

#PAYMENTSECURITY

Добавляем автоматизацию в контроли PCI DSS без головной боли

Виктория Гадалова

Яндекс

5–6 августа 2026



Виктория Гадалова

Старший специалист по ИБ Компаенсу · Яндекс

5 лет QSA

1,5 года внутренний специалист ИБ

EMAIL

roryvee@yandex-team.ru

TELEGRAM

@roryvee

01

РАЗДЕЛ 01

Зачем нужен PCI DSS?

Что такое PCI DSS и зачем он нам?

04

Применим к компаниям, которые:

Хранят

Обработывают

Передают

Влияют на безопасность



Сервисы

05

1

Сервис, который хранит,
обрабатывает и передает данные
карт

> 30

Сервисов, которые влияют на
безопасность данных карт

02

РАЗДЕЛ 02

В чём проблема?

Какие есть проблемы?

07



Количество проверок для 30 сервисов

5

Одинаковых ручных проверок

3

Дня на каждый сервис

03

РАЗДЕЛ 03

Какие есть проверки?

Какие есть проверки?

09

ASV-сканирование

Требование 11.3.2 PCI DSS –
раз в 3 месяца

Внутреннее сканирование

Требование 11.3.1 PCI DSS –
раз в 3 месяца

Контроль прав доступа

Требования 7.2.4 PCI DSS –
раз в 6 месяцев

Соблюдение SDLC

Требование 6.2 и 12.4.2 PCI
DSS – раз в 3 месяца

Реагирование на события

Требование 12.4.2 PCI DSS –
раз в 3 месяца

Автоматизация по созданию задач

Создано 03 июл, 16:17, обновлено 23 июл, 15:03

Ежеквартальный аудит PCI DSS 2026-2027 (2й)

Переоткрыть

Нужна информация

В работу

Необходимо выполнить ежеквартальный аудит сервиса.

Скоуп (Схема потоков данных, Скоуп PCI DSS):

- веб-приложение,
- мобильное приложение,
- бэкенд-приложение.

Необходимые проверки:

- Внешнее сканирование на наличие уязвимостей (ASV),
- Внутреннее сканирование на наличие уязвимостей,
- Проверка учетных записей и прав доступа,
- Соблюдение регламента SDLC,
- Проверка реагирования на события.

Проверяем за период: 02.06.2026 - 03.07.2026.

Тикет на прошлый аудит

📎 Прикрепить файлы

+ Связь с задачей

📋 Чеклист

Связанные задачи 5 ^ +

Статус

Тип

Приоритет

Автор

Исполнитель

Наблюдатели

Теги

✔️

Закрит

 ▾

Решен

📄

Задача

==

Средний

●

Robot

👤

Виктория Гадалова

👤

Виктория Гадалова

q2-pcidss

Пример внешнего вида задач

Автоматизация по созданию задач

11

Моё автодействие

Виктория Гадалова

Добавить описание

Выберите тип автодействия

Обновление задач

Создание задач

⌚

График срабатывания

Настройте расписание для автодействия

Повторение

По часам

По дням

По неделям

Повторять раз в 13 недель

Дни недели

☐

пн

☐

вт

☐

ср

☐

чт

☒

пт☐☐

Начать

03.07.2026 15:00

Закончить

ДД.ММ.ГГГГ чч:мм

☐ Отправлять уведомление при каждом срабатывании

➔

Создать задачу с заданными параметрами

📄 Новая задача

Название задачи*

Ежеквартальный аудит PCI DSS 2026-2027

Описание

Необходимо выполнить ежеквартальный аудит сервиса.

Пример настройки
автосоздания

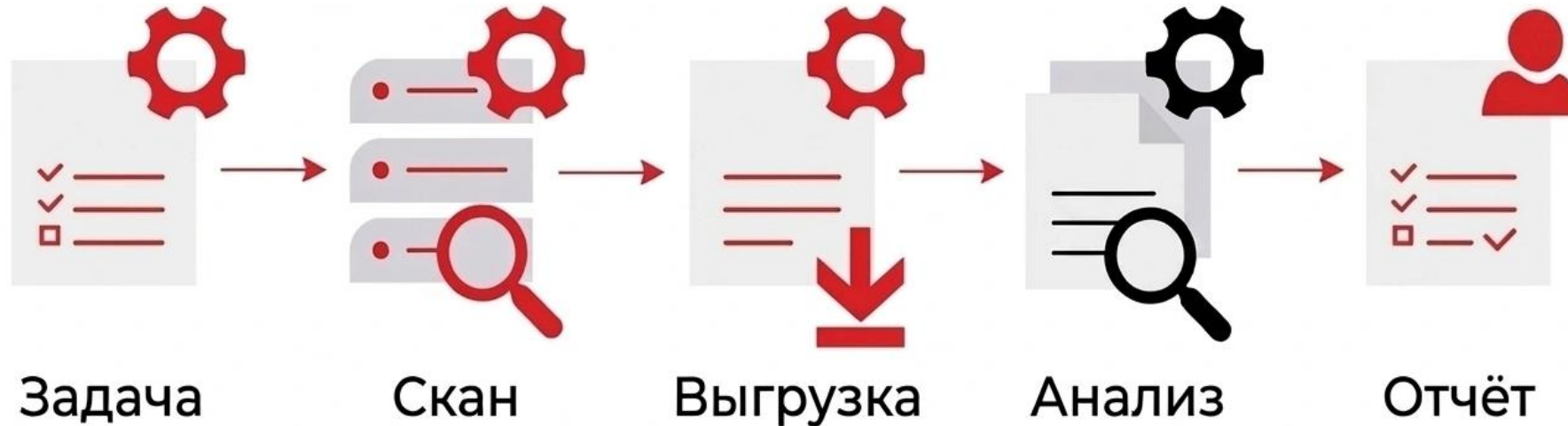
ASV и внутреннее сканирование

12



ASV и внутреннее сканирование

13



Стало

ASV и внутреннее сканирование

Robot призвал Виктория Гадалова · 03 июл, 21:33

Сканирования завершены



Важно

Необходимо провести триаж находок по результатам сканирований.

ASV

Цели	Статус	Запуск	Завершение	Ссылка	Результат
yandex.ru	Finished	2026-07-03 17:37	2026-07-03 21:33	Скан	Результаты сканирования

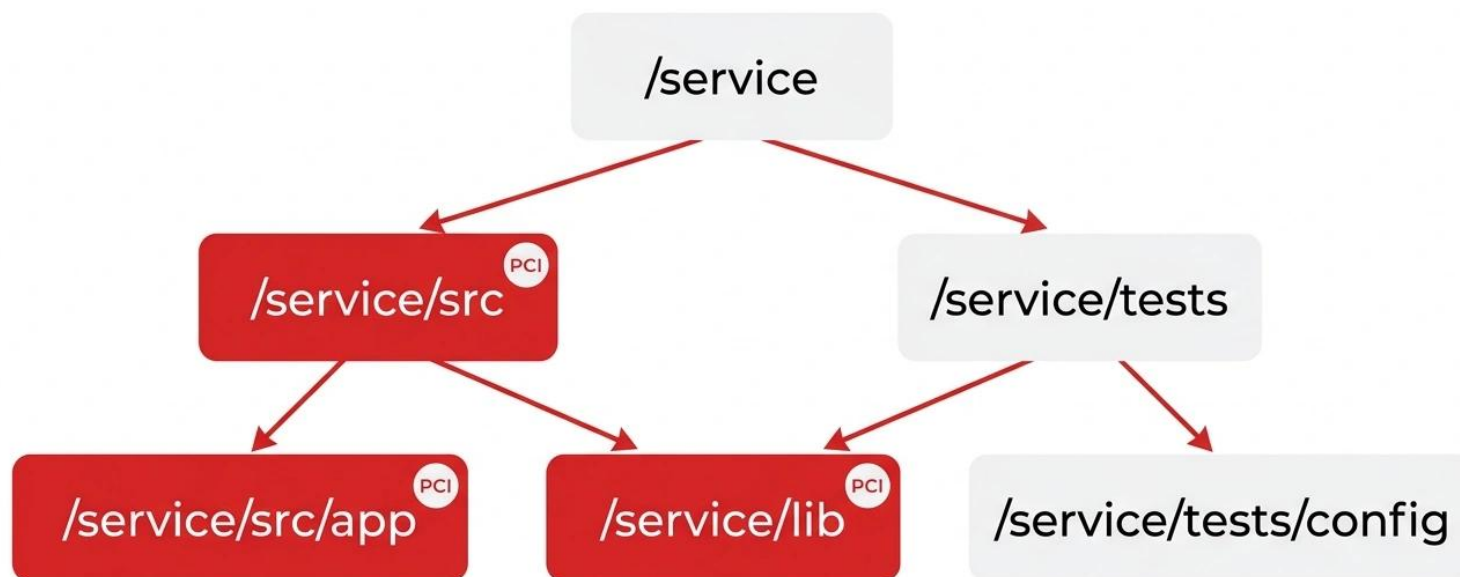
Пример сканирования

Robot · 03 июл, 17:36
/scan.asv yandex.ru

Скан ASV запущен: 3983388

Контроль соблюдения SDLC

15



Репозиторий

Контроль соблюдения SDLC

16



Контроль соблюдения SDLC

17



Контроль соблюдения SDLC

18



Контроль соблюдения SDLC

PCI DSS commits

PCI DSS service ▾

03.04.2026 ▾

03.07.2026 ▾

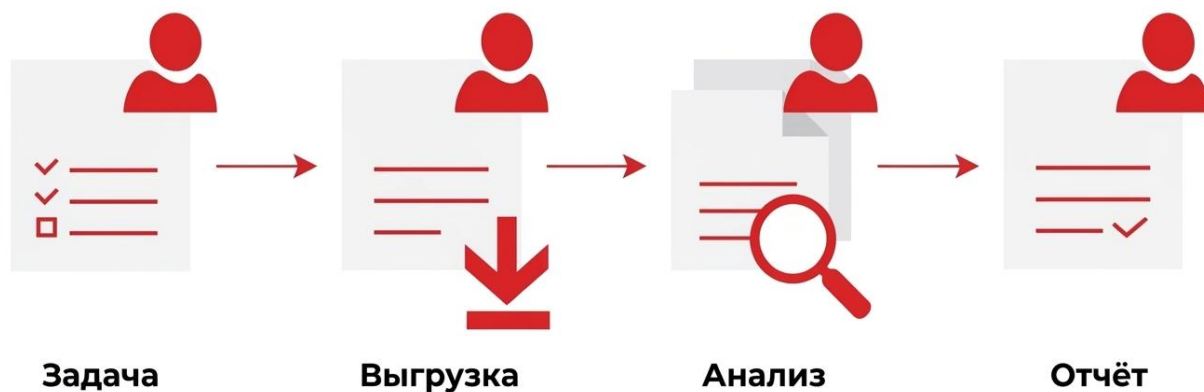
All

PCI DSS Not reviewed

03.04.2026 10:15	Migrated key management system to use Hardware Security Module (HSM).	PCI DSS reviewed
04.04.2026 09:30	Patched critical vulnerability in payment processing gateway application.	PCI DSS Not reviewed
12.04.2026 14:00	Documented internal procedures for semi-annual firewall rule reviews.	PCI DSS reviewed
25.04.2026 11:45	Implemented multi-factor authentication (MFA) for administrative access.	PCI DSS reviewed
05.05.2026 16:20	Reviewed and updated data retention policy for cardholder data.	PCI DSS Not reviewed
18.05.2026 08:30	Restored and tested backups of systems handling payment card data.	PCI DSS reviewed
29.05.2026 15:00	Updated vendor compliance documentation for all service providers.	PCI DSS reviewed
10.06.2026 13:30	Documented recent risk assessment and related remediation plans.	PCI DSS Not reviewed
22.06.2026 10:00	Patched operating system vulnerabilities on cardholder data environment (CDE) servers.	PCI DSS reviewed
03.07.2026 17:00	Signed latest attestation of compliance (AoC) for the current year.	PCI DSS Not reviewed

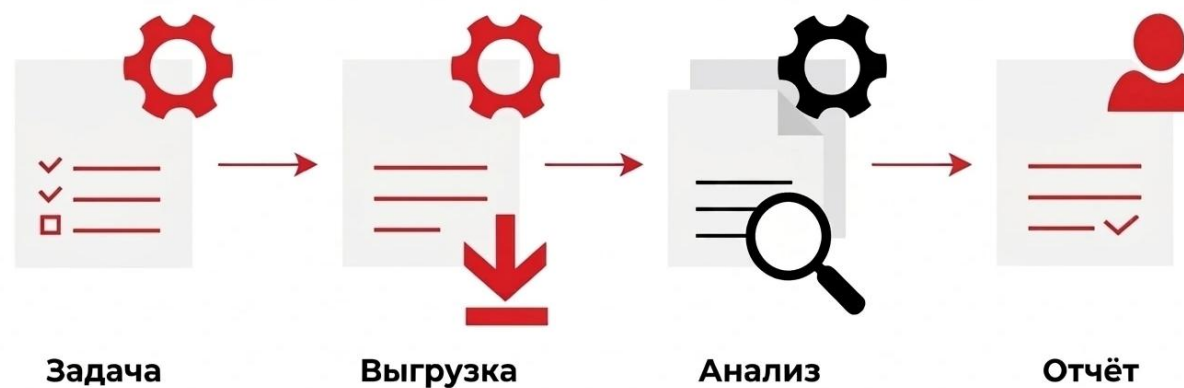
Контроль соблюдения SDLC

20



Было

Стало



Контроль прав доступа

21

Инфраструктура

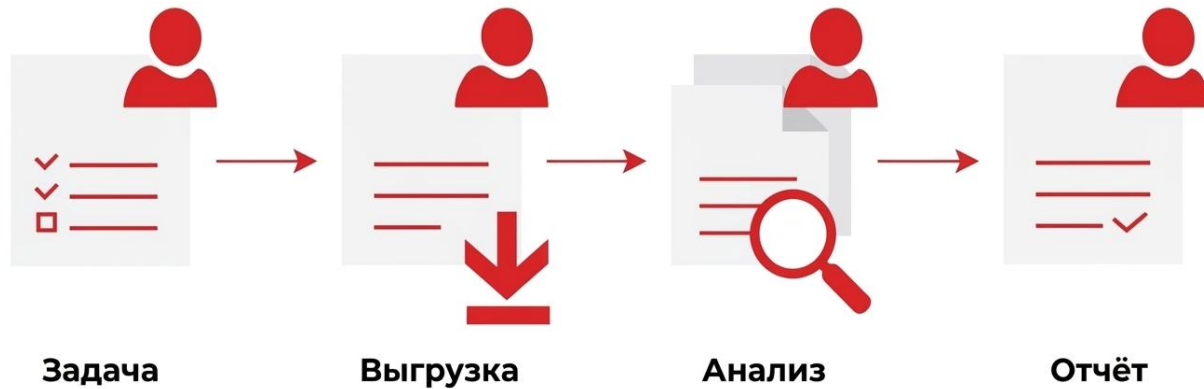
- Ограничение административных прав доступа
- Read-only fs или алерты на изменения

Репозиторий

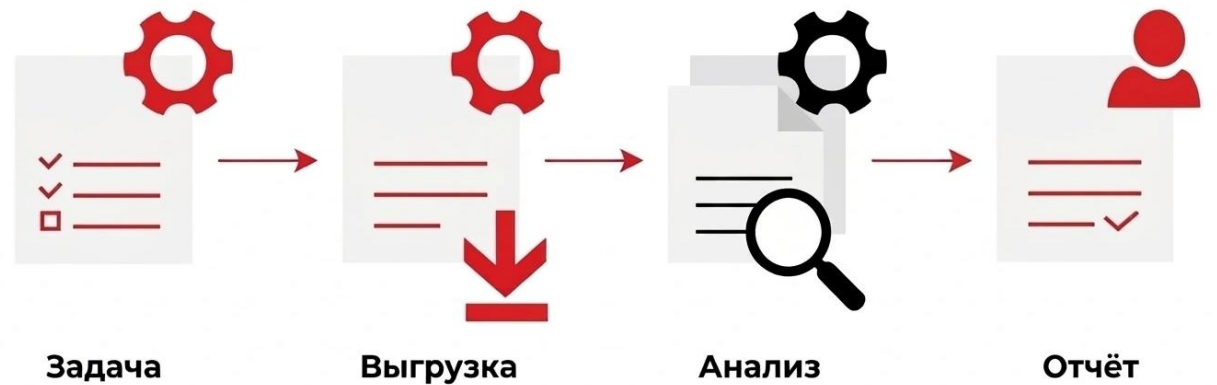
- Настройки прав доступа

Контроль прав доступа

22



Стало



Проверка реагирования на события

23



Было

Проверка реагирования на события

24



Стало

04

РАЗДЕЛ 04

Чем лучше?

Плюсы и минусы

26

Чем помогает автоматизация?

- Меньше времени на выполнение проверок
- Меньше влияния человеческого фактора в проверках
- Проще контролировать прохождение обучения и количества ревьюеров

Какие минусы?

- Риск возникновения ошибок/пропуска нюансов, которые мог бы выявить человек
- Работает на заранее обозначенной области применимости

Сравнение

27

-65%

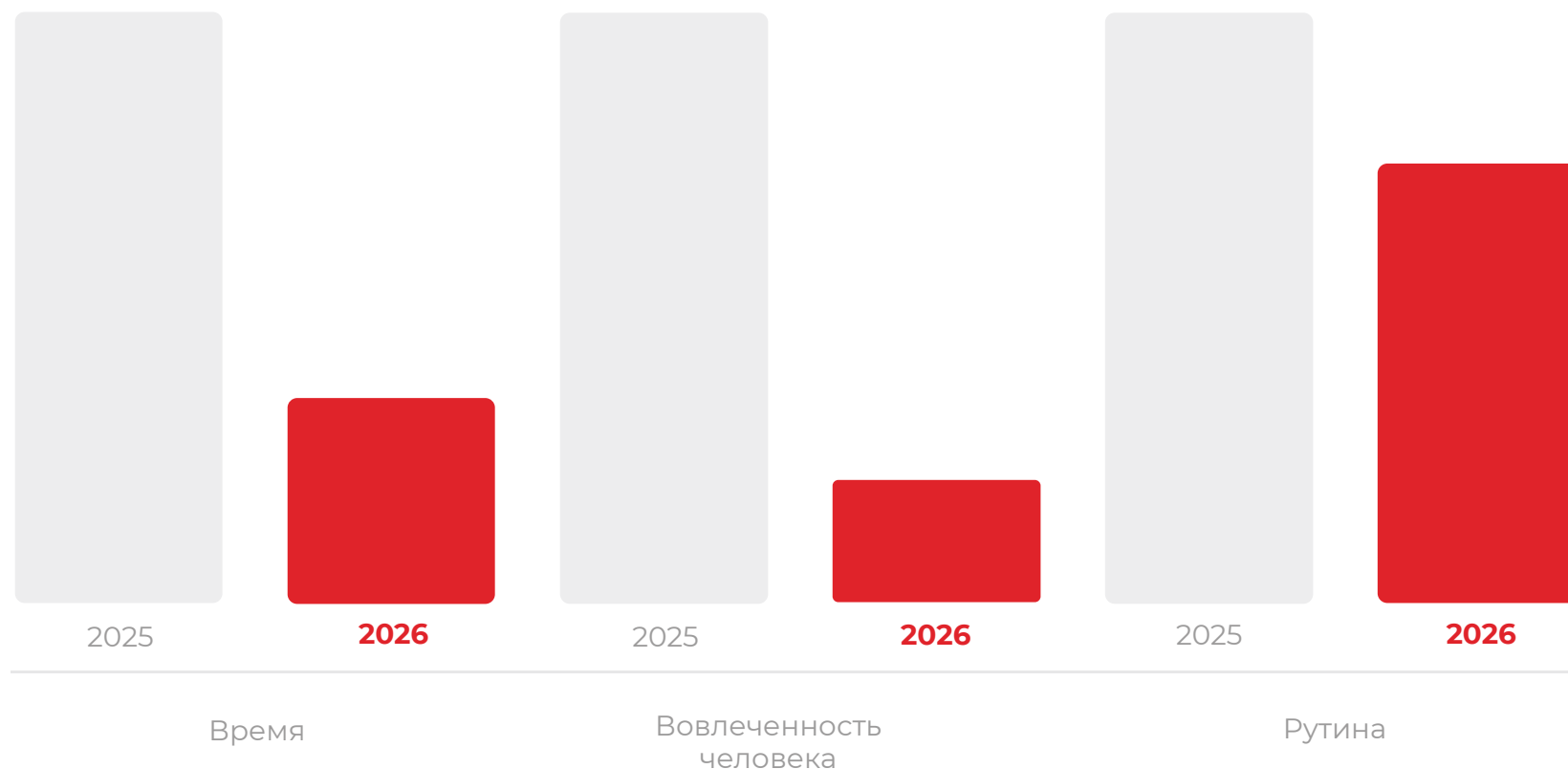
Затрачиваемого времени

-80%

Вовлеченности человека в
выполнение задачи

-30%

Рутинны



#PAYMENTSECURITY

Добавляем автоматизацию в контроли PCI DSS без головной боли · Виктория Гадалова

Что важно не забыть?

28

Создание задачи

Призыв ответственных



Запуск проверок

Контроль перечня
компонентов



Выгрузки

Разметка сервисов/скоупа



Анализ результатов

Проблемные моменты



Формирование отчёта

Создание задач на
устранение

#PAYMENTSECURITY



**Автоматизация не значит отказ от людей, это
значит позволить им решать более важные
задачи внутри компании**

© Aneesh Paul Chopra

#PAYMENTSECURITY

Вопросы?

EMAIL

roryvee@yandex-team.ru

TELEGRAM

[@roryvee](https://t.me/roryvee)