

Ginc Radar

Технологический стек под **постоянным контролем**

Автоматизированный техрадар: непрерывный аудит зависимостей, управляемое устранение уязвимостей и предсказуемый темп обновления стека



Технологический стек — источник **прямых потерь инженерного времени** и неуправляемого риска. Ginc Radar переводит его в контролируемый процесс

168 млн р / год

Прямые потери инженерного времени на работу с легаси

20 команд * 10 человек * 20% времени

35 млн р

Разовая «расчистка» стека: остановка выпуска функциональности на 2 недели

Повторяется пока процесс ручной

77 млн р / год

Экономия в базовом сценарии — доля легаси снижается с 20 % до 10 %

Расчет - слайд 12, Сценарии – слайд 8

• Что происходит

- Данные о стеке фрагментированы: репозитории, чаты, устаревшая документация
- Аудит вручную занимает месяцы и устаревает в момент завершения
- Уязвимости и несовместимости накапливаются быстрее, чем закрываются

• Что предлагается

- Непрерывное сканирование репозиторий и построение актуальной карты стека
- Политики отставания версий и лимиты использования легаси
- Подготовленные миграции с прогоном CI и обязательным review

• Что требуется решить

- Утвердить пилотную зону и ответственного от ИТ
- Согласовать критерии успеха пилота
- Согласовать коммерческие условия



Данные о стеке фрагментированы, а цикл устранения проблемы не имеет управляемого срока

Решение принимается по картине, которая устарела на момент принятия, и исполняется по остаточному принципу

• Где сейчас лежат данные о стеке

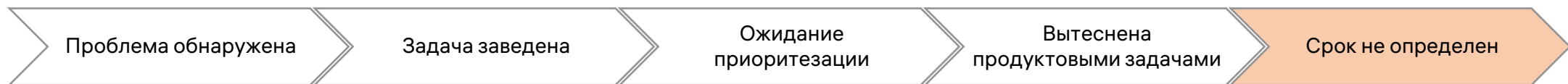
- В головах инженеров — уходят вместе с людьми
- В чатах и тикетах — не агрегируются и не проверяются
- В документации — актуальна на дату последнего аудита
- В репозиториях — источник истины, но никем не сведён воедино

Транзитивные зависимости — основная масса кода в проде — не отражены нигде

• Что это означает на практике

- Нельзя достоверно ответить, где в ландшафте используется конкретная уязвимая библиотека
- Нельзя спланировать миграцию: неизвестен объём работ и число затронутых сервисов
- Нельзя подтвердить регулятору состав ПО без ручной инвентаризации
- Нельзя оценить, растёт технический долг или сокращается — нет метрики

ТИПОВОЙ ЦИКЛ УСТРАНЕНИЯ ПРОБЛЕМЫ





Ручное управление стеком стоит 168 млн ₽ в год — это инженерное время, не потраченное на продукт

Все величины ниже выведены из одной базовой ставки на 20 команд

350 тыс р / мес

Стоимость одного инженера для компании

Базис для расчета

700 тыс р / мес

Потери одной команды из 10 человек в месяц

20% времени на работу с легаси*

168 млн р / год

Постоянные потери инженерного времени

20 команд * 700 тыс. р * 12 мес

35 млн р

Разовая «расчистка»: остановка выпуска на 2 недели

200 инженеров * 0,5 месяца

• Что скрыто за числами

- Архитекторы собирают данные вместо проектирования — недели вместо часов
- Разработчики чинят зависимости вместо новой функциональности
- Догоняющая миграция через две мажорные версии стоит на порядок дороже серии микро-шагов

• Что не учтено в оценке

- Стоимость инцидента из-за неустранимой уязвимости и простоя сервиса
- Недополученная прибыль от функциональности, сдвинутой на период расчистки
- Стоимость срочного найма под кризисную миграцию



Ginc Radar встраивается в существующий контур и превращает аудит из проекта в фоновый процесс

Три процесса работают непрерывно, без выделенной проектной команды и без остановки продуктовой разработки

• 1 - Сканирование

- Подключение к GitLab, Bitbucket, GitHub по read-only токену
- Разбор манифестов и лок-файлов, включая транзитивные зависимости
- Инвентаризация языков, фреймворков, платформ и базовых образов

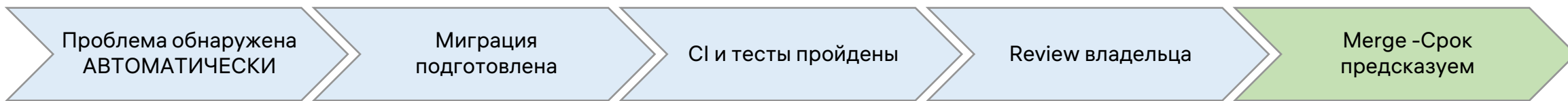
2 – Аналитика и контроль

- Актуальная карта технологий с владельцами и распределением по сервисам
- Политики: максимальное отставание версий, допустимая доля легаси
- Сопоставление с базами уязвимостей и оповещение при нарушении стандарта

3 - Действие

- Автоматическая подготовка миграции в отдельной ветке
- Прогон CI и тестов до предъявления изменений
- Обязательное review команды-владельца, merge — только вручную

ЦИКЛ УСТРАНЕНИЯ ПРОБЛЕМЫ ПОСЛЕ ВНЕДРЕНИЯ





Исходный код не покидает периметр заказчика: система разворачивается в вашем контуре

• Развертывание

- **On-premise** — полностью в контуре заказчика, без исходящих соединений

• Что система читает

- Файлы сборок и конфигурации в git репозиториях
- Метаданные и настройки корпоративных пакетных реестров для аудита актуальности версий/лицензий и верификации цепочек поставок.
- Операционные системы и пакеты на хостах

• Что система не делает

- Не выгружает исходный код за пределы контура
- Не требует write-доступа в режиме аудита
- Не выполняет merge в защищённые ветки
- Не отправляет данные о стеке третьим лицам

МОДЕЛЬ ДОСТУПА

Read-only токен для аудита. Write — только в выделенные ветки миграции, без прав на main

ХРАНЕНИЕ ДАННЫХ

СУБД в контуре заказчика

СЕРТИФИКАЦИЯ

сертификаты технологической совместимости с Axiom JDK и PostgresPro



Автоматическая миграция не может уронить продуктив: изменение проходит полный путь ревью, откат — закрытие запроса

• Поддерживаемые экосистемы

Java/Kotlin (Maven и Gradle)

.Net (Nuget)

JavaScript/Typescript (Npm)

Go (go.mod)

Ruby (Bundler)

Python (pip)

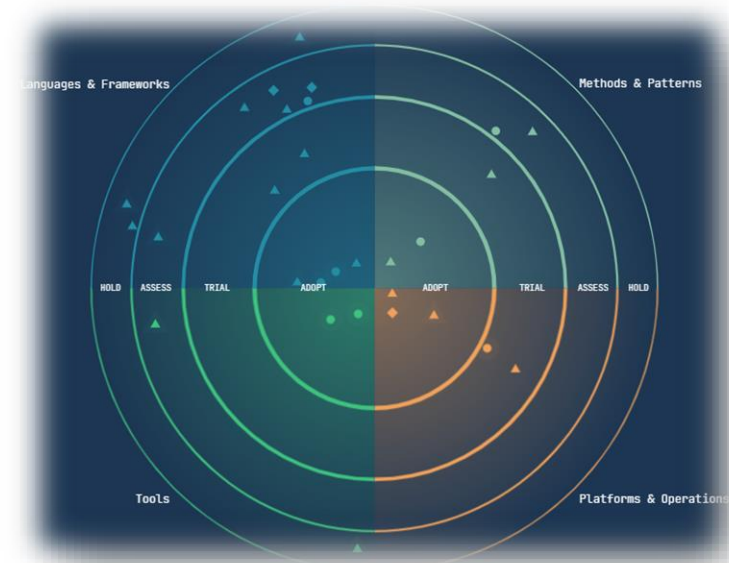
Swift (Spm)

PHP (Composer)

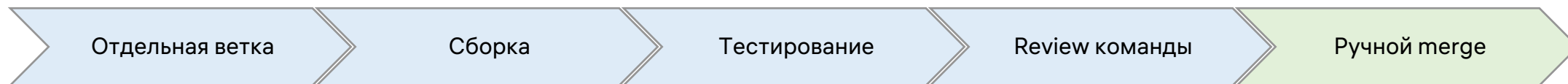
C++ (Conan)

• Интеграция контура

- Репозитории: GitLab, Bitbucket, GitHub
- CI: прогон существующих пайплайнов заказчика без изменения конфигурации
- Трекер: связка находок с задачами
- Источники уязвимостей: публичные базы CVE



КОНТРОЛЛИРУЕМЫЙ ПУТЬ МИГРАЦИИ



Откат до merge — закрытие запроса на слияние, следов в основной ветке не остаётся.

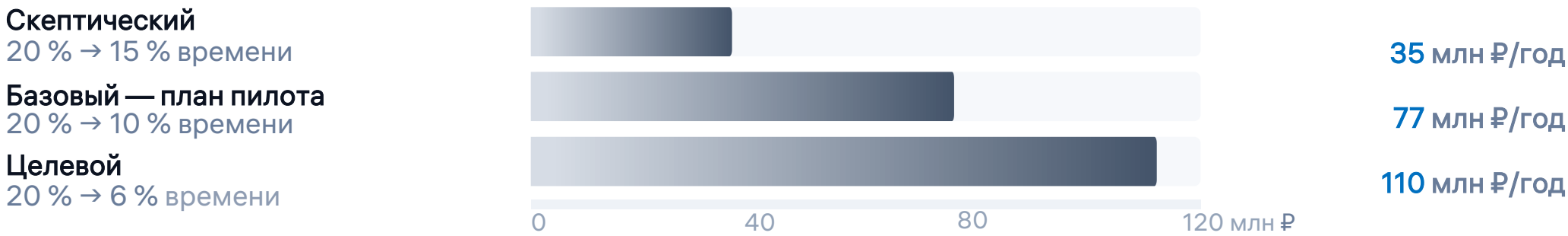
Изменение, не прошедшее тесты, до ревью не доходит. Автоматический merge в защищённые ветки не выполняется ни при каких настройках

Ответственность: система готовит и проверяет изменение, решение о применении всегда остаётся за командой-владельцем сервиса



Даже в скептическом сценарии эффект превышает стоимость владения

Эффект измеряется одной величиной: доля инженерного времени, уходящая на работу с легаси. Расчет произведен для стартовых затрат в 20 %



• **Стоимость владения и окупаемость**

Подписка, годовая стоимость на 20 команд	~ 6 млн руб
Стоимость внедрения пилота	< 1 млн руб*
Эффект в базовом сценарии в год	77 млн руб
Окупаемость при стоимости подписки 5 млн руб в год	< 1 месяца

• **Из чего складывается эффект**

- Возврат инженерного времени — основная часть эффекта, измерима по трекеру
- Отказ от разовых расчисток «завалов» — 35 млн руб, учтено в базовый и целевой сценарии
- Снижение вероятности инцидента — в расчёт не включено, считается сверху

Сценарии различаются только глубиной снижения доли легаси. Никаких других допущений в модели нет

Проверяемость: базовый сценарий подтверждается или опровергается на фактических данных пилотной зоны за 4 недели. Масштабирование — только после подтверждения

* Ориентировочная оценка включает в себя время работы специалистов заказчика и поставщика



Существующие инструменты закрывают отдельные задачи. Ginc Radar закрывает связку «карта стека → политика → миграция → отчётность»

Функционал	Dependabot / Renovate	Backstage	Snyk / Trivy	Ginc Radar
Автообновление зависимостей запросом на слияние	✓	—	~ только в части зависимостей с уязвимостями	✓
Поиск уязвимостей в зависимостях	✓	—	✓	✓
Пользовательские автоматизации рефакторинга	—	—	—	✓
Единая карта стека по всему ландшафту	—	~ ручное ведение	—	✓автоматически
Политики легаси и лимиты отставания версий	—	—	—	✓
Отчётность уровня СТО и совета директоров	—	—	~по ИБ	✓
Реестр отечественного ПО, поддержка и SLA	—	—	—	✓
Стоимость владения	Настройка и сопровождение силами команд	Платформенная команда на постоянной основе	Лицензия зарубежного вендора	Подписка по количеству репозиториев



Продукт включён в Реестр российского ПО — это снимает вопрос импортозамещения и даёт налоговые эффекты

• Реестровый статус

Реестровая запись Минцифры РФ	№ 28996
Дата включения	31.07.2025
Правообладатель	ООО «Джинк»
Соответствие политике импортозамещения	полное

• Что это дает заказчику

- **Повышающий коэффициент при расчёте амортизации** — расходы на ПО из реестра учитываются с коэффициентом
- **Федеральный инвестиционный налоговый вычет** — при соблюдении условий применения
- **Доступ к субсидиям** — для малого и среднего бизнеса
- **Прохождение аудита на импортозамещение** — без замечаний по данному классу ПО

Пилот на 4 недели: от подключения репозиторийев до подтверждённого расчёта эффекта на ваших данных

Цель пилота — не демонстрация продукта, а получение эффекта, на основании которого принимается решение о масштабировании

1

НЕДЕЛЯ 1

Развертывание и baseline

- Установка в контуре, подключение репозиторийев пилотной зоны
- Настройка политик и лимитов, обучение команды
- Фиксация исходного состояния: карта стека, отставание версий, уязвимости

2

НЕДЕЛЯ 2 - 3

Эксплуатация и миграции

- Приоритизация находок совместно с командами-владельцами
- Подготовка и проведение контролируемых миграций
- Замер фактических трудозатрат на каждое изменение

3

НЕДЕЛЯ 4

Итоги и решение

- Фиксация конечного состояния и расчёт дельты
- Расчёт эффекта на фактических данных пилотной зоны
- Презентация результатов CIO и решение о масштабировании

Критерии успеха

- Просканировано ≥ 95 % репозиторийев пилотной зоны
- Построена карта стека с указанием владельцев
- Не менее 3 миграций доведены до merge без отката
- Расчёт эффекта подтверждён фактическими данными

Что требуется от заказчика

- Вычислительный ресурс для развертывания
- Доступ к репозиториям пилотной зоны
- Ответственный от ИТ — точка входа на весь период
- Ориентировочно 16 часов архитектора и 8 часов DevOps*
- Согласование со службой ИБ до начала работ

Коммерческие условия

Кол-во репозиторийев пилотной зоны	_____
Стоимость пилота	_____
Модель подписки	По репозиториям
Предлагаемая дата старта	_____

Все цифры в презентации выведены из одной базовой ставки и двух допущений

Исходные величины

Полная стоимость инженера для компании, в месяц	350 тыс ₽
Размер продуктовой команды	10 человек
Количество продуктовых команд в периметре	20
Число инженеров в периметре	200
Годовой фонд инженерного времени в деньгах	840 млн ₽
Доля времени на работу с легаси сегодня	20%

Расчет затрат на Ginc Radar

Количество репозиторийев	1000
Стоимость подписки за репозиторий в месяц	500 ₽
Стоимость лицензий в год	6 млн ₽
Стоимость внедрения, единоразово**	1 млн ₽

Расчет потерь

Потери одной команды: $3,5 \text{ млн} \times 20 \%$, в месяц	700 тыс ₽
Потери периметра: $700 \text{ тыс} \times 20 \times 12 \text{ мес}$, в год	168 млн ₽

Расчет эффекта

Скептический: $840 \text{ млн} \times (20 \% - 15 \%) - 7 \text{ млн} \text{ ₽}$, в год	> 35 млн ₽
Базовый: $840 \text{ млн} \times (20 \% - 10 \%) - 7 \text{ млн} \text{ ₽}$, в год	> 77 млн ₽
Целевой: $840 \text{ млн} \times (20 \% - 6 \%) - 7 \text{ млн} \text{ ₽}$, в год	> 110 млн ₽

Что в модель не заложено: стоимость инцидента ИБ, недополученная прибыль от сдвига релизов, стоимость срочного найма под кризисную миграцию, эффект от снижения времени вывода функциональности. Оценка сознательно консервативная

* Предполагается, что разовая расчистка производится раз в год

** Включается оплата услуг поставщика и затраты персонала заказчика



СПАСИБО ЗА ВНИМАНИЕ !

<https://ginc-it.ru>

sales@ginc-it.ru

+7 495 940 7771