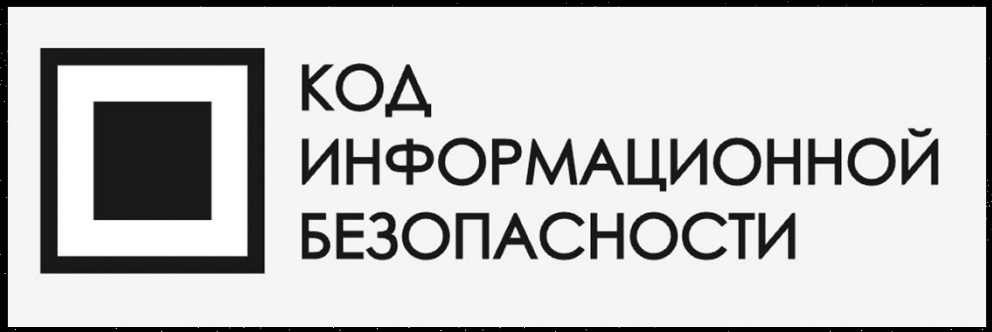
АНТИФИШИНГ

Безопасная разработка и Shift-Left Security: как далеко влево вы готовы зайти?



blog.antiphish.ru

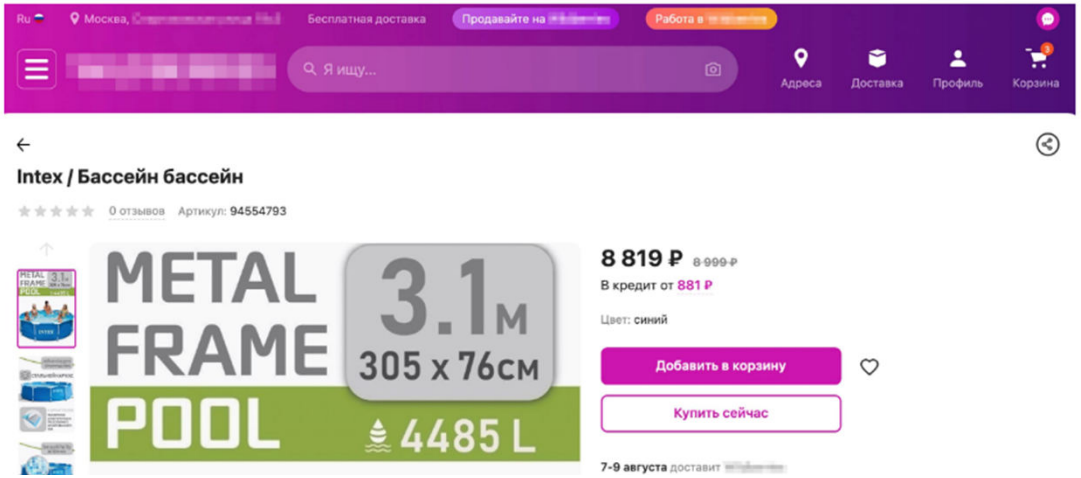
t.me/antph

Киберкампании

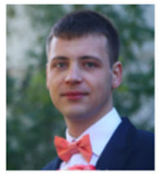
Обнаружена мошенническая кампания, для проведения которой используется популярный маркетплейс.

Схема действий мошенников

1. Мошенники выкладывают на официальный сайт известного маркетплейса несколько товаров. Это может быть все, что угодно: от дачного бассейн до смартфона. Преступники представляются разными продавцами, но используют один и тот же номер.



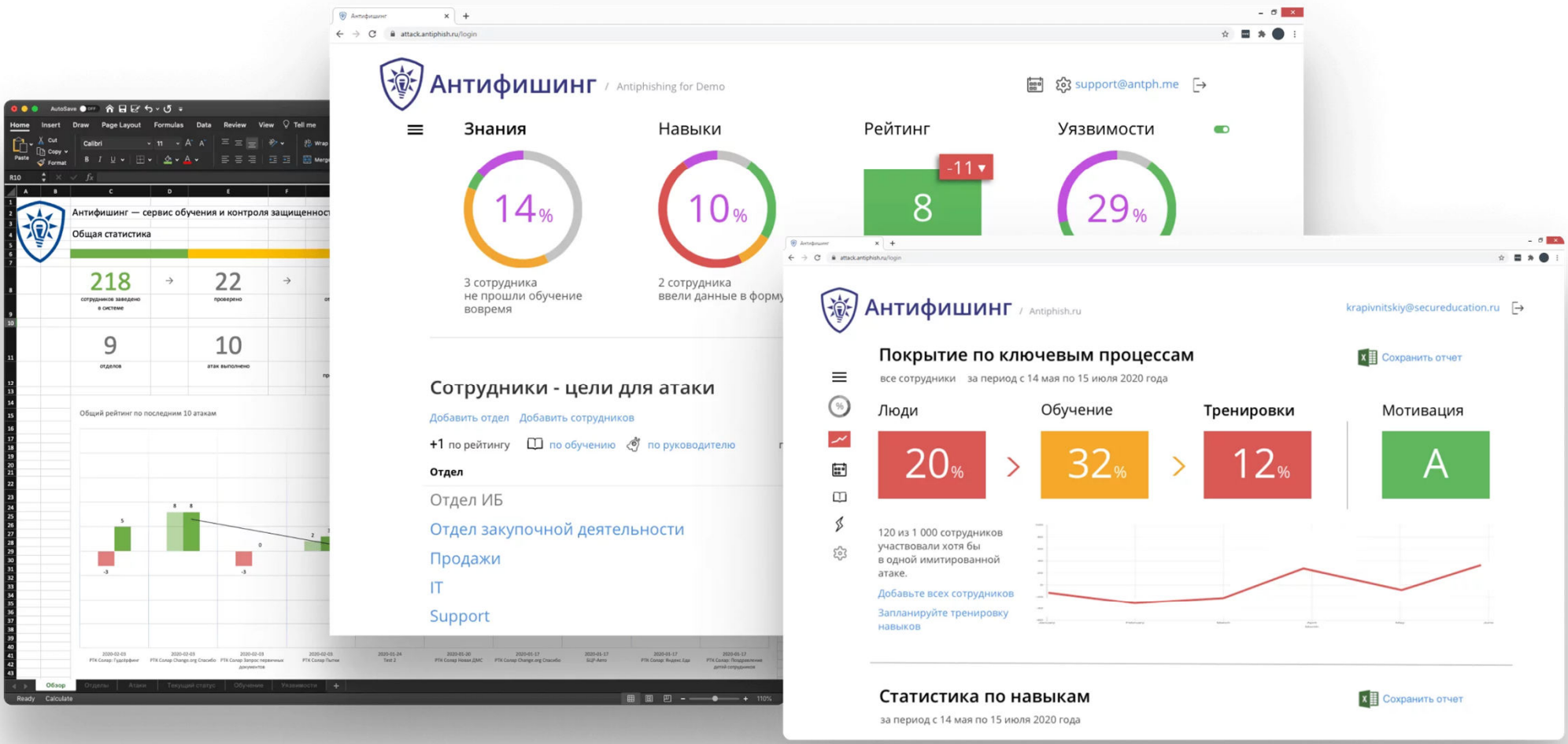
Андрей Жаркевич
редактор



Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

Антифишинг для всех сотрудников



Новости 12.10.2(

19:25

SpaceX отправит первого в исто
рии космического туриста в по-
лет вокруг Луны

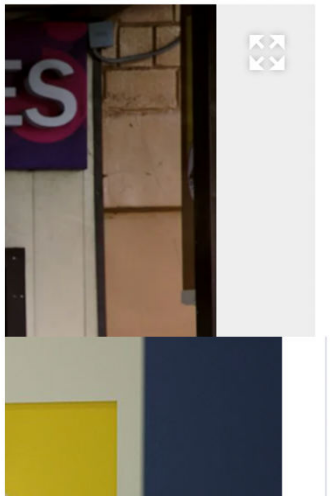
Информационная безопасность

26.01.2022, 00:47

Вирус взял подработкой

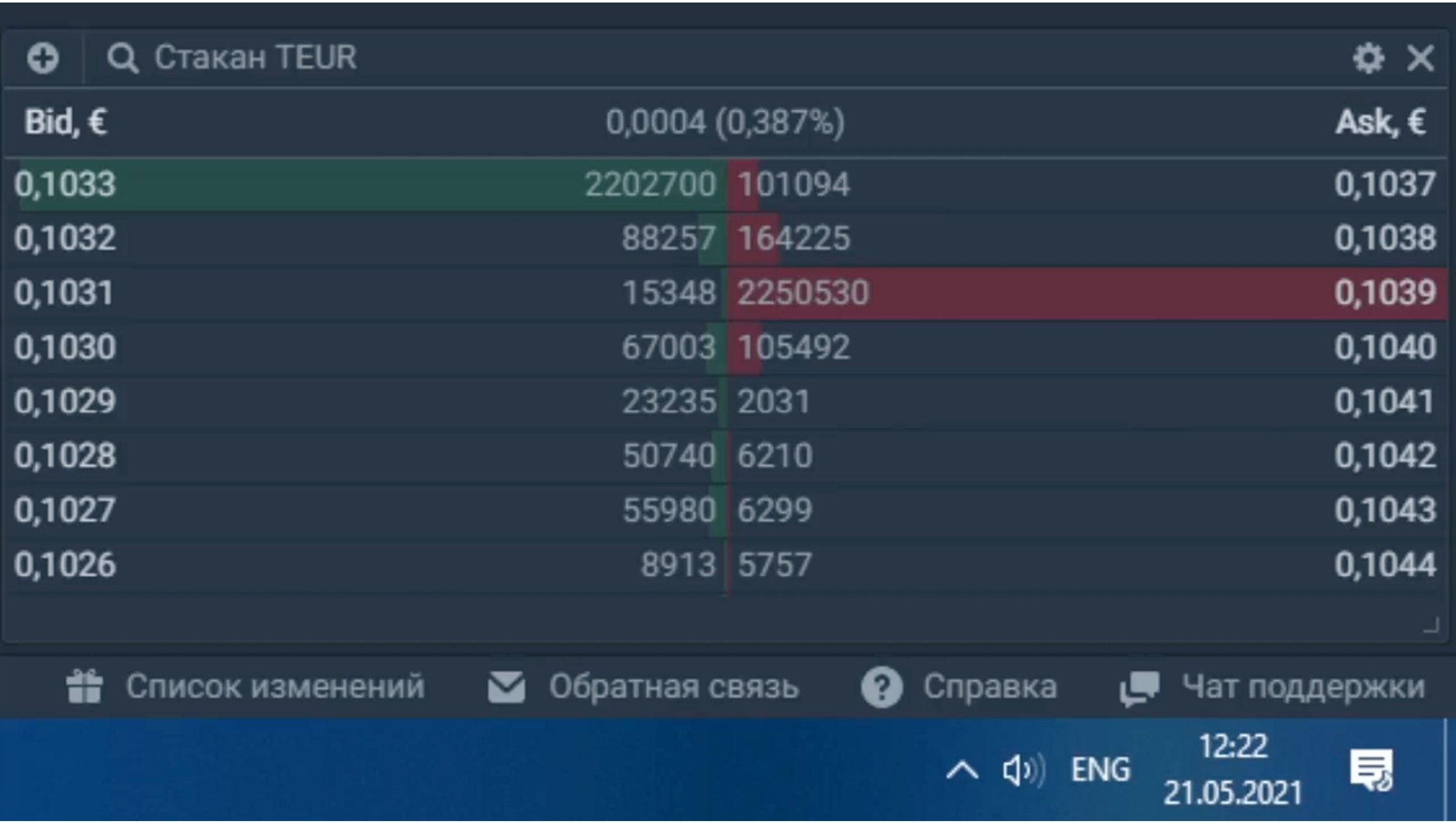
В доработанных модулях 1С нашли вредоносный код

Данные нескольких десятков компаний были украдены через вредоносный код в модулях 1С, обнаружили в RTM Group. По ее данным, он встраивался в программное обеспечение (ПО) во время доработки модулей у программистов на аутсорсинге. В самой 1С утверждают, что не сталкивались с такими случаями, но, чтобы избежать злоупотреблений, предлагают клиентам обращаться к официальным сертифицированным партнерам. Подобные вещи не всегда происходят умышленно, уточняют эксперты, заражен может быть компьютер самого исполнителя.



нное

головное дело
и регистрировались
, а затем уже под
изитам. Тем не менее
ошеннические схемы
ыстром росте, отсюда


Стакан TEUR
Bid, €
0,0004 (0,387%)
Ask, €
0,1033 2202700 101094 0,1037
0,1032 88257 164225 0,1038
0,1031 15348 2250530 0,1039
0,1030 67003 105492 0,1040
0,1029 23235 2031 0,1041
0,1028 50740 6210 0,1042
0,1027 55980 6299 0,1043
0,1026 8913 5757 0,1044
Список изменений
Обратная связь
Справка
Чат поддержки
ENG
12:22
21.05.2021

Doublesharp 2 апреля 2021 в 18:49

Путаница зависимостей. Как я взломал Apple, Microsoft и десятки других компаний

Код предназначался для внутреннего использования в PayPal, и в его файле package.json, по-видимому, содержалась смесь публичных и частных зависимостей — публичные пакеты от npm, а также имена непубличных пакетов, скорее всего, размещённых внутри PayPal. В то время этих имён не было в публичном реестре npm.

https://habr.com/ru/company/skillfactory/blog/550380/

```
"dependencies": {
  "express": "^4.
  "dustjs-helpers
  "continuation-l
  "pplogger": "^0
  "auth-paypal":
  "wurfl-paypal":
  "analytics-payp
}
```

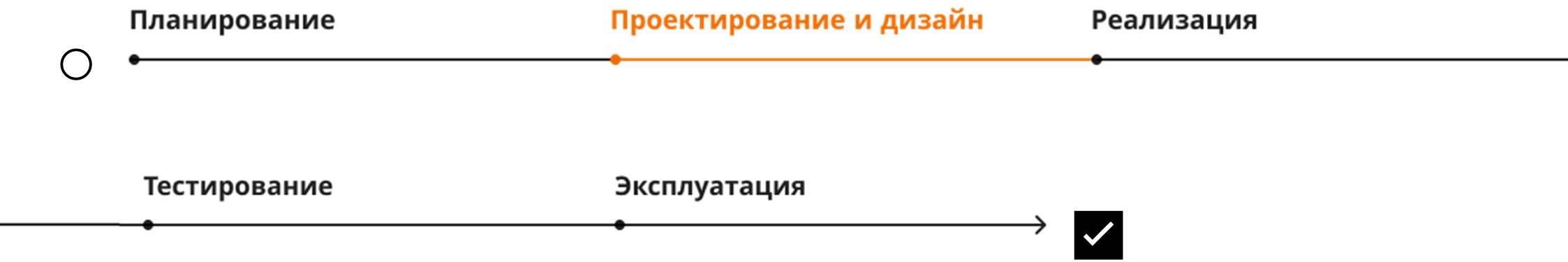
При загрузке зависимостей менеджеры пакетов npm, pip и gem в осн ли пакеты из основных общедоступных репозиториев NPM, PyPI и RubyGems, кот е приоритетными.

Присутствие похожих пакетов с такими же именами в репо игнорировалось без отображения предупреждений и сбое е администраторов. В PyPI на приоритет загрузки влиял номер в ория была загружена самая последняя версия пакета). В NPM и Ruby ько от репозитория.

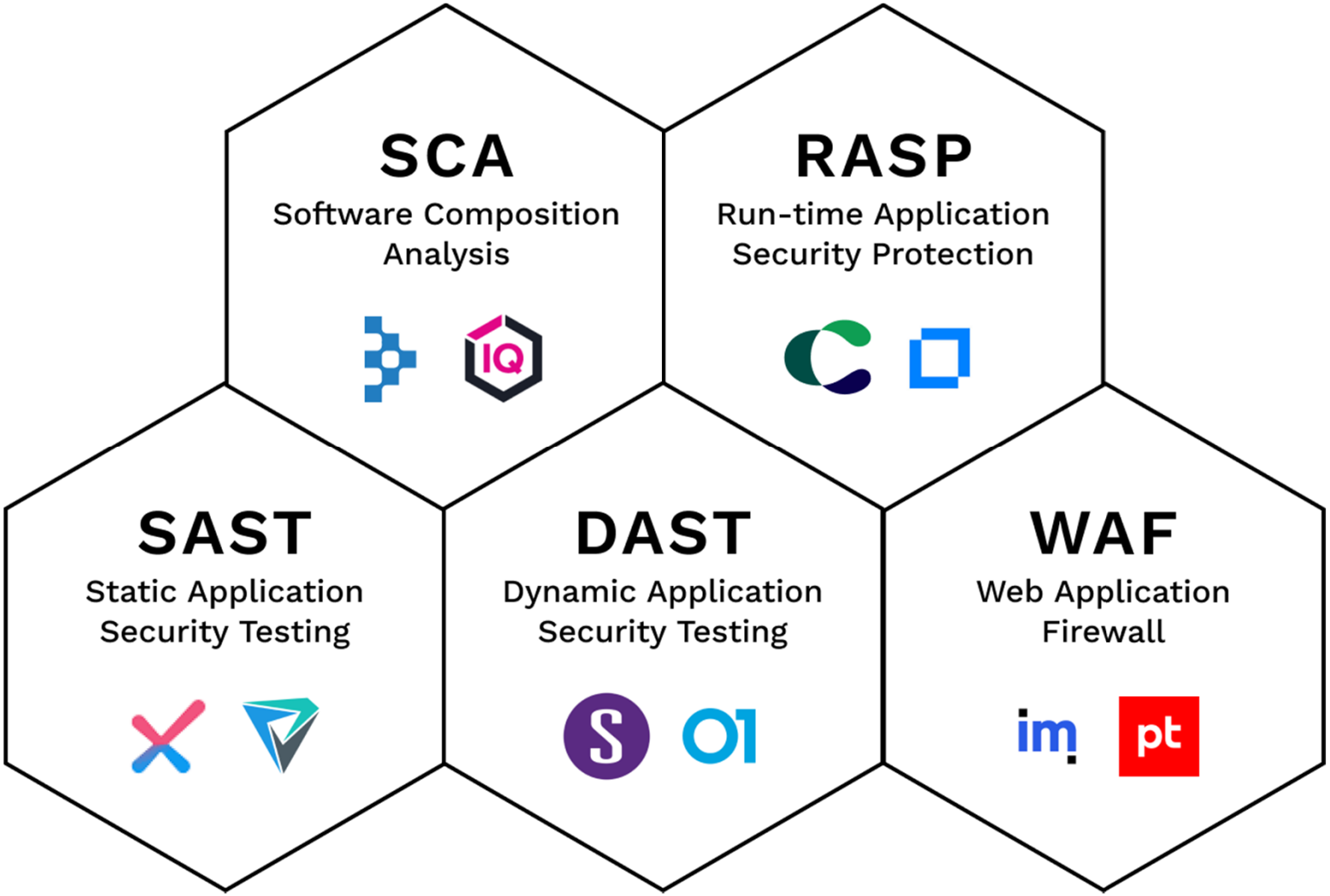
Что такое Shift-Left Security?

Shift-Left Security — внедрение проверок и практик безопасности в процессе SDLC так рано и так часто, как это возможно.

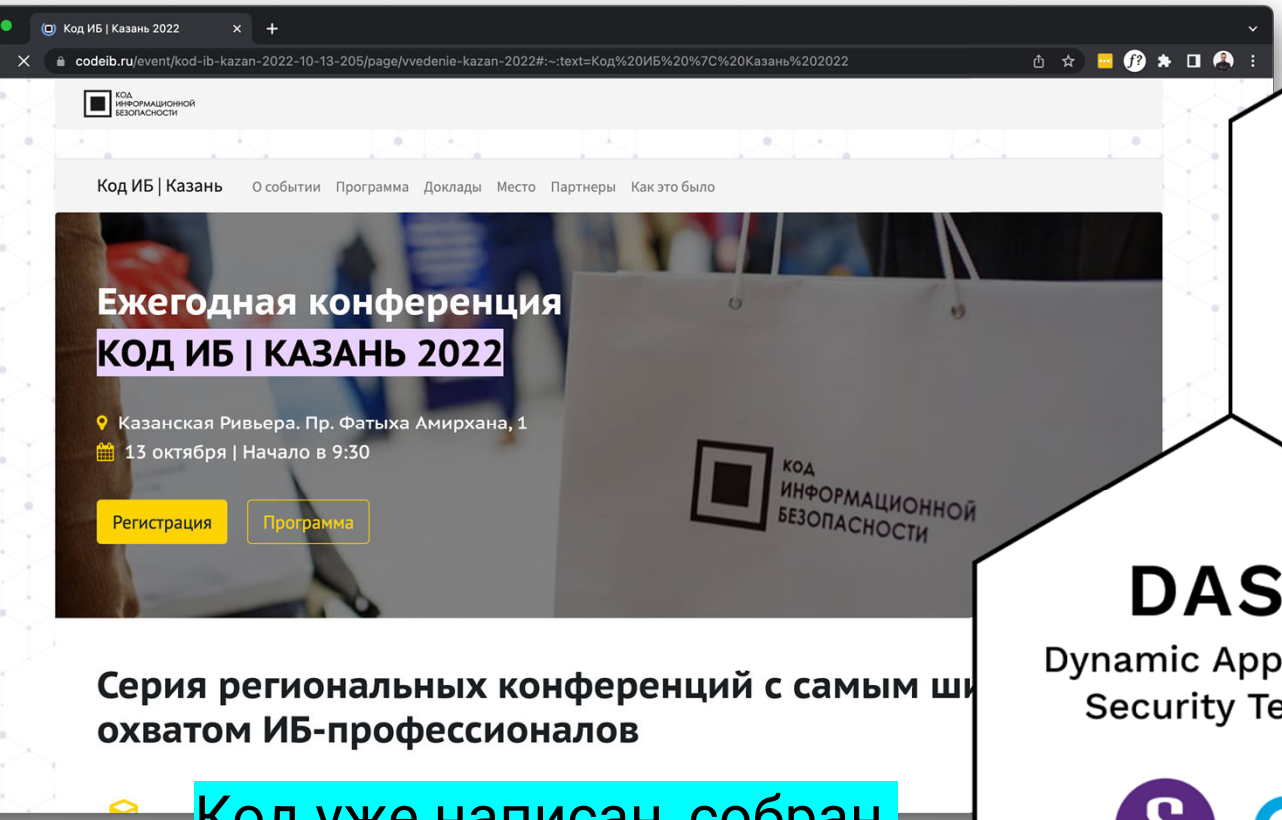
Устранение уязвимостей, выявленных как можно раньше в процессе разработки, значительно проще и обходится значительно дешевле

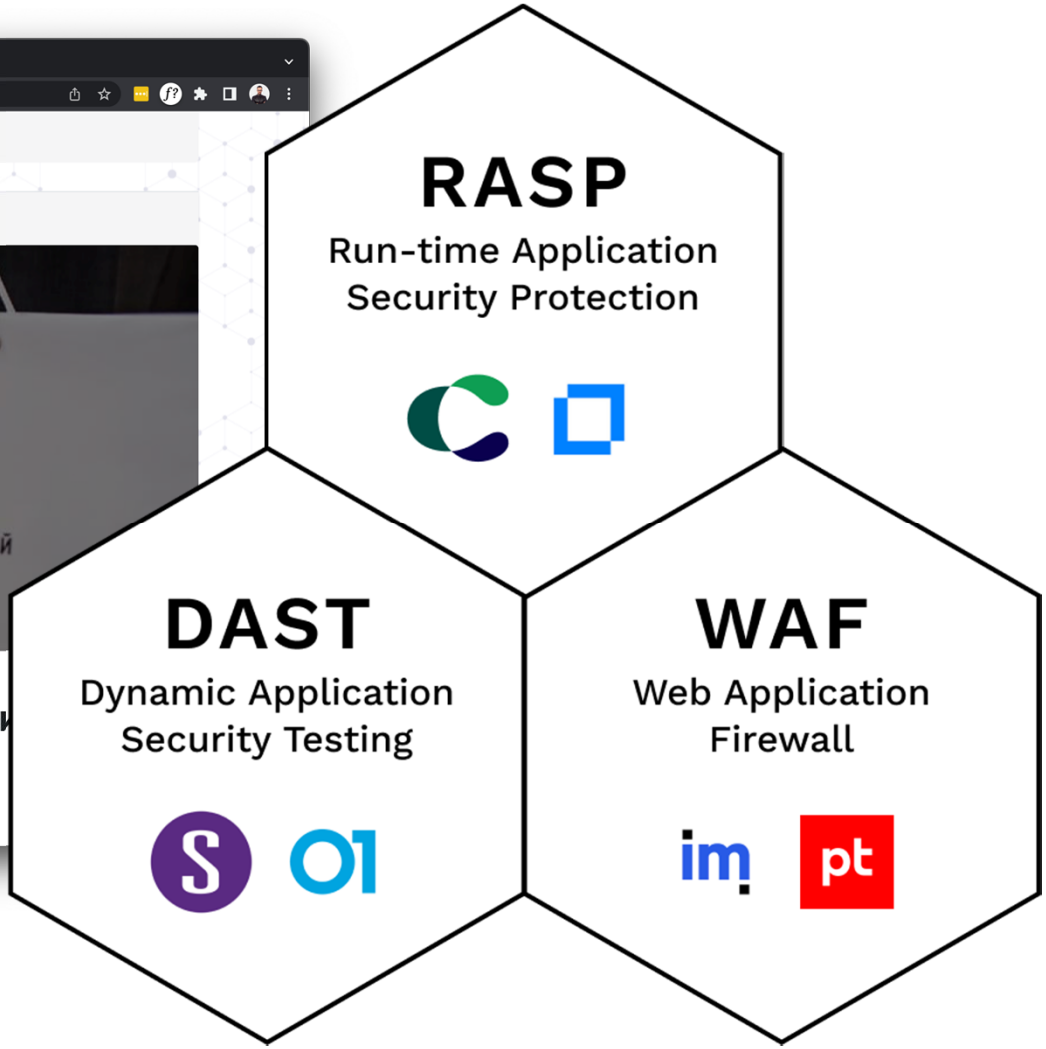


Какие инструменты делают продукт безопасным?

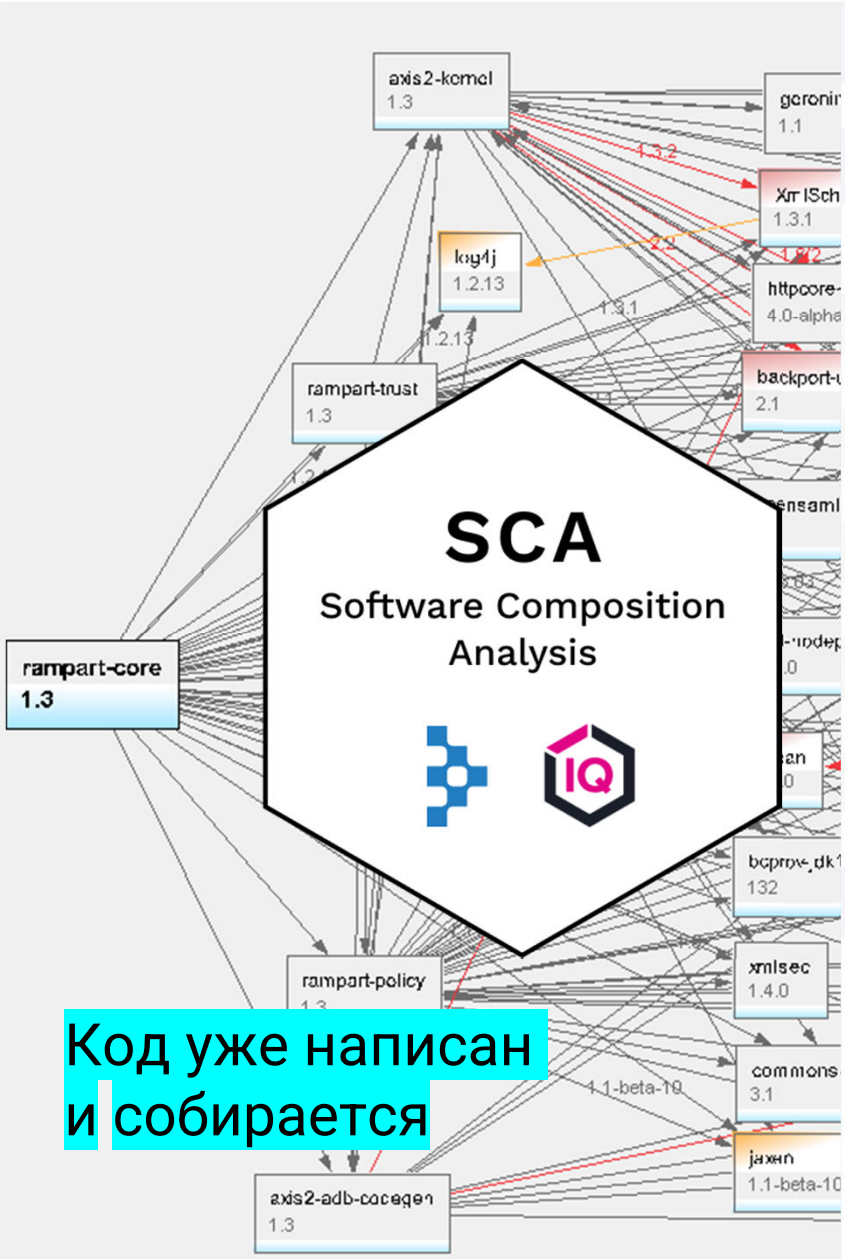


Какие инструменты делают продукт безопасным?





Код уже написан, собран и эксплуатируется



Код уже написан и собирается

Dashboard > Antiphish

Build History trend

Filter builds...

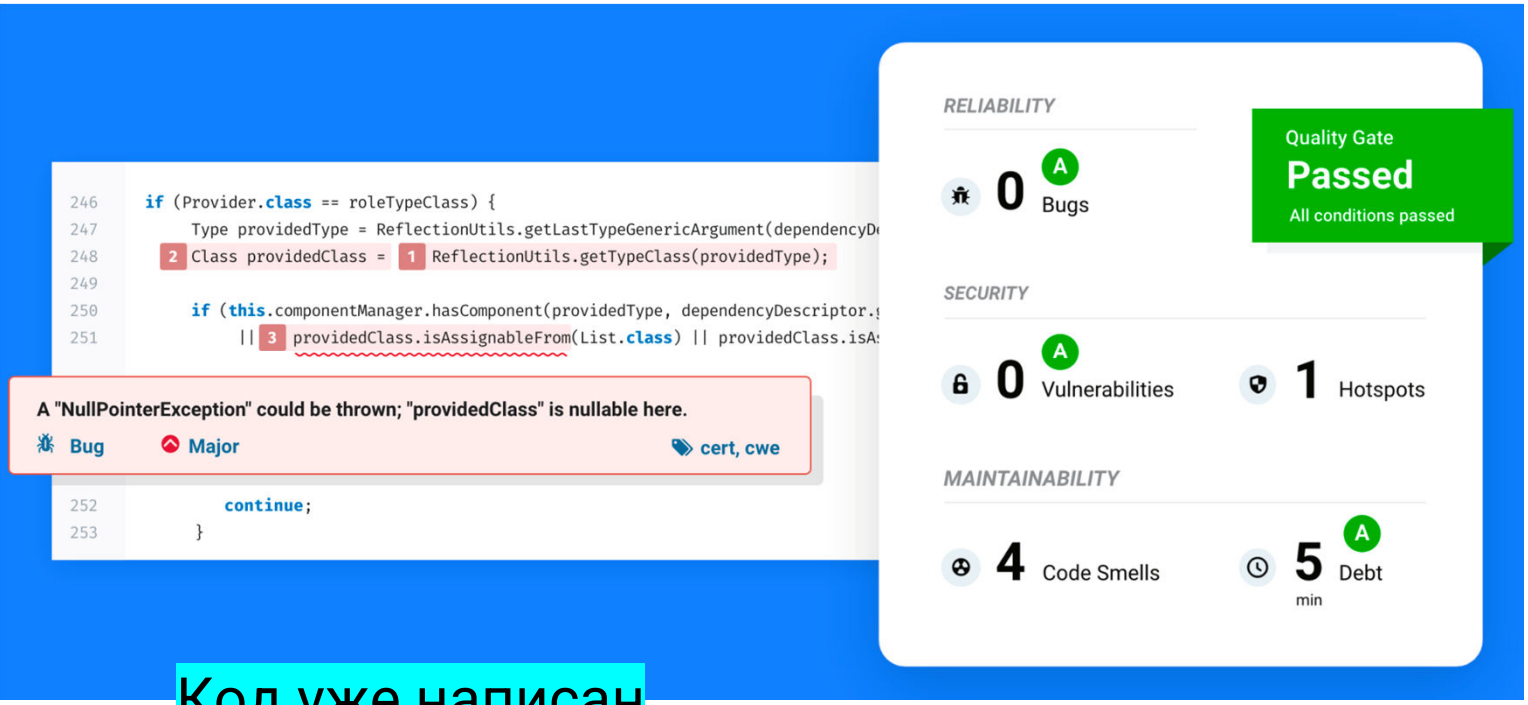
#649	28 Sep 2022, 15:03
#648	26 Sep 2022, 11:59
#647	26 Sep 2022, 11:41
#646	23 Sep 2022, 17:28
#645	23 Sep 2022, 16:38
#644	23 Sep 2022, 10:33
#643	22 Sep 2022, 18:08
#642	22 Sep 2022, 17:23
#641	22 Sep 2022, 15:36
#640	20 Sep 2022, 17:47

Atom feed for all Atom feed for failures

Stage View

	Checkout
Average stage times: (Average full run time: ~4min 46s)	52s
#649 Sep 28 15:03 — No Changes	21s
#648 Sep 26 11:59 — No Changes	59s
#647 Sep 26 11:41 — 3 commits	46s
#646 Sep 23 17:28 — 1 commit	54s
#645 Sep 23 16:38 — 4 commits	47s
#644 Sep 23 — 2	46s

Какие инструменты делают продукт безопасным?

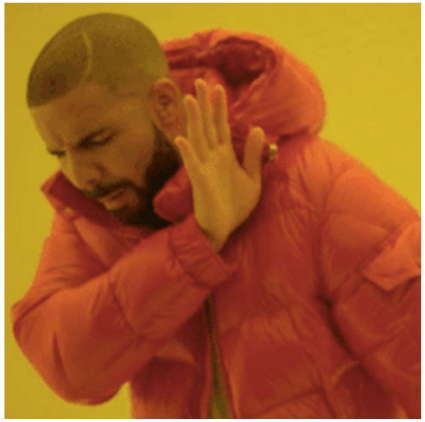


Код уже написан

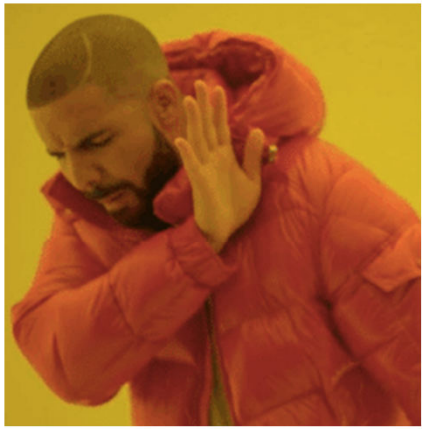
Что такое Shift-Left Security?

Планирование — Проектирование и дизайн — Реализация

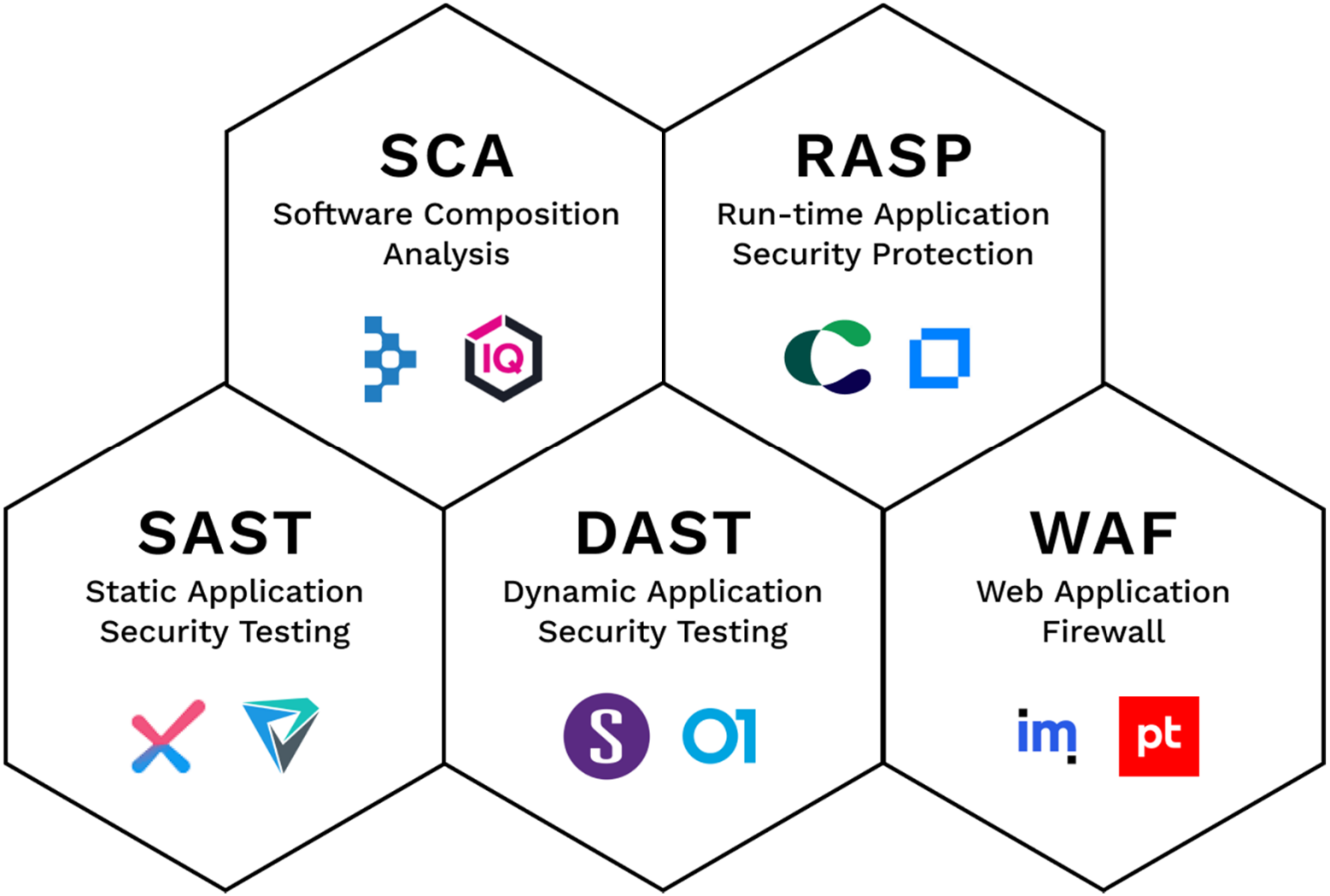
Тестирование — Эксплуатация



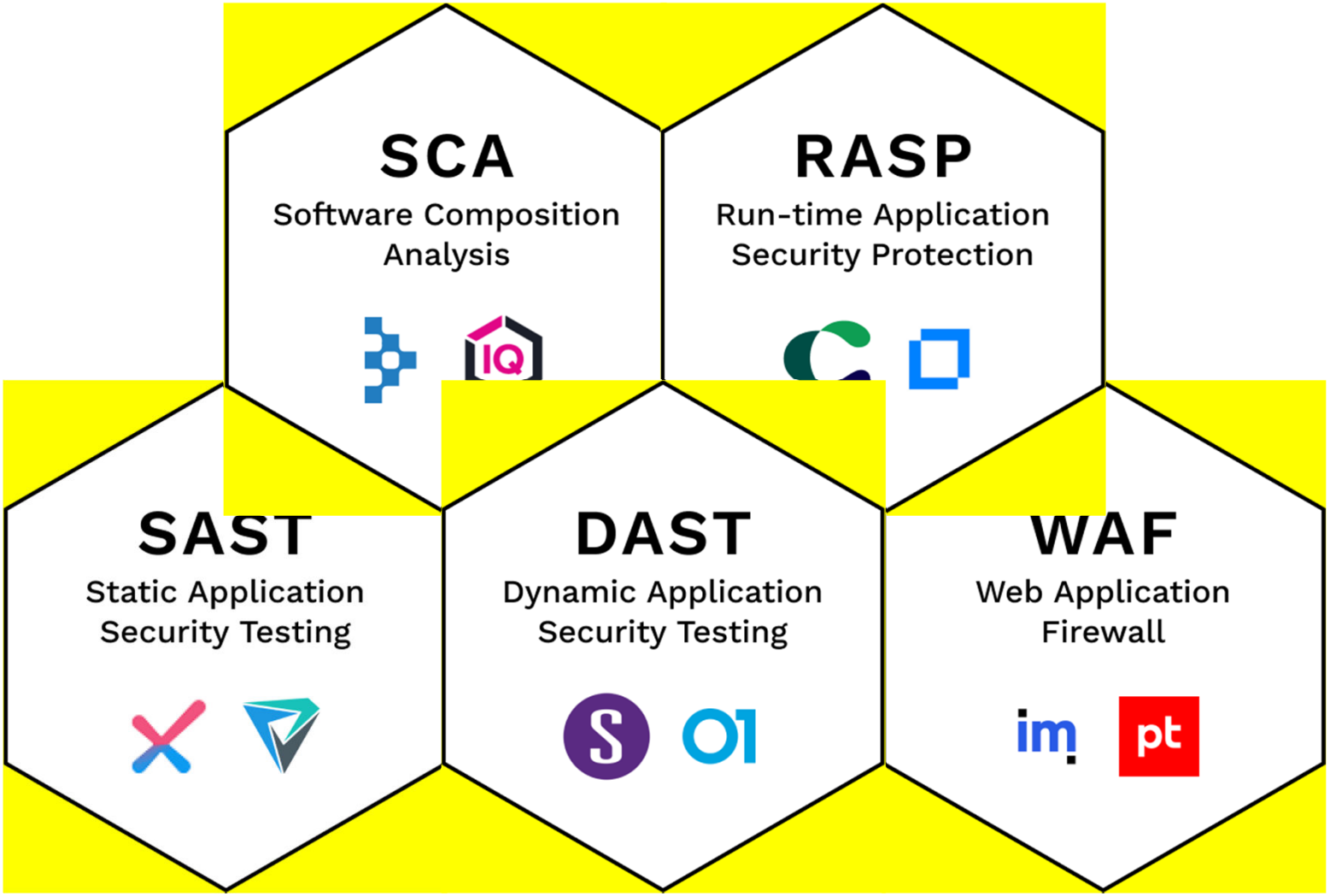
Относительная стоимость устранения дефектов ПО на разных этапах разработки



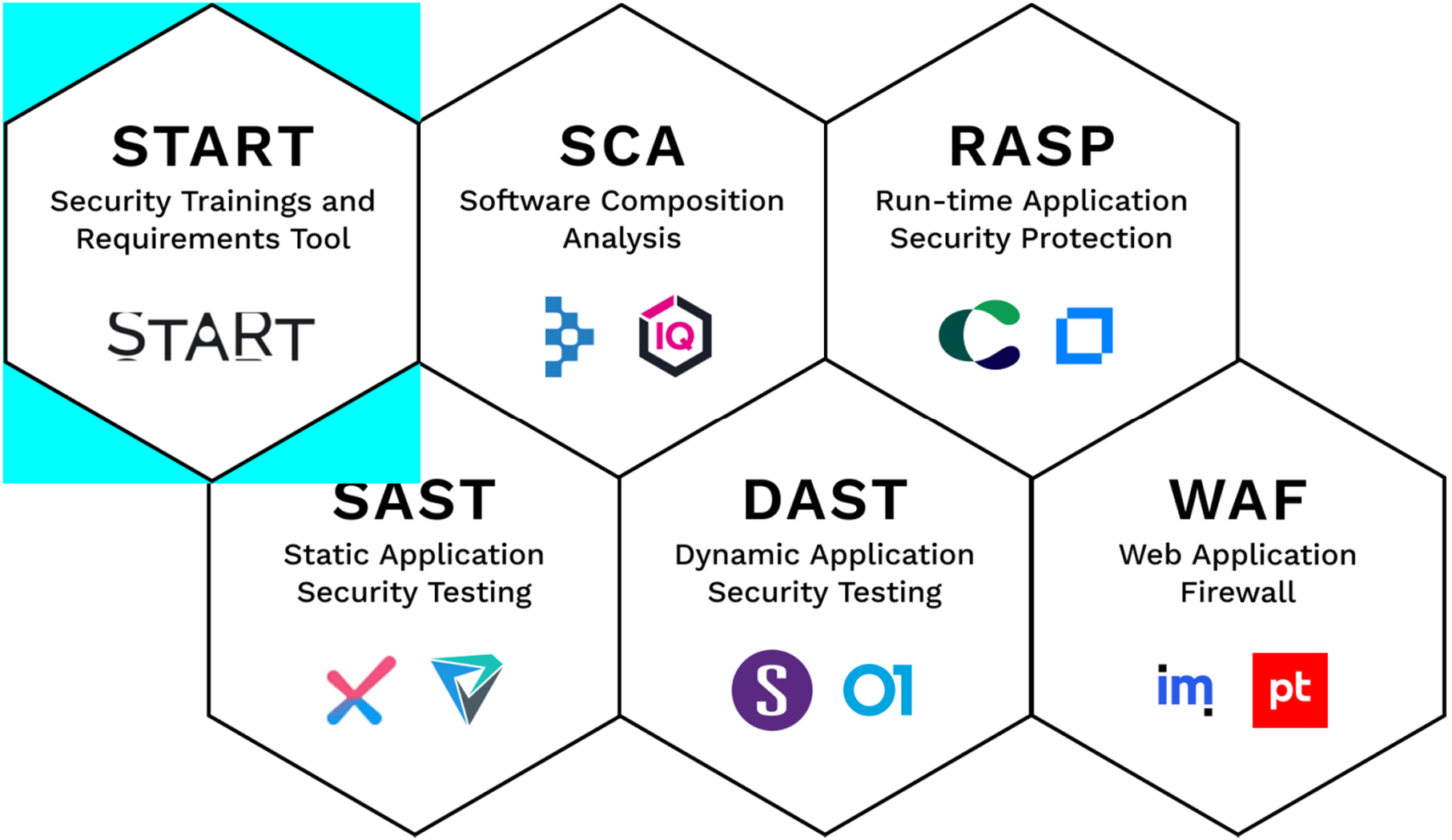
Какие инструменты делают продукт безопасным?



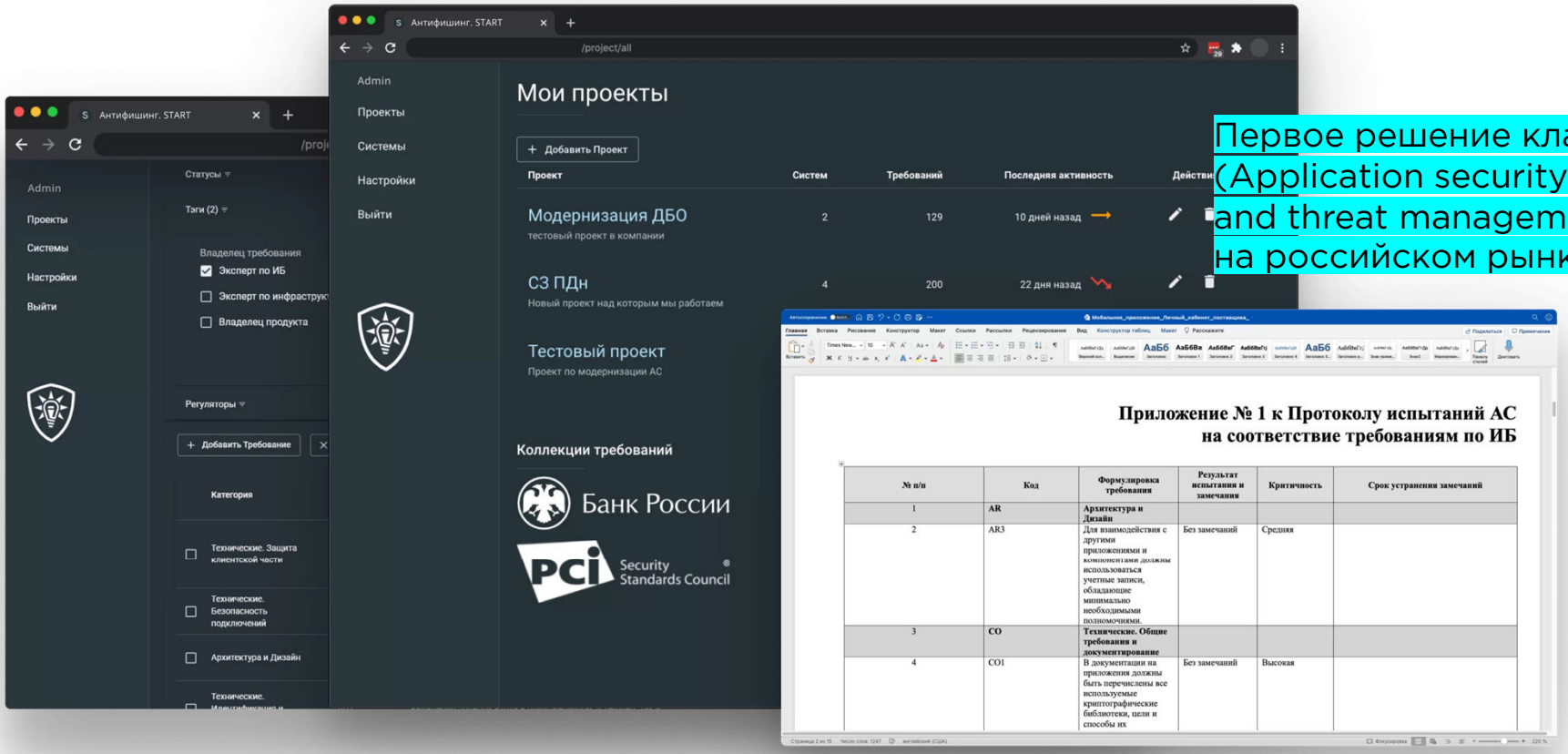
Инструменты не делают продукт безопасным



Люди делают продукт безопасным



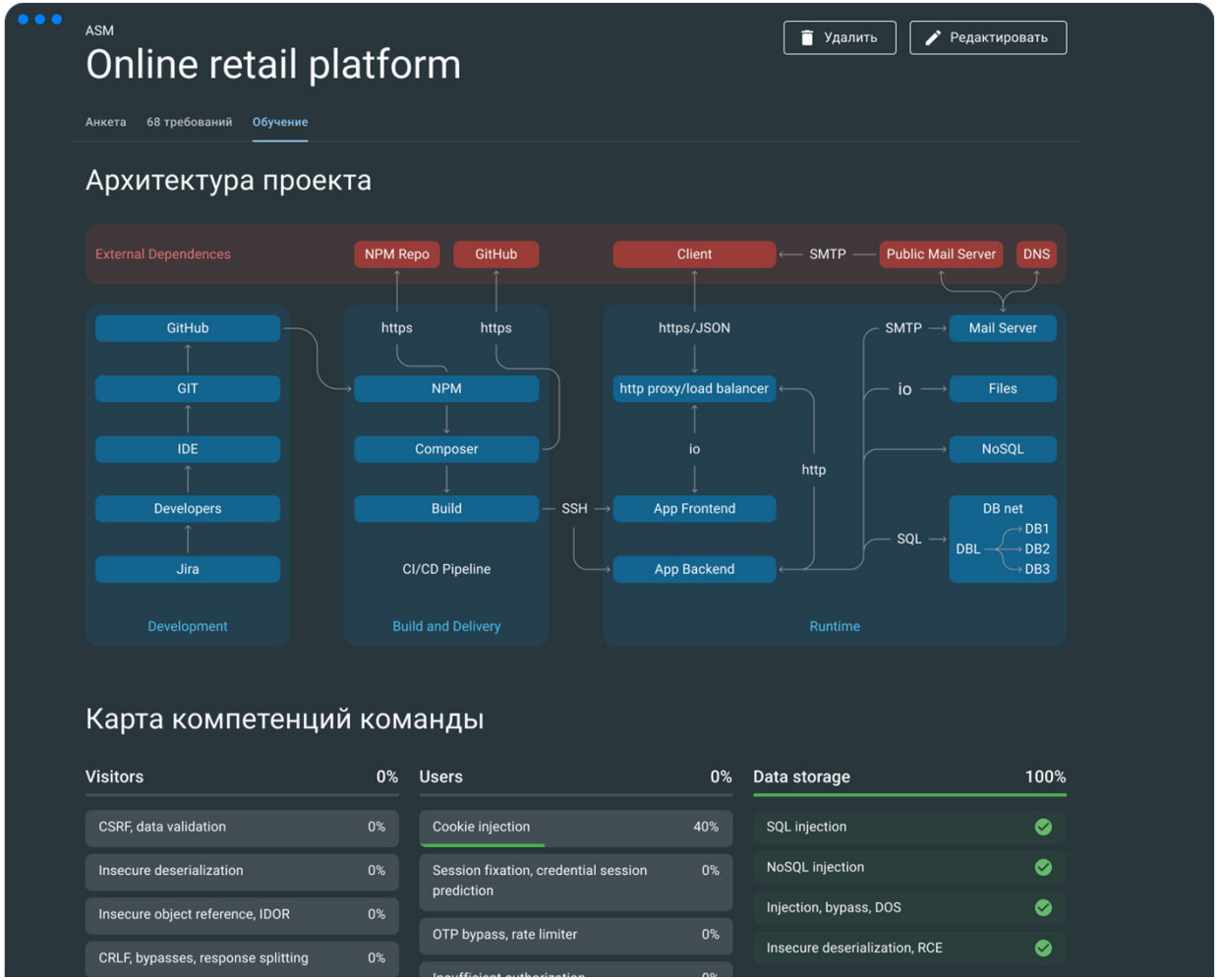
Антифишинг. START для продуктовых команд



Первое решение класса ASRTM (Application security requirements and threat management) на российском рынке.

Система для управления требованиями и знаниями по безопасности приложений, а также для обучения разработчиков ПО и продуктовых команд вопросам безопасной разработки.

Антифишинг. START. EDU — интерактивный модуль обучения для продуктовых команд



Jira

Строит карту проекта

Назначает только актуальные обучающие модули

Доставляет знания и навыки прямо в Jira

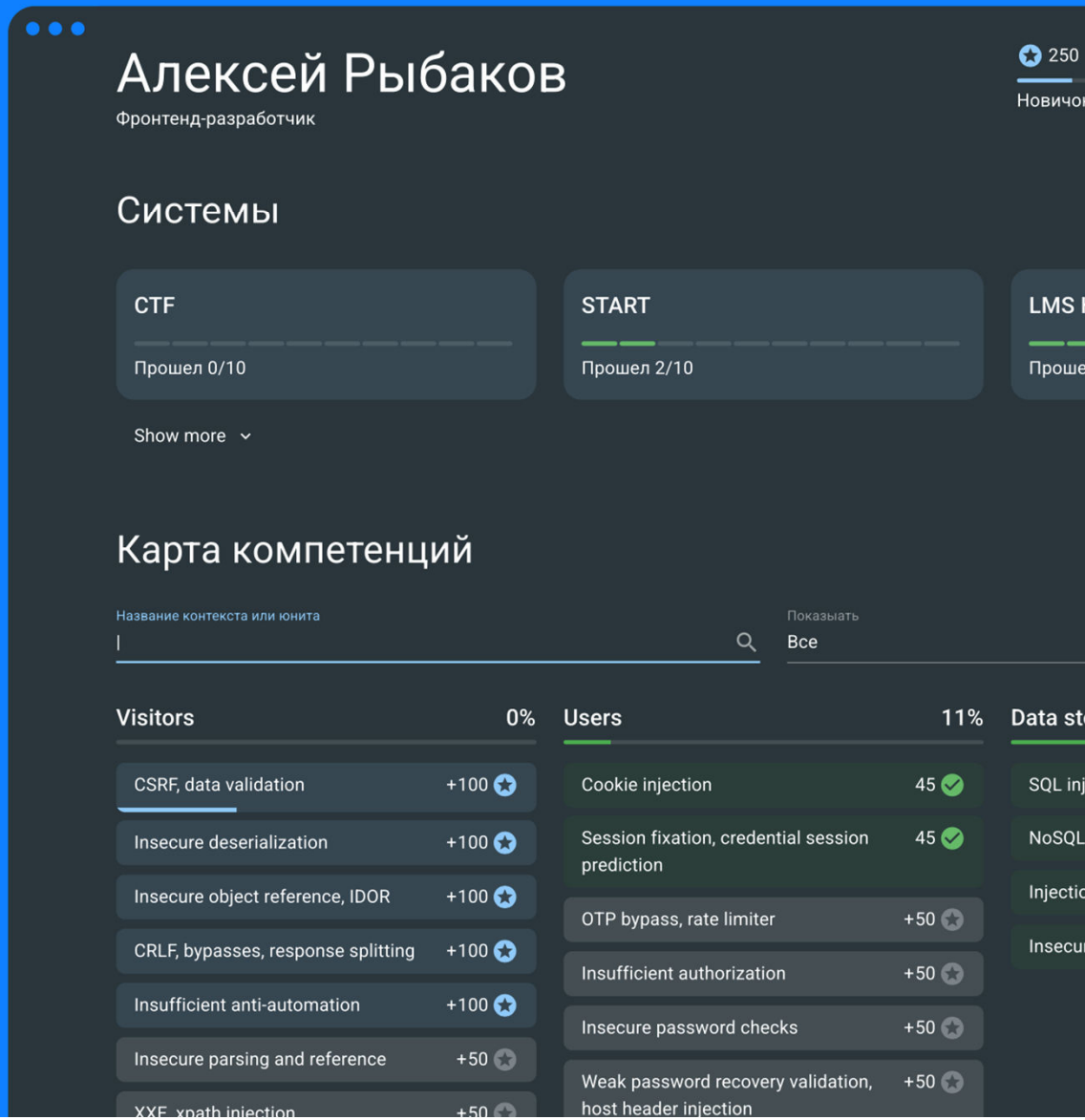
START.EDU

Модуль интерактивного обучения команд актуальным вопросам безопасной разработки в рамках продукта Антифишинг.START.

Платформа за 15 минут выявит навыки разработчиков через тестирование и автоматически составит матрицу их компетенций.

Каждому разработчику подбирается обучающий курс, согласно навыкам и текущим проектам, в которых он задействован.

START

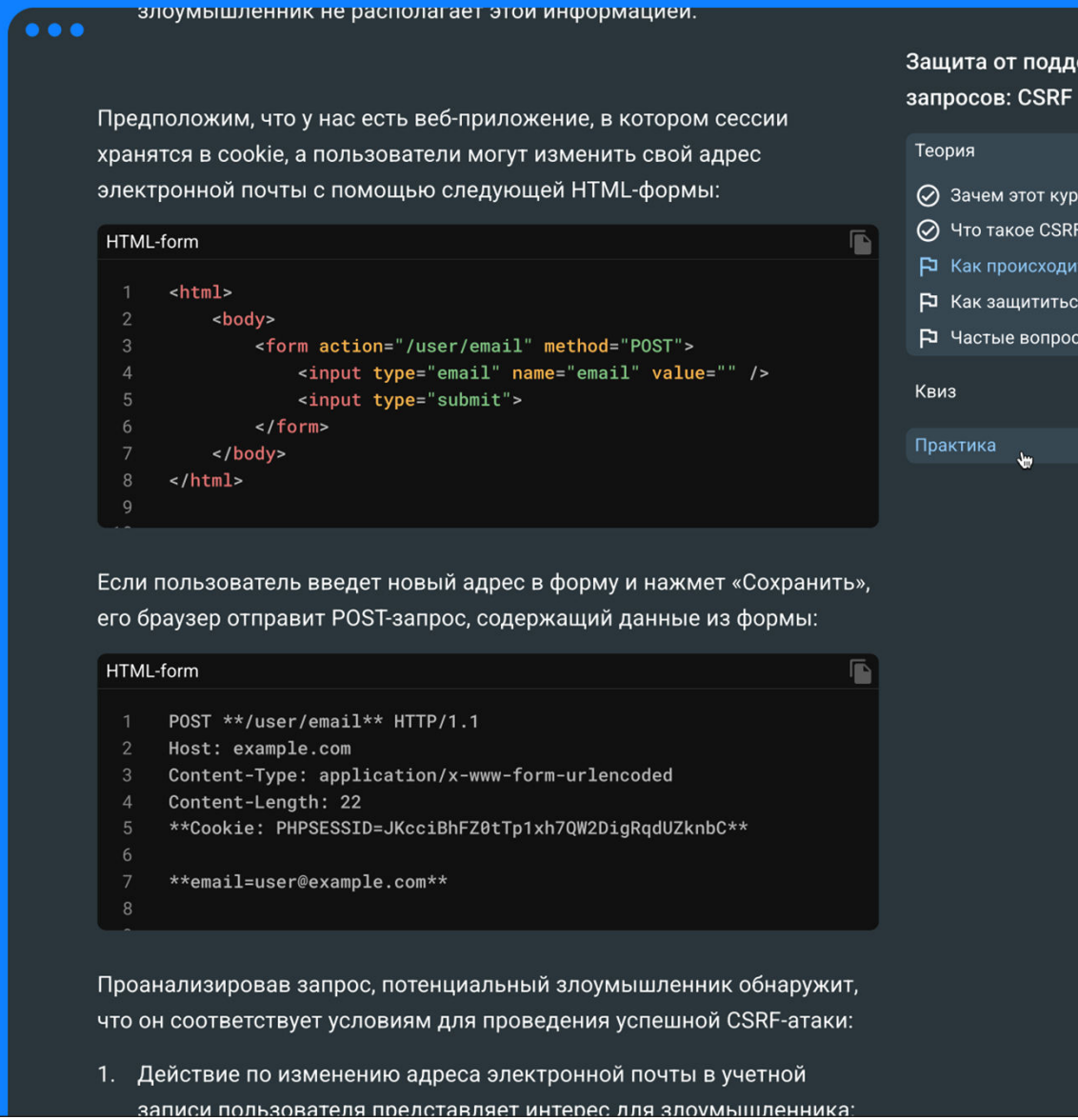


START.EDU

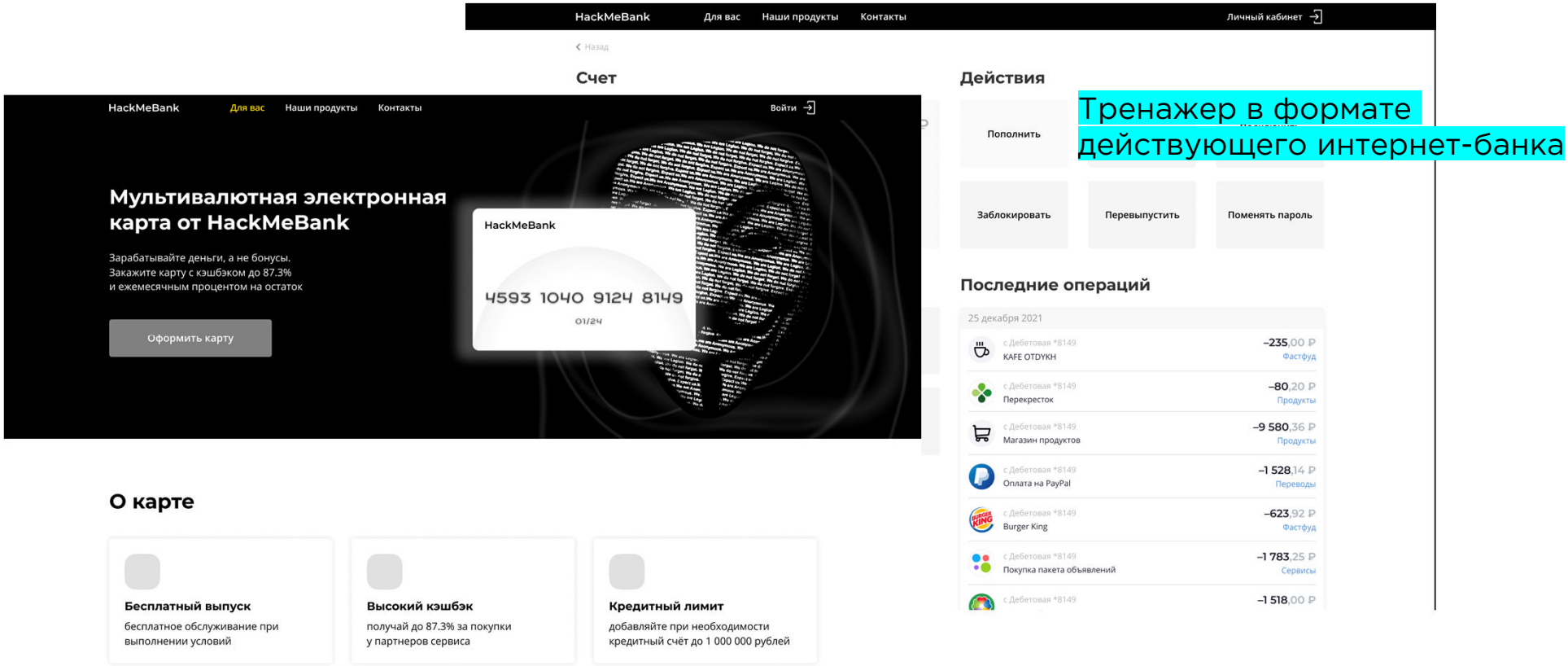
Каждый курс состоит из юнитов с актуальной теорией, обязательными примерами из реальной среды и проверочными заданиями, которые основаны на кейсах уязвимых приложений и помогают закрепить и проверить полученные знания.

Интеграция с JIRA синхронизирует обучение с другими рабочими процессами.

START



Антифишинг. START. CTF



Тренажер в формате действующего интернет-банка

Тренажер по практической безопасности в рамках Антифишинг. START.

START

CTF

Как вести безопасную разработку и создавать защищённые продукты

Используйте наши рекомендации, чтобы ваши процессы и продукты соответствовали лучшим практикам безопасной разработки

antiphish.ru/products/start

devsecops@antiphish.ru

Шаги по разработке защищенного продукта

1
Создайте собственный каталог требований

2
Использ
обеспеч
безопас
д

4
Делайте качественный код-ревью

5
Используйте CI-системы правильно

6
Примен
анализа
бственное
кение

8
Делайте автотесты и динамический анализ

9
Проводите ручное тестирование

10
Проводите внутренние пентесты

Повышайте квалификацию разработчиков

Продукты «Антифишинга» уже используют

www.antiphish.ru
ask@antiphish.ru

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

antiphish.ru/products/start