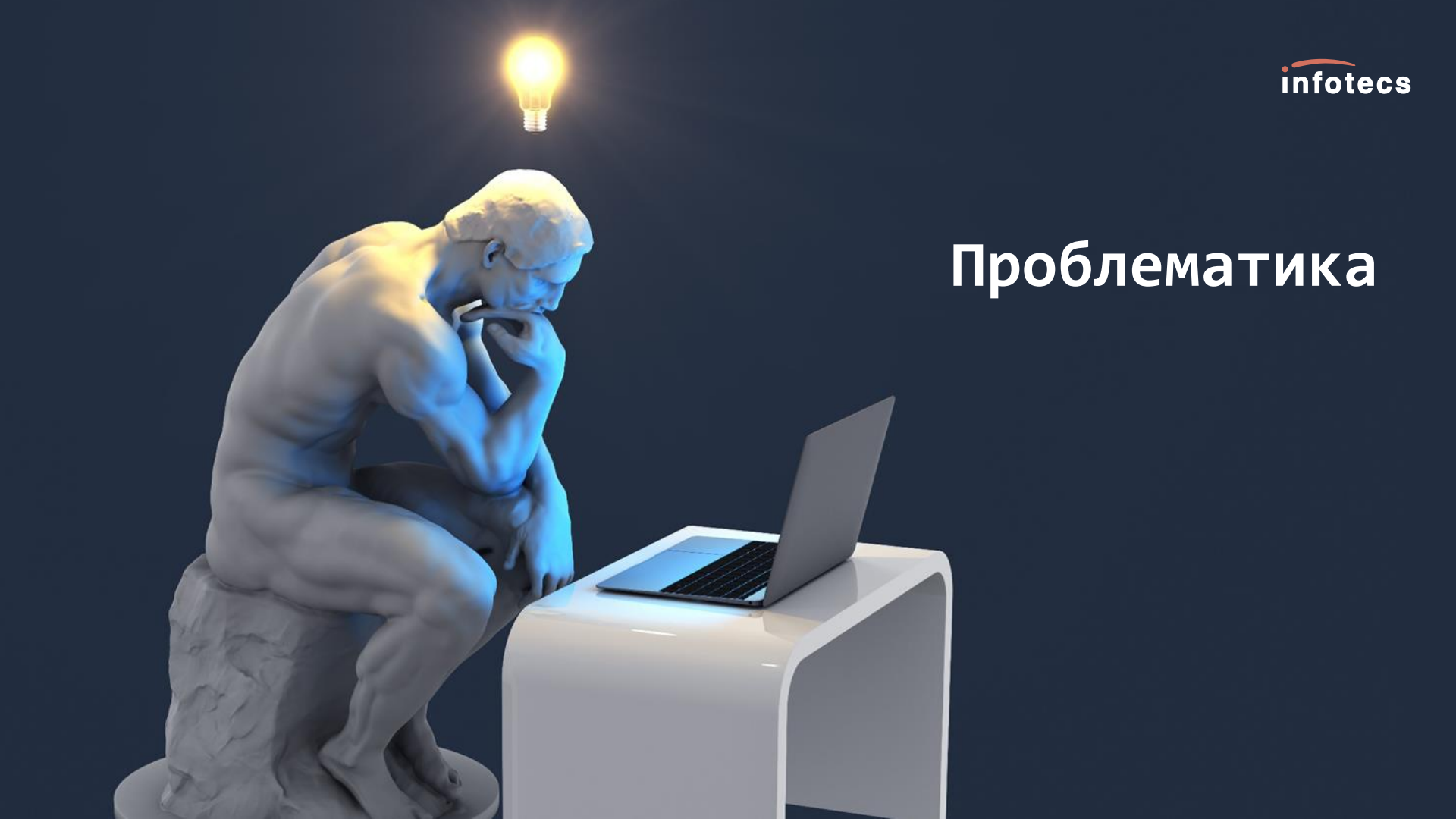
The Open Group Open Certified

TOGAF® 9

План доклада

1. Проблематика
2. Технологический радар
3. Правила использования
4. Опыт внедрения
5. Ответы на вопросы





Проблематика

О компании

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3692

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
26 января 2017 г.

Выдан: 26 января 2017 г. Переоформлен: 20 июня 2022 г.
Действителен до: 26 января 2020 г.
Срок действия продлен до: 26 января 2025 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «ViPNet Coordinator HW 4»**, разработанный АО «ИнфоТеКС» и производимый АО «ИнфоТеКС» и ООО «Инфотекс», является межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвёртого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа Б четвёртого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016) при выполнении указаний по эксплуатации, приведённых в формуляре ФРКЕ.00130-03 30 01 ФО.

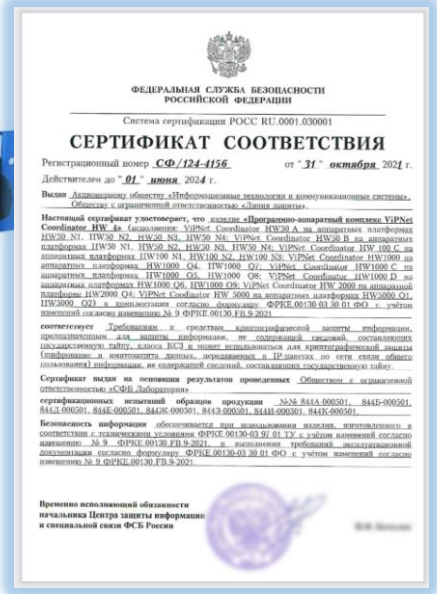
Действие настоящего сертификата не распространяется на встроенные модули криптографической защиты информации.

Сертификат выдан на основании технического заключения от 22.12.2016, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.БЭ00), экспертного заключения от 28.12.2016, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 07.02.2020, 29.12.2020 и 25.05.2022, оформленных испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 08.02.2021, оформленного органом по сертификации АО «Лаборатория ППШ».

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4156 от "31" октября 2021 г.

Действителен до "01" июня 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы», Обществу с ограниченной ответственностью «Линия защиты».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный комплекс ViPNet Coordinator HW 4»** (исполнения: ViPNet Coordinator HW50 A на аппаратных платформах HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW50 B на аппаратных платформах HW50 N1, HW50 N2, HW50 N3, HW50 N4; ViPNet Coordinator HW 100 C на аппаратных платформах HW100 N1, HW100 N2, HW100 N3; ViPNet Coordinator HW1000 на аппаратных платформах HW1000 O4, HW1000 O7; ViPNet Coordinator HW1000 C на аппаратных платформах HW1000 O5, HW1000 O8; ViPNet Coordinator HW1000 D на аппаратных платформах HW1000 O6, HW1000 O9; ViPNet Coordinator HW 2000 на аппаратной платформе HW2000 O4; ViPNet Coordinator HW 5000 на аппаратных платформах HW5000 O1, HW5000 O2) в комплектации согласно формуляру ФРКЕ.00130-03 30 01 ФО с учётом изменений согласно извещению № 9 ФРКЕ.00130.FB.9-2021

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и может использоваться для криптографической защиты (шифрование и контроль целост. передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лабораторией»

сертификационных испытаний образцов продукции №№ 844А-000501, 844Э-000501, 844Д-000501, 844Е-000501, 844Ж-000501, 844З-000501, 844И-000501, 844К-000501

Безопасность информации обеспечивается при использовании изделия, изготовленного в соответствии с техническими условиями ФРКЕ.00130-03 97 01 ТУ, с учётом изменений согласно извещению № 9 ФРКЕ.00130.FB.9-2021, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00130-03 30 01 ФО с учётом изменений согласно извещению № 9 ФРКЕ.00130.FB.9-2021

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России

Проблематика выбора технологий

- Большое количество уникальных технологий увеличивает затраты на разработку общих компонентов
- Увеличиваются затраты компании на сопровождение повторной реализации решений
- Требуется тратить дополнительные ресурсы на сертификацию решения

Методика ФСТЭК ВУ и НДВ

Статический анализ проводится в отношении модулей, составляющих **поверхность атаки**, **реализующих функции безопасности**, реализующих **среду выполнения интерпретируемого кода** или кода, компилируемого в промежуточное представление.

ГОСТ Р 56939-2016

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

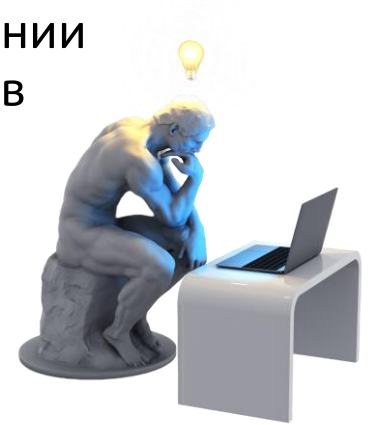
Разработчик ПО **должен идентифицировать каждое инструментальное средство**, используемое при разработке ПО, и определить его настройки (опции), применяемые при создании программы. При разработке ПО должны применять только идентифицированные инструментальные средства.

Проект ГОСТ Р

Руководство по реализации мер по разработке безопасного программного обеспечения

1) **оценить** предлагаемые к использованию при разработке **ПО компоненты, заимствованные у сторонних разработчиков** ПО, и выбрать компоненты, использование которых не приведет к ухудшению общей защищенности разрабатываемого ПО;

2) **документировать** и поддерживать в актуальном состоянии (т.е. при изменении используемых сторонних компонентов и/или их версий, соответствующую информацию следует задокументировать) **результаты анализа и обоснование выбора**



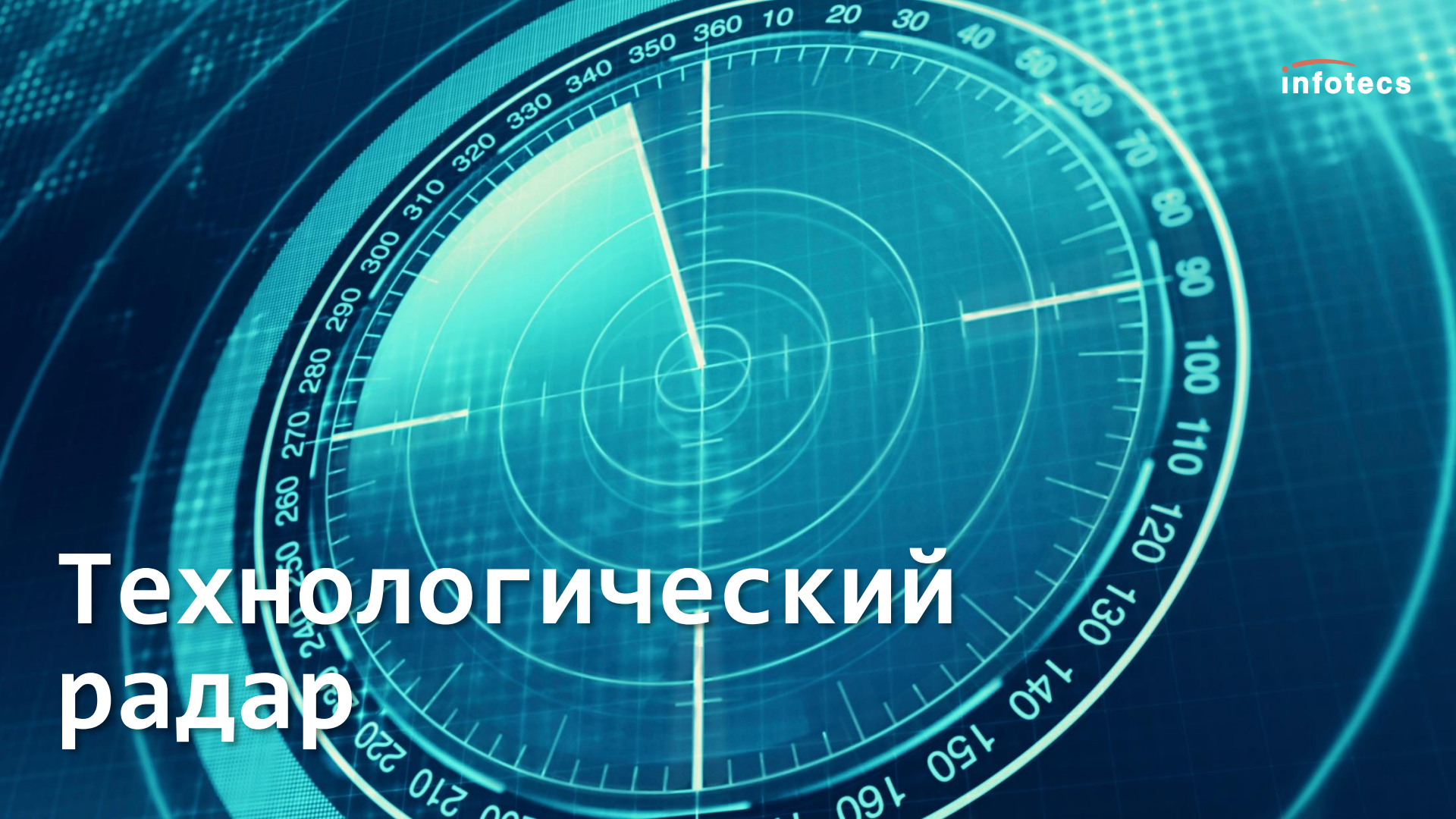
Проблематика выбора технологий

- Большое количество уникальных технологий увеличивает затраты на разработку общих компонентов
- Увеличиваются затраты компании на сопровождение повторной реализации решений
- Требуется тратить дополнительные ресурсы на сертификацию решения
- Увеличиваются издержки на выполнение практик безопасной разработки
- Большое количество уникальных технологий увеличивает проблемы с подбором кадров

Практика: Используется согласованный стек технологий

Описание: Разработка продуктов должна производиться в рамках заранее определенного и согласованного стека технологий.

В большинстве случаев следует использовать одинаковый стек технологий для решения родственных задач, поскольку это экономит ресурсы компании на дальнейшую поддержку систем.


infotecs
Технологический радар

Volume 25

Technology Radar

An opinionated guide to technology frontiers

https://www.thoughtworks.com/radar

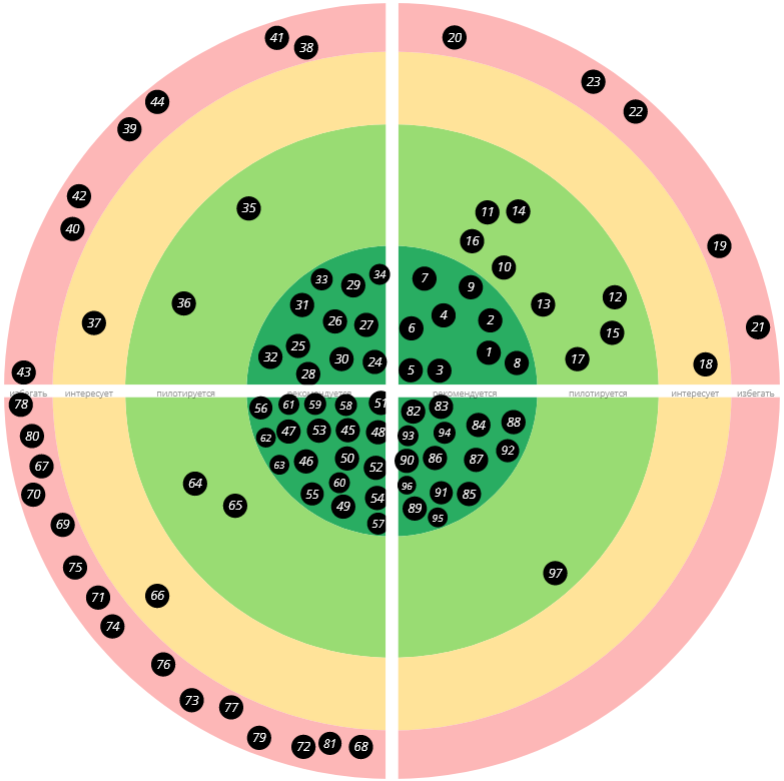
ТЕХНОЛОГИЧЕСКИЙ РАДАР

Правила использования, формирования и развития Технологического радара

Языки/фреймворки | Платформы | Утилиты/библиотеки | Практики

Print this radar | HOME

Search



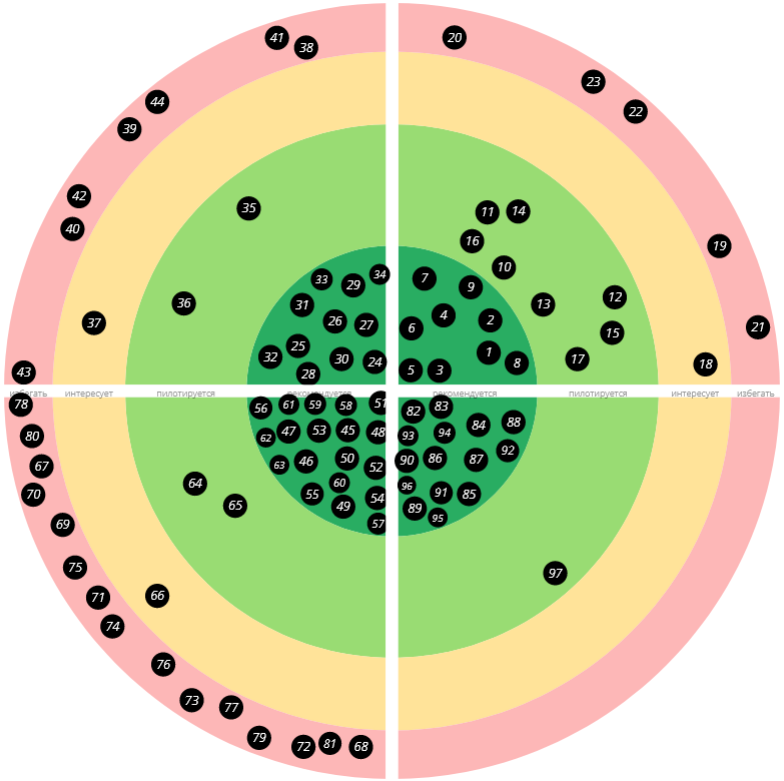
ТЕХНОЛОГИЧЕСКИЙ РАДАР

Правила использования, формирования и развития Технологического радара

Языки/фреймворки | Платформы | Утилиты/библиотеки | Практики

Print this radar | HOME

Search



ТЕХНОЛОГИЧЕСКИЙ РАДАР

Правила использования, формирования и развития Технологического радара

Языки/фреймворки | Платформы | Утилиты/библиотеки | Практики | Print this radar | HOME

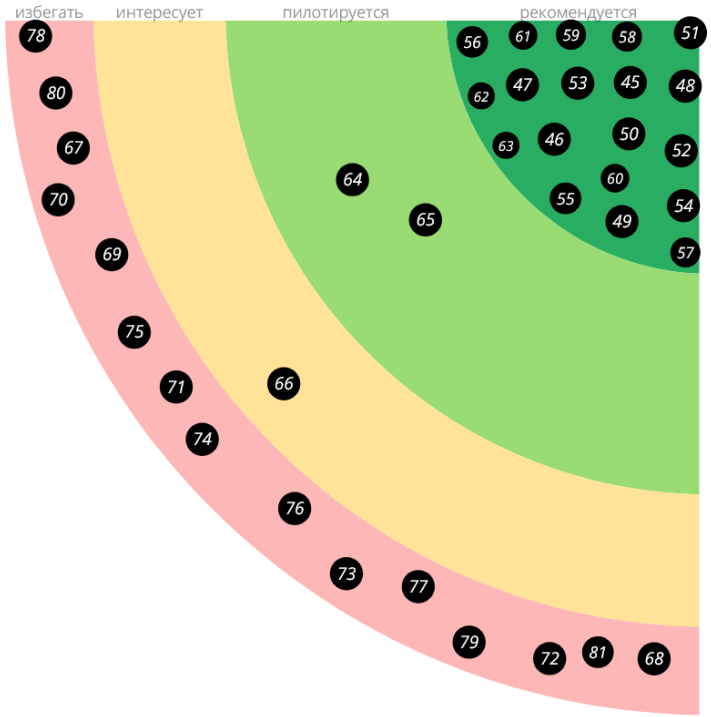
« Back to Radar home

РЕКОМЕНДУЕТСЯ

45 crgtools
46 iplir_gle
47 OpenSSL
48 ossl
49 soft_token
50 uprng
51 JSON
52 Xerces-C++
53 benchmark
54 fmt
55 googletest
56 libevent
57 libzip
58 zlib
59 itcshub
60 uni_logger
61 doxygen
62 licensing_system
63 reg_system

ПИЛОТИРУЕТСЯ

64 json-c
65 Conan



ТЕХНОЛОГИЧЕСКИЙ РАДАР

Правила использования, формирования и развития Технологического радара

Языки/фреймворки | Платформы | Утилиты/библиотеки | Практики | Print this radar | HOME

« Back to Radar home

РЕКОМЕНДУЕТСЯ

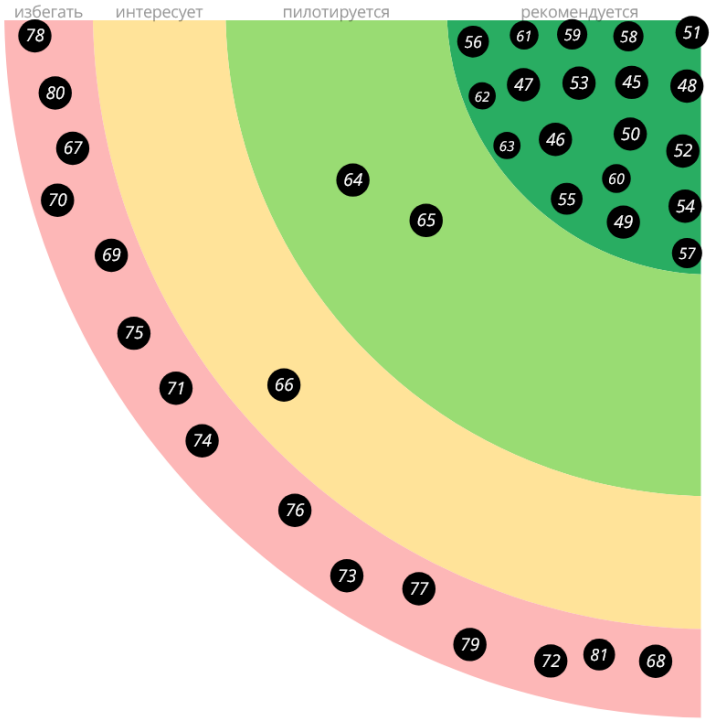
45 crgtools
46 iplir_gle
47 OpenSSL

Широко распространенная и хорошо поддерживаемая библиотека которую рекомендуется использовать для развертывания и/или использования инфраструктуры PKI совместно с распространенными криптографическими форматами и протоколами TLS и CMS. Работу с библиотекой из коробки поддерживают web сервера nginx и apache. Оригинальную версию без модификаций для поддержки ГОСТ алгоритмов (см ossl) рекомендуется использовать если в вашем продукте нет и не планируется необходимости использовать ГОСТ алгоритмы или в продукте есть исполнение для западного рынка в котором важно оперативно поднимать версию этой библиотеке, так как в ней, в силу её функционала, довольно часто находят и закрывают уязвимости.

Ссылка на паспорт компонента без модификаций для поддержки ГОСТ: OpenSSL

Ссылка на паспорт компонента с поддержкой ГОСТ: Паспорт набора компонентов ossl

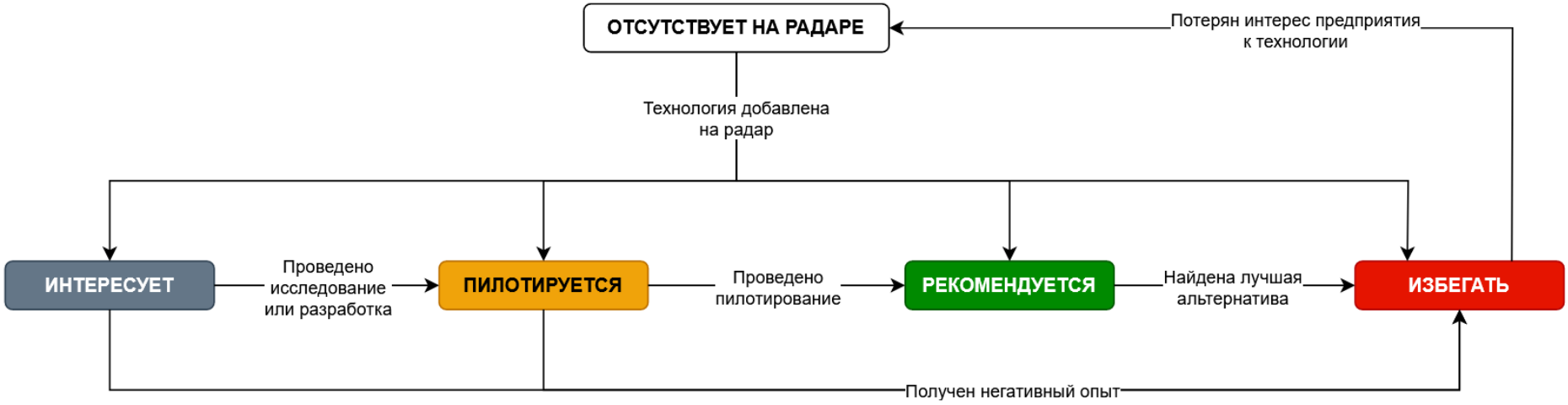
48 ossl
49 soft_token
50 uprng



Зоны Технологического радара

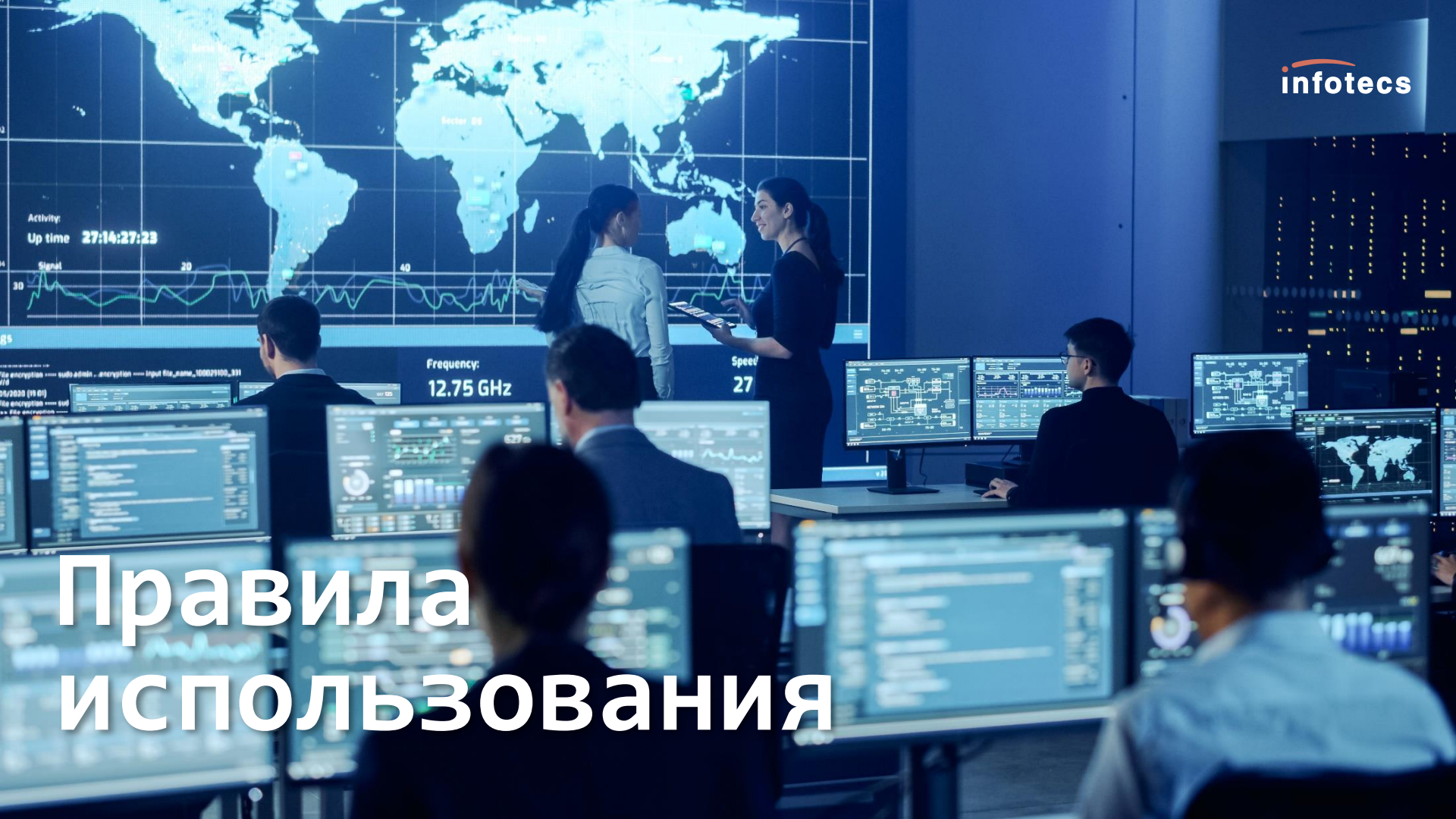
Зона	Значение
РЕКОМЕНДУЕТСЯ	Технология **разрешена и рекомендуется** для решения подходящих задач во всех проектах.
ПИЛОТИРУЕТСЯ	Технология успешно прошла предварительное исследование и **разрешена для пилотного использования в ограниченном наборе проектов**.
ИНТЕРЕСУЕТ	Технология **представляется потенциально полезной** и находится в состоянии исследования или разработки.
ИЗБЕГАТЬ	Технология **запрещена** к использованию без согласования с архитектором направления. В компании есть негативный опыт использования технологии или от технологии решено избавляться в пользу более подходящих альтернатив.

Жизненный цикл технологий



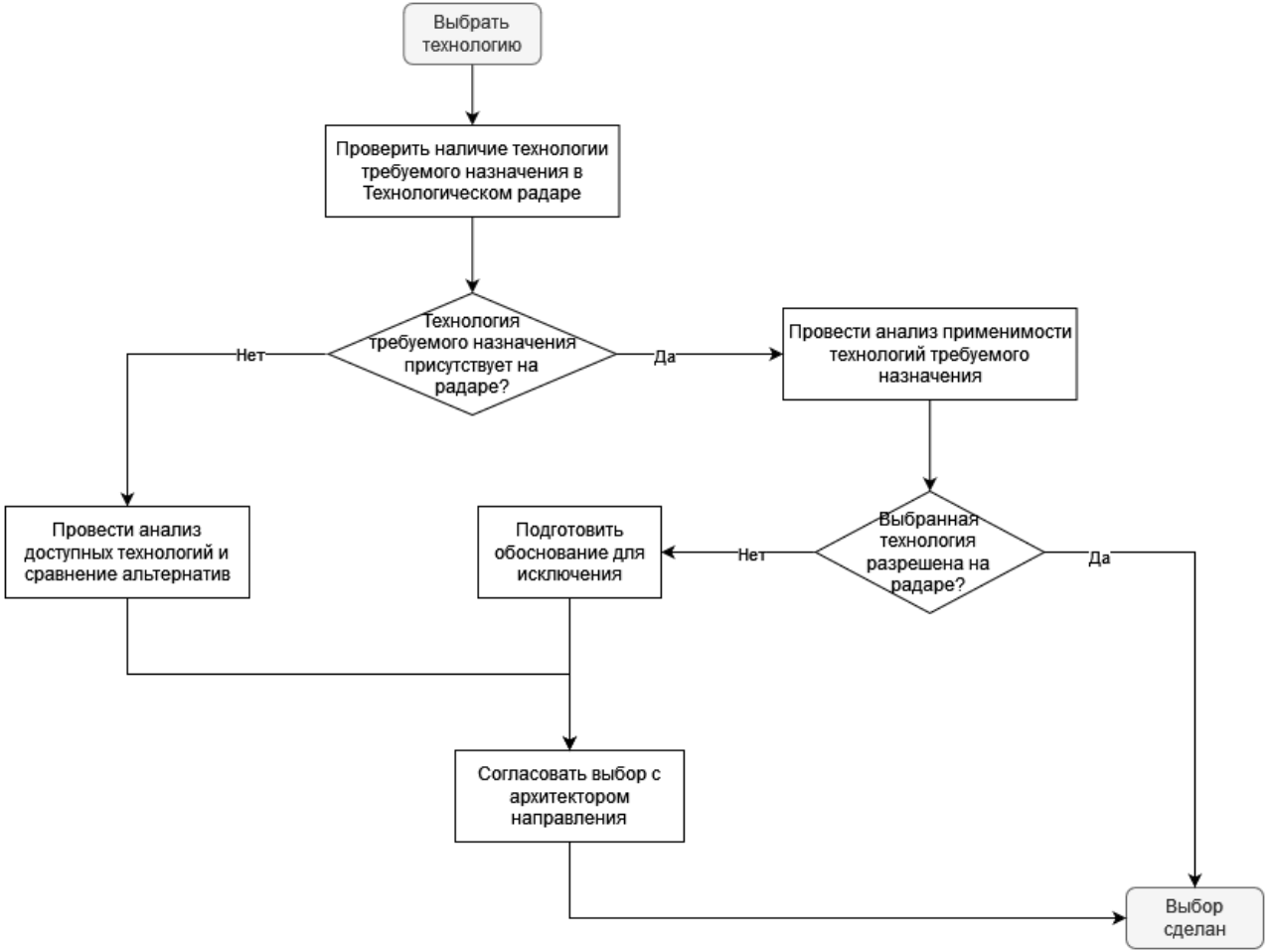
Границы Технологического радара

- Описывает только процесс выбора технологий
- Учитывает наименования технологий, а не конкретные версии
- Учитывает только программные технологии



Правила использования

Алгоритм выбора технологий



ADR для оценки технологий

Architecture Decision Record

Status

Accepted

Context

We need to record the architectural decisions made on this project.

Decision

We will use Architecture Decision Records, as described by Michael Nygard in this article: http://think
/documenting-architecture-decisions

Consequences

See Michael Nygard's article, linked above.

ADR в ИнфоТеКС

- Заголовок
- Форма согласования
- Контекст
- Решение
- Подверженные решению продукты
- Рассмотренные варианты
- Сравнение вариантов
- Последствия

Критерии сравнения технологий

Функциональные критерии:

- Наличие функций из предметной области, которые уже нужны по текущим требованиям
- Наличие функций из предметной области, которые потенциально могут быть востребованы при развитии

Критерии сравнения технологий

Нефункциональные критерии:

- Производительность и потребление аппаратных ресурсов
- Наличие поддержки целевых платформ и ОС
- Наличие поддержки целевых процессорных архитектур

Критерии сравнения технологий

Операционные критерии:

- Распространённость технологии в продуктах компании
- Качество документации и сложность освоения технологии
- Наличие активных изменений в коде за последний год
- Общее количество контрибьюторов в исходный код
- Наличие пакета в основных репозиториях платформ

Критерии сравнения технологий

Сертификационные критерии:

- Доступность исходных кодов
- Наличие известных замечаний исследовательской лаборатории

Критерии сравнения технологий

Критерии оценки качества:

- Степень покрытия модульными и интеграционными тестами

Критерии сравнения технологий

Критерии безопасности:

- Наличие известных уязвимостей в базах
- Наличие результатов проведения динамического или статического анализа

Критерии сравнения технологий

Лицензионные, экономические и политические критерии:

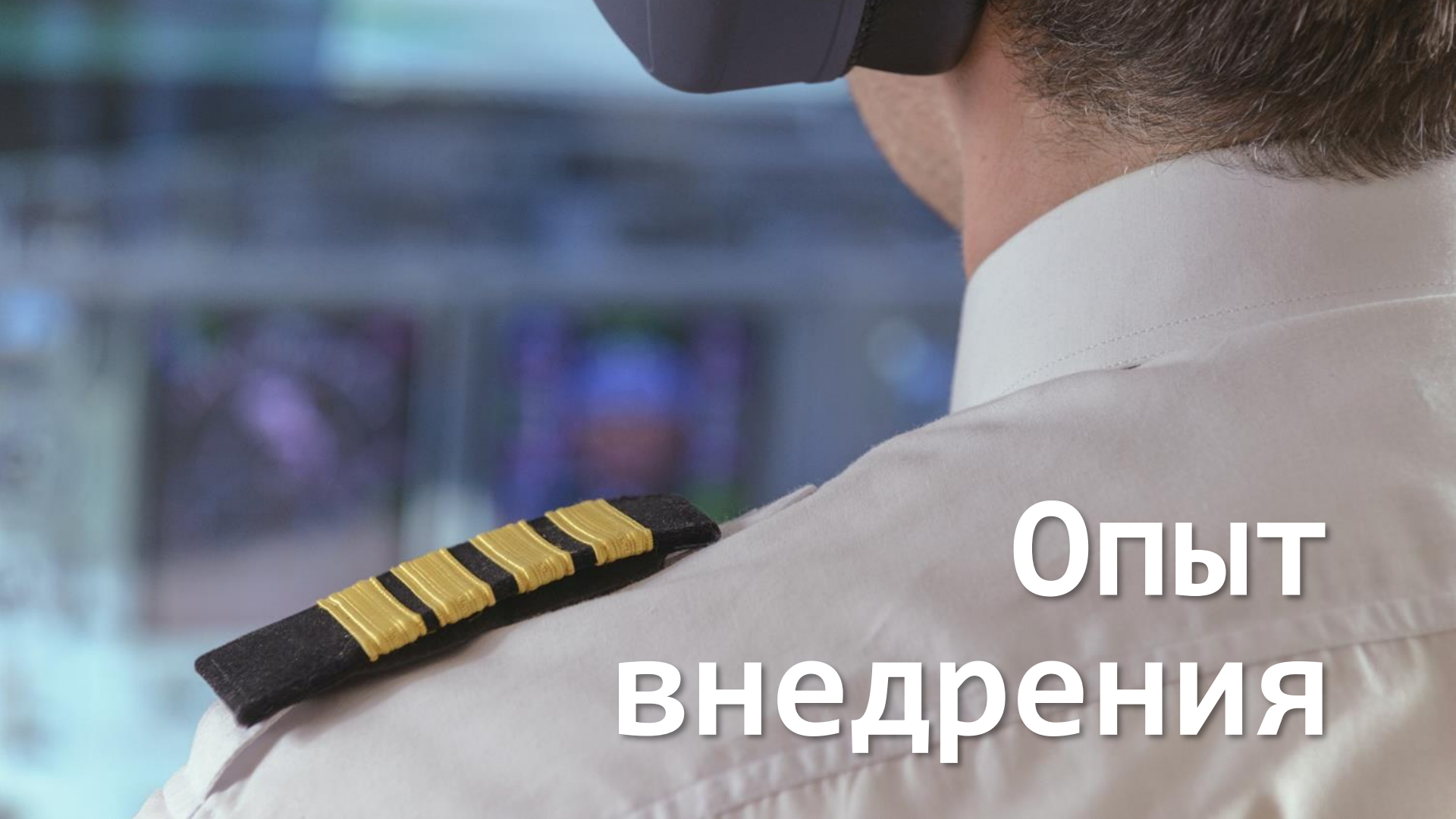
- Допускает ли лицензия использование технологии в коммерческих продуктах
- Стоимость лицензии на использование в коммерческих продуктах
- Проверка нахождения владельца технологии в РФ
- Проверка наличия технологии в реестре технологи с инъекциями на политической основе

Критерии сравнения технологий

Технологические критерии:

- Удобство интеграции технологии в продукт
- Зависимости времени исполнения
- Наличие дополнительных инструментов и зависимостей для сборки технологий

Лицензионные и экономические критерии	Лицензия допускает его использование в коммерческих продуктах	MIT License	BSD 2-Clause	MIT License	MIT License	MIT License	Apache License 2.0
	Стоимость лицензии на использование в коммерческих продуктах	-	-	-	-	-	-
	Политико-экономические риски (санкции и т.п.)	открытый код	открытый код	открытый код	открытый код	открытый код	открытый код
Сертификационные критерии	Доступность исходных кодов	GitHub	GitHub, GitHub	GitHub	GitHub	GitHub	GitHub
	Наличие замечаний исследовательской лаборатории	N/A	N/A	N/A	Нет	Нет	N/A
Операционные критерии	Активные изменения в коде за последний год	Нет	Да/Нет	Да	Да	Да	Да
	Релизы за последние два года (с мая 2020 года) + дата последнего релиза	Да (26 июля 2020)	Нет(12 июня 2014)/Нет(-)	Нет (15 декабря 2016) в форке от Infotecs релизов нет, но изменения с новых релизов забираются с оригинального репозитория	Да (3 января 2022)	Нет (25 августа 2016)	Да (28 октября 2021)
	Общее количество контрибьюторов в код (+ изменения за 3 месяца)	115 (+1)	28/4(+1)	171(-1)	226 (+11)	167(+1)	96(+2)
	Рейтинг на GitHub (+ изменения за 3 месяца)	2.8k(-0.4к)	1.1k(+0.1к)/111(-1)	6.1к (+0.2к)	28.6k (+1.7к)	11.7k(+0.3к)	15.4k(+0.2к)
	Наличие пакета основных репозиториях платформ (в Debian, NuGet и т.п.)	Да	Да/Нет	Да	Да	Да	Да
Качественные критерии	Степень покрытия модульными тестами	Хорошее (88%)	Тесты есть, но нет информации о покрытии	Хорошее (94%)	Отличное (100%)	Отличное (100%)	Тесты есть, но нет информации о покрытии
	Качество документации	Хорошее	Мало	Отличное	Отличное	Отличное	Хорошее
	Наличие предупреждений от компилятора (компилятор msvc, используются опции: /W4; для C++ файлов /std:c++17)	Да	Да	Да	Нет	Да	Да
Функциональные критерии	Поддержка целевых платформ и ОС	Cross platform (OS: Linux, MacOs, Windows)	Cross platform	Cross platform (OS: Linux, MacOs, Windows)	Cross platform (OS: Linux, MacOs, Windows, Platform: x86_64, aarch64 (rpi), armhf (rpi), aarch64 (android), armv7 (android), armv5el (openwrt), e2k-v4)	Cross platform (OS: Linux, MacOs, Windows, Platform: x86_64, aarch64 (rpi), armhf (rpi), aarch64 (android), armv7 (android), armv5el (openwrt), e2k-v4)	Cross platform (OS: Linux, MacOs, Windows, Platform: x64, haswell, westmere, arm64, ppc64)
Нефункциональные критерии	Указана поддержка спецификаций JSON	Да (RFC 7159)	Нет	Нет	Да (RFC-6901, RFC-6902, RFC-7159, RFC-7049, RFC-8259)	Да (RFC6901, RFC7159/ECMA-404)	Да (RFC-8259)
	Соответствие спецификации JSON (RFC7159, ECMA-404) по результатом тестов (детальные результаты тестов представлены ниже)	85%	75%	92%	99%	100%	92%
	Соответствие спецификации JSON (RFC 8259) по результатом тестов (детальные результаты тестов представлены ниже)	80%	Нет данных	Нет данных	87%	87%	Нет данных
	Производительность (по сравнению с rapidjson, детальные результаты тестов представлены ниже) — Чтение (DOM)	3-11x	2-8x	3-30x	2-9x	1x	0.2-0.8x
	Производительность — Сериализация	0.4-2x	0.5-6x	5-10x	0.6-2x	1x	0.5-1.5x
	Производительность — Сериализация (с форматированием)	0.3-2x	0.5-4x	Не поддерживается	0.6-1.5	1x	Не поддерживается
	Производительность — Чтение (SAX)	Не поддерживается	Не поддерживается	Не поддерживается	1-9x	1x	0.4-1x
Критерии безопасности	Известные уязвимости	3 (исправлены)	Нет данных	1 (исправлена)	Нет	Нет	Нет данных
	Уровень риска в BlackDuck	Нет	Нет	Нет	Нет	Нет	Нет
	Технология прошла фаззинг-тестирование	Да	Нет данных	Да	Да (1 и 2)	Да	Да

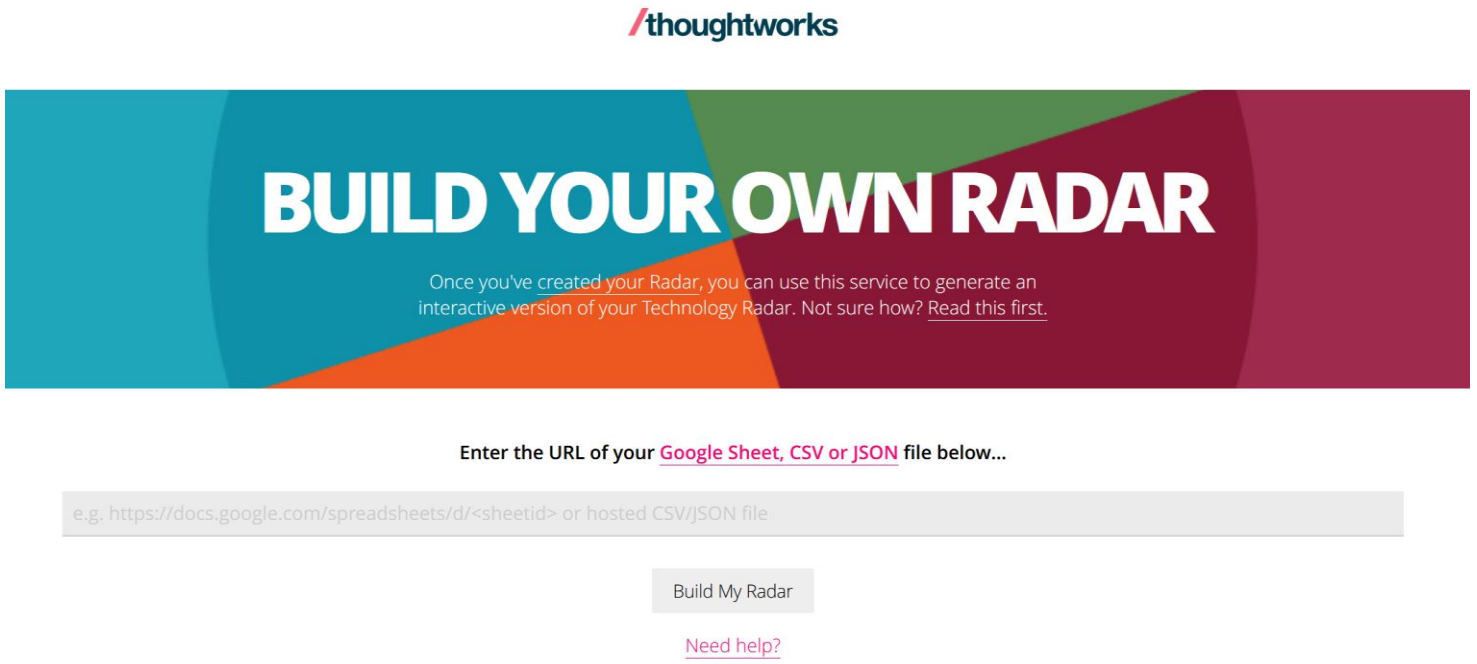


Опыт внедрения

Опыт внедрения

- Обеспечьте наличие API
- Используйте реализацию радара от ThoughtWorks

Реализация представления



https://github.com/thoughtworks/build-your-own-radar

Опыт внедрения

- Обеспечьте наличие API
- Используйте реализацию радара от ThoughtWorks
- Используйте ADR для обоснования оценки
- Актуальность важнее полноты

Какие технологии будут на радаре?

Актуальность радара важнее полноты.

Основной критерий для определения объёма радара - количество доступных ресурсов для поддержки радара в актуальном состоянии.

Учитываются следующие критерии:

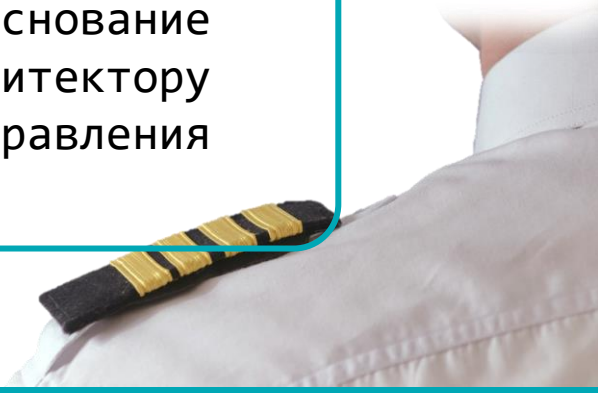
- Распространённость технологии в предприятии;
- Перспективы использования технологии в предприятии;
- Оценка последствий от выбора ошибочной технологии.

Опыт внедрения

- Обеспечьте наличие API
- Используйте реализацию радара от ThoughtWorks
- Используйте ADR для обоснования оценки
- Актуальность важнее полноты
- Обеспечьте широкое вовлечение участников

Как повлиять на оценки технологий?

1. Подготовить собственную оценку технологии
2. Подготовить в свободной форме обоснование изменения оценки технологии
3. Предложить подготовленные оценку и обоснование архитектору направления



Правила предложения технологий

Каждый может создать запрос на добавление технологии на радар.

Если предлагается уже используемая в проекте технология, рекомендуется помимо оценки технологии подготовить сравнение технологии с альтернативами.

Опыт внедрения

- Обеспечьте наличие API
- Используйте реализацию радара от ThoughtWorks
- Используйте ADR для обоснования оценки
- Актуальность важнее полноты
- Обеспечьте широкое вовлечение участников
- Важно, нужно, полезно

infotecs

ответы на вопросы

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363

Спасибо за внимание!

Минко Виталий

Руководитель архитектурного направления

e-mail: vitaly.minko@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363