



Наливайте чай/кофе Скоро начинаем!

Начало вебинара в 12:00 (мск)

Rostelecom
Solar



Спикер вебинара



Сергей Деев

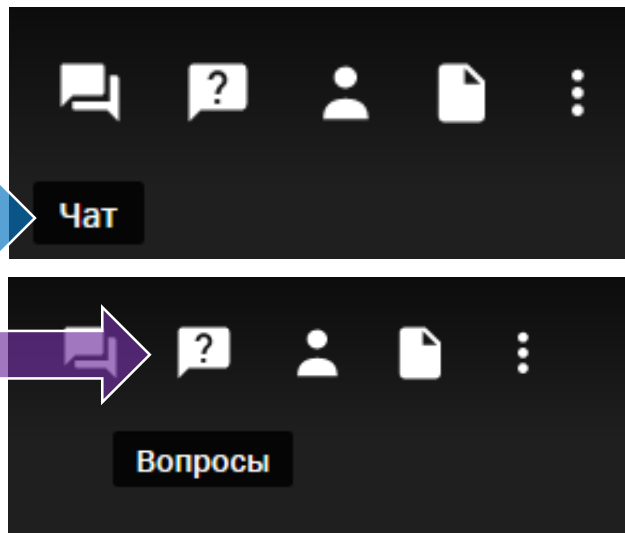
Менеджер продукта appScreener

Центр разработки решений по контролю
безопасности ПО «Ростелеком-Солар»

s.deev@rt-solar.ru

Организационные детали

- Длительность вебинара – **1 час**
- Если вы хотите пообщаться с другими участниками вебинара, **добро пожаловать в чат!**
- Свои вопросы спикерам мероприятия просьба задавать **в специальном разделе «Вопросы»**
- Запись вебинара, презентации спикеров и другие материалы будут отправлены участникам на указанные при регистрации email **в течение 2-3 дней после мероприятия**





Solar appScreener

Анализ кода приложений при
выполнении требований Банка
России 683-П и 684-П

Rostelecom
Solar

Деев Сергей

менеджер продукта appScreener

s.deev@rt-solar.ru



Сегодня мы поговорим...

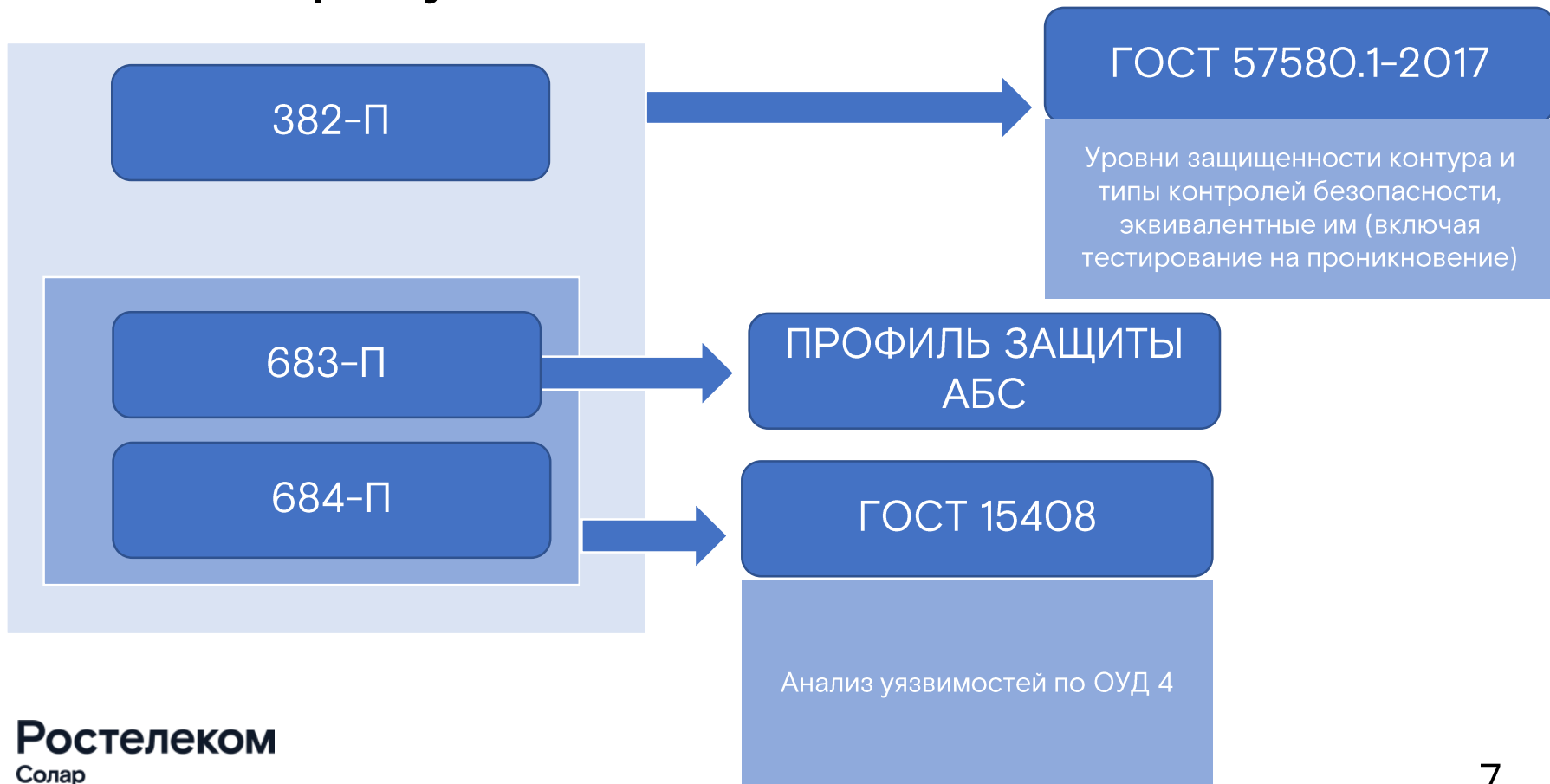
- О безопасности финансовых организаций: анализируем и разбираем ключевые аспекты
- Почему важен контроль безопасности в организациях финансового сектора?
- Что возможно выявить с помощью анализа кода?
- Об оценке ПО по ГОСТ Р ИСО/МЭК 15408 и сертификации на отсутствие НДВ
- Solar appScreener – современный инструмент анализа кода и выявления уязвимостей
- Ответим на ваши вопросы!



Роль требований регулятора в деятельности организаций по обеспечению ИБ



Роль НПА при аудите БР



Требования БР к безопасности



Организации, подотчетные БР



Банк России

683-П

684-П

Кредитные
организации

Некредитные
организации

Поставщик
Сертифици-
рованного
ПО

Поставщик
ПО

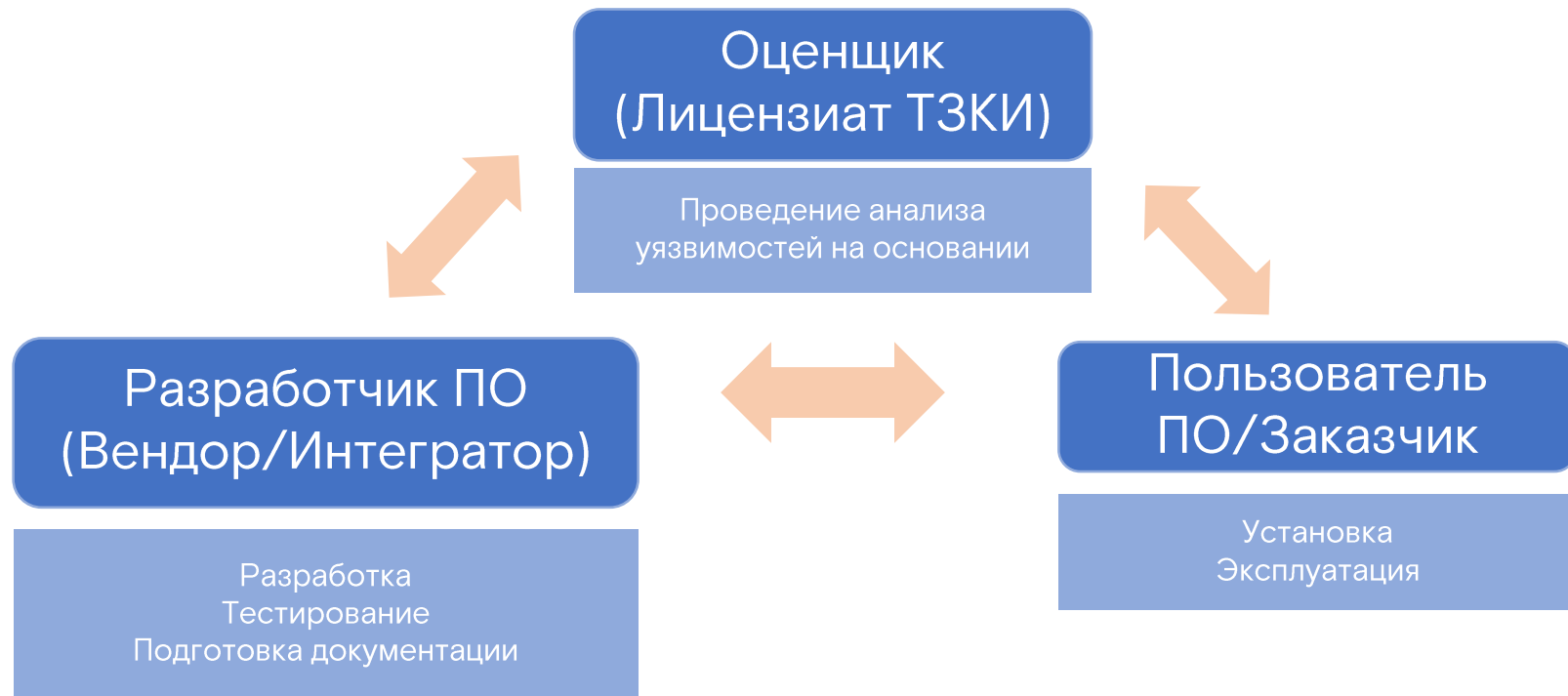
Лицензиат
ТЗКИ

Поставщик
ПО

Поставщик
Сертифици-
рованного
ПО

Ростелеком
Солар

Роли при оценке защищенности



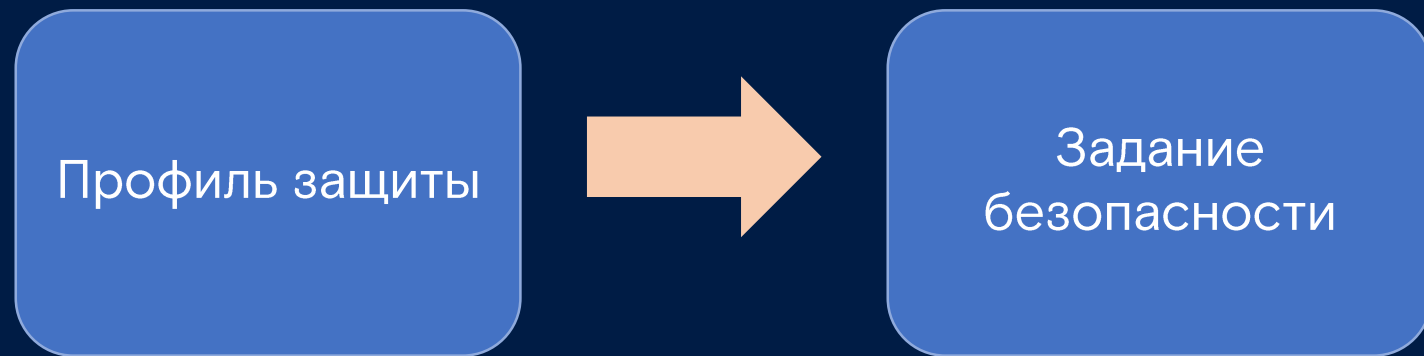
Что передает Разработчик для оценки

Описание
архитектуры
безопасности

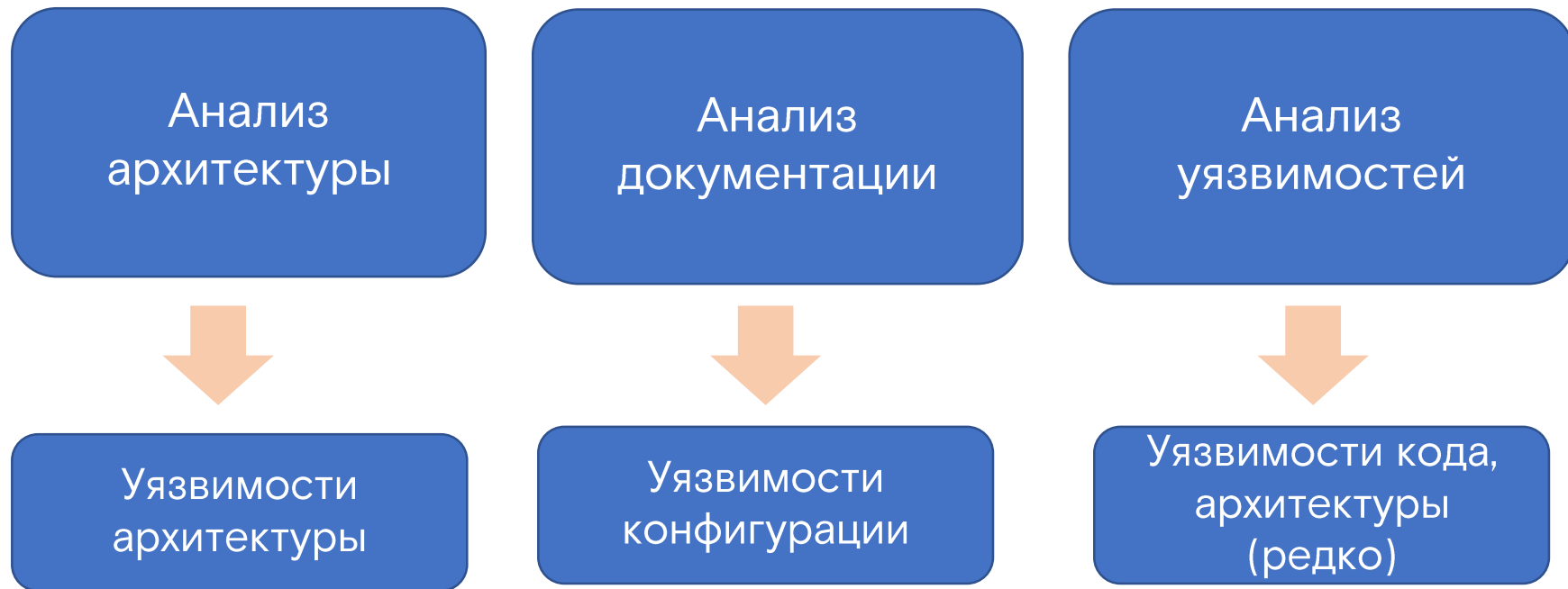
Пользовательску
ю и проектную
документацию

Исходный код,
экземпляр ПО

Описание архитектуры безопасности (выполняет разработчик ПО)

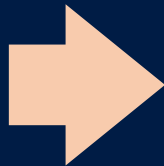


Типы контроля (Выполняет оценщик/Лицензиат ФСТЭК)



Критерии оценки

Функции
безопасности и
условия доверия



Оценочный
уровень доверия

Оценка по общим критериям

Классы требований к функциям безопасности (15408-2)

FAU (аудит безопасности)
FCO (связь)
FDP (защита данных пользователя)
FIA (идентификация и аутентификация)
FPR (секретность)
FPT (защита функций безопасности)
FRU (использование ресурса)
FTA (доступ к ОО)
FTP (надежный маршрут/канал)

Классы требований доверия (15408-3)

ACM (управление конфигурацией)
ADO (поставка и эксплуатация)
ADV (разработка)
AGD (руководства)
ALC (поддержка жизненного цикла)
ATE (тестирование)
AVA (оценка уязвимостей)

Оценочные уровни доверия

ОУД 1 – функционально проверенный проект

ОУД 2 – структурно проверенный проект

ОУД 3 – методически проверенный и оттестированный проект

ОУД 4 – методически разработанный и проверенный проект

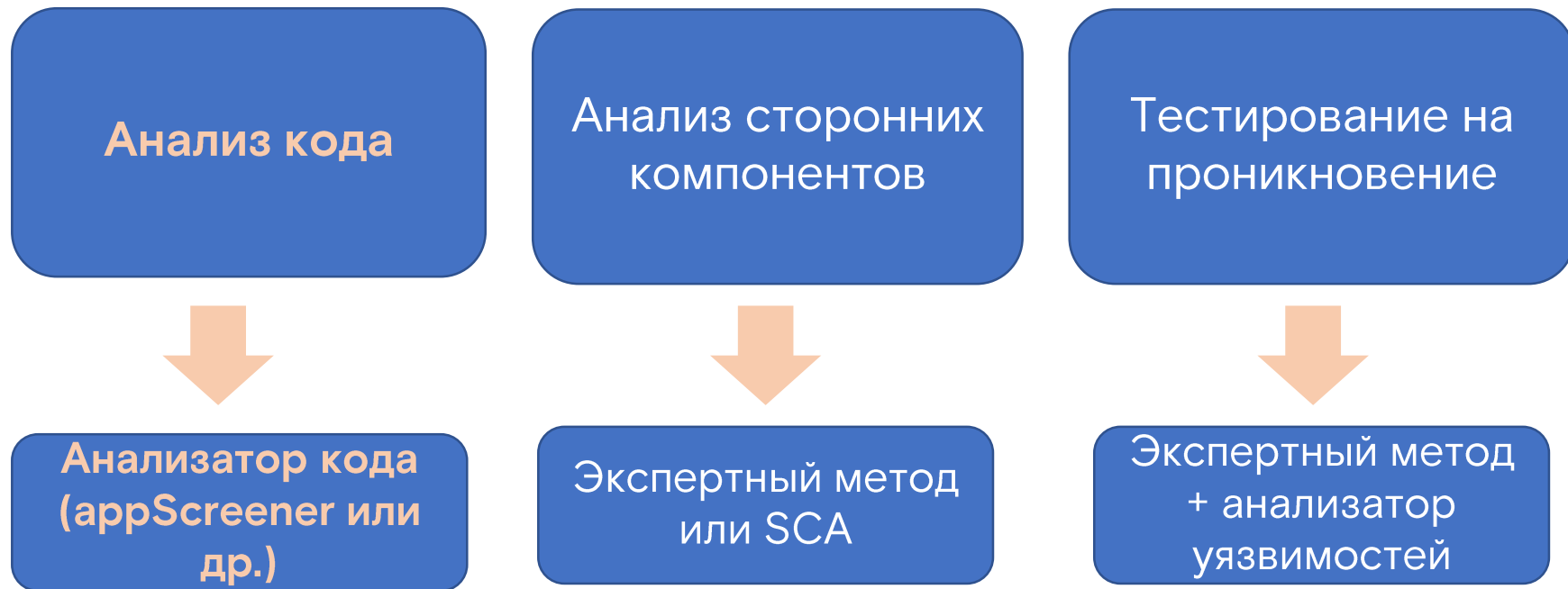
ОУД 5 – полужформально разработанный и проверенный проект

ОУД 6 – полужформально верифицированный и проверенный проект

ОУД 7 – формально верифицированный и проверенный проект

Анализ уязвимостей ПО

(Выполняет оценщик/Лицензиат ФСТЭК)

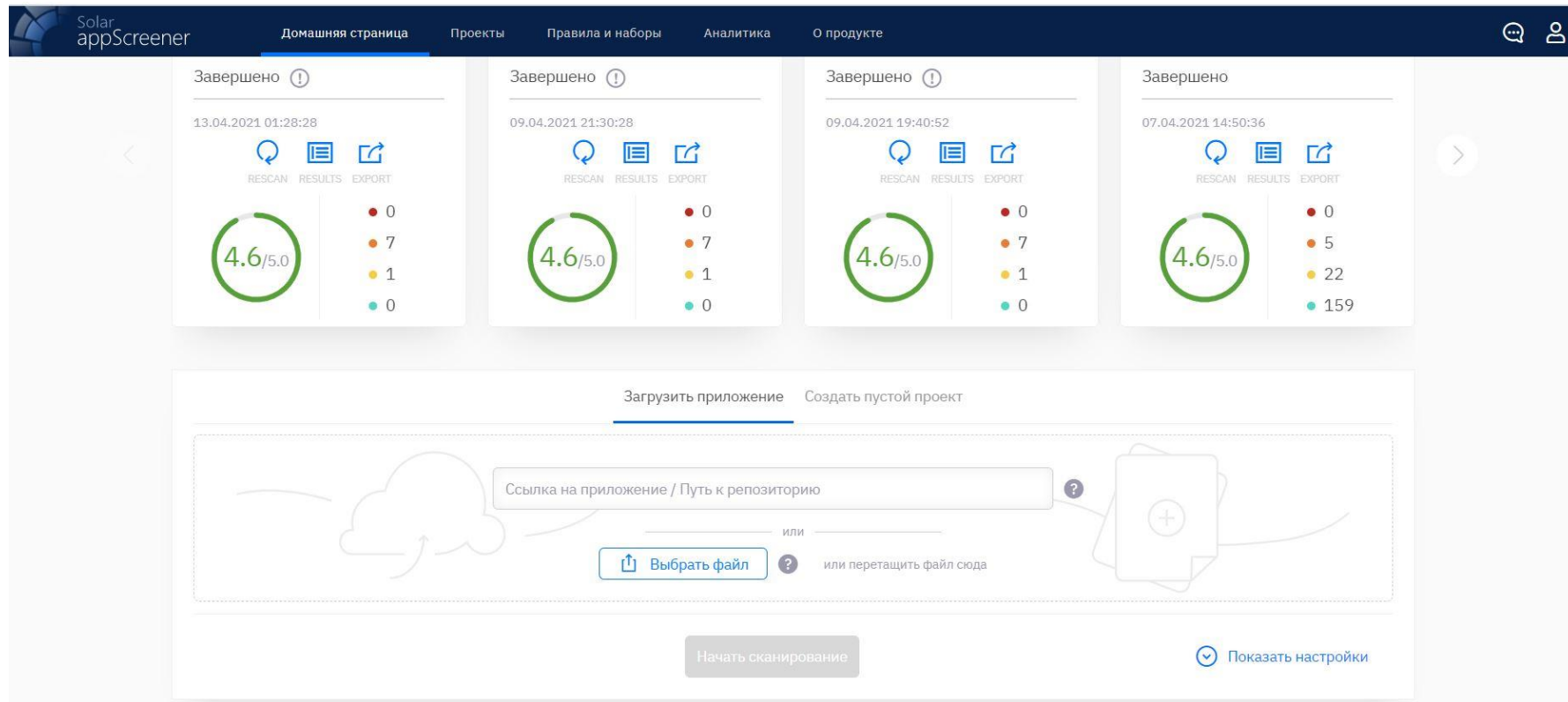


Роль статического анализа

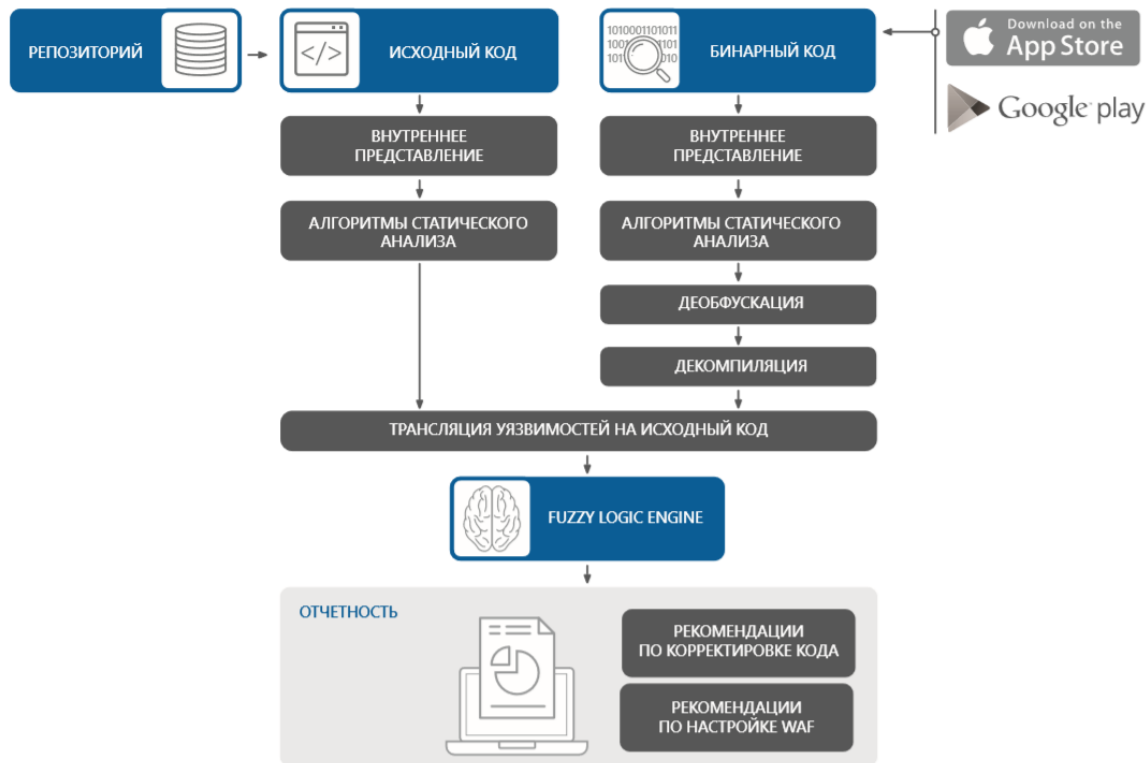
Ростелеком
Солар



Графический интерфейс



Принцип работы



Результаты анализа

Реализован в виде **веб-сервиса**. Соединение защищено с помощью протокола **HTTPS**

The screenshot displays the Solar appScreener web interface. The top navigation bar includes links for 'Домашняя страница', 'Проекты', 'Правила и наборы', 'Аналитика', and 'О продукте'. The left sidebar contains a menu with options like 'Обзор', 'Подобные результаты', 'Новое сканирование', 'Сканирования', 'Экспорт отчёта', 'Сравнение сканиваний', and 'Настройки'. The main content area shows the project 'integration.zip' with a summary of findings: 1714 total, 194 critical, 795 medium, 333 low, and 392 info. A list of vulnerabilities is shown, with 'HMAC со слабым алгоритмом хеширования' highlighted. The right panel displays the source code for 'integration/java8/JAVA_CRYPT0_BAD_HMAC.java:8', showing a Java class with a 'bad()' method that uses a weak HMAC algorithm. Below the code, there is a detailed description of the vulnerability in Russian, explaining that the application uses a weak HMAC algorithm for integrity checking, which can lead to data confidentiality loss.

integration.zip ID 70A3B2

Проекты > integration.zip > Подробные результаты

Всего 1714 Критический 194 Средний 795 Низкий 333 Инфо 392

Поиск по файлу и названию уязвимости

- Небезопасная собственная реализация SSL (пустой метод) 1
- HMAC со слабым алгоритмом хеширования 2**
- integration/j.../JAVA_CRYPT0_BAD_HMAC.java:8
- integration/j.../JAVA_CRYPT0_BAD_HMAC.java:9
- Внедрение в SQL-запрос 9
- Внедрение в XPath 3
- Внедрение внешней сущности в XML 19
- Десериализация недоверенных данных 6
- Ключ шифрования задан в исходном коде 16
- Манипулирование политикой безопасности

integration/java8/JAVA_CRYPT0_BAD_HMAC.java:8

```
3 import javax.crypto.KeyGenerator;
4 import java.security.NoSuchAlgorithmException;
5
6 public class JAVA_CRYPT0_BAD_HMAC {
7     public void bad() throws NoSuchAlgorithmException {
8         KeyGenerator.getInstance("HmacSHA1"); //@ JAVA_CRYPT0_BAD_HMAC-cbh000
9         KeyGenerator.getInstance("HmacMD5"); //@ JAVA_CRYPT0_BAD_HMAC-cbh000
10    }
11
12    public void good() throws NoSuchAlgorithmException {
13        KeyGenerator.getInstance("HmacSHA512");
14    }
15}
```

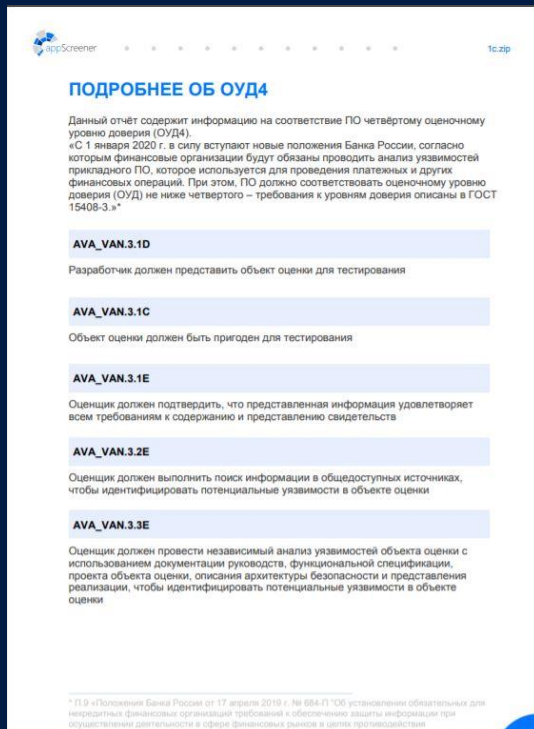
Описание уязвимости | Пример | Рекомендации | Ссылки | Классификации | Трасса | Управлен

Приложение использует метод проверки подлинности HMAC со слабым алгоритмом хеширования. Его использование может привести к утрате конфиденциальности данных.

В криптографии HMAC (сокращение от англ. hash-based message authentication code, код проверки подлинности сообщений, использующий односторонние хеш-функции) - один из механизмов проверки целостности информации, использующий секретный ключ и хеш-функцию.

Криптографическая стойкость HMAC зависит от криптографической стойкости используемой хеш-функции, от длины и качества секретного ключа, от размера выходного значения алгоритма.

Отчет по ОУД4

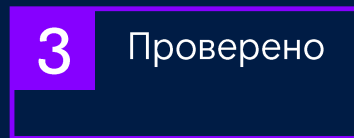
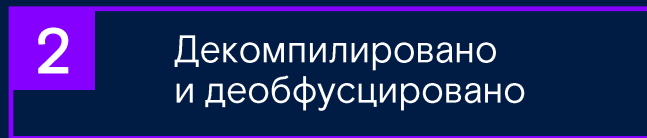
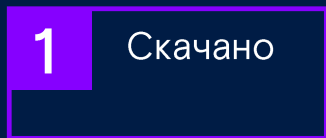


Анализ бинарного кода – 9 форматов файлов

Для мобильных приложений достаточно **скопировать ссылку** из Google Play или App Store



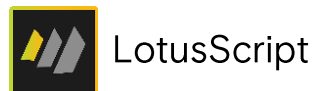
Приложение будет **автоматически**:



Анализ исходного кода – 36 языков



Ростелеком
Солар



COBOL

Microsoft
VBScript

appScreener соответствует требованиям к отечественному ПО

1

Включен
в Единый реестр
отечественного ПО

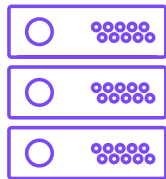


2

Проходит
сертификацию
ФСТЭК России



Лицензирование и поставка



Установка на собственный сервер (On-premise)

- Лицензирование осуществляется по количеству пользователей, которые имеют доступ к системе
- Подходит при необходимости постоянного анализа ПО (крупные вендоры и компании)



Сервис из облака «Ростелеком-Солар» (SaaS)

- Оплачивается количество произведенных проверок
- Подходит, если потребность в проверке приложений возникает время от времени (небольшие вендоры, использование заказного ПО, «перестраховка»)

Возможности интеграции

Репозитории



VCS-хостинги



Средства разработки



Средства сборки



Серверы CI/CD



Отслеживание задач



Анализ кода



Открытый API предоставляет широкие возможности по дополнительной интеграции и автоматизации. Включает в себя **JSON API** и **CLI**

Гибкая настройка выводимых результатов об уязвимостях

Подробные результаты

Всего	Критический	Средний	Низкий	Инфо
8	0	7	1	0

Поиск по файлу и названию уязвимости

☒ FUZZY LOGIC ENGINE

Mode
Только истинные

Критические high confidence low confidence

Средние high confidence low confidence

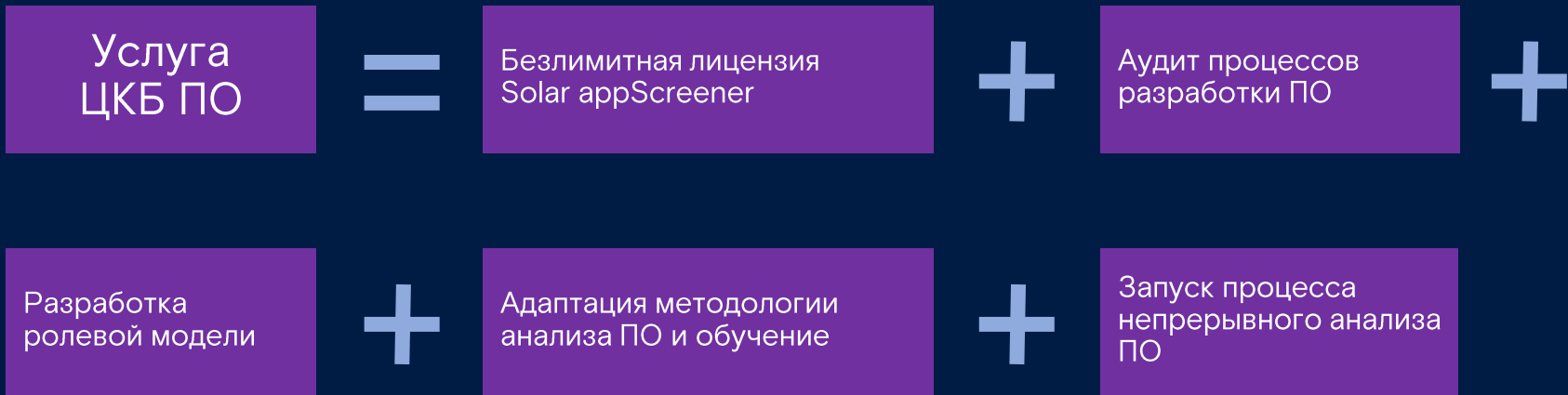
Низкие high confidence low confidence

Информационные

Применить

Контроль безопасности ПО как часть безопасности организации

На основе Solar appScreener можно реализовывать проекты по внедрению практик безопасной разработки. Отдельным примером таких практик может служить построение Центра контроля безопасности ПО (ЦКБ ПО)



Попробуй Solar appScreener!



The screenshot displays the Solar appScreener web application interface. The top navigation bar includes the logo and links for "Домашняя страница", "Проекты", "Правила и наборы", "Аналитика", and "О продукте". The sidebar on the left contains navigation options: "Обзор", "Подробные результаты", "Сканирования", "Экспорт отчёта", "Сравнение сканирований", and "Настройки". The main content area is divided into three sections. The left section shows project details for ID 7F5020, including a table of results: "Всего 420" and "Критический 46". The center section features a large QR code. The right section displays a code editor with a snippet of Java code and a summary of findings, including a note about authentication bypass and OWASP Top 10 2014 vulnerabilities.

Top Navigation Bar:

- Solar appScreener
- Домашняя страница
- Проекты
- Правила и наборы
- Аналитика
- О продукте

Sidebar:

- Обзор
- Подробные результаты
- Сканирования
- Экспорт отчёта
- Сравнение сканирований
- Настройки

Main Content Area:

Left Panel (Project Details):

- Проекты >
- Всего 420
- Критический 46
- Поиск по файлу и названию
- FUZZY LOGIC ENGINE
- Mode: Только истинные
- Критические: high confidence
- Средние: high confidence
- Низкие: high confidence
- Информационные: high confidence
- Перцентиль

Center Panel (QR Code):

Right Panel (Code Editor and Results):

```
InjectionChallenge.java:51
ibaseUtilities.getConnection(webSession);

lect userid from " + USERS_TABLE_NAME + " where
:tion.createStatement();
ment.executeQuery(checkUserQuery);

.feedback("user.exists").feedbackArgs(username_
redStatement = connection.prepareStatement("INSI
```

Navigation Links: Ссылки, Классификации, Трасса, Управление

Findings Summary:

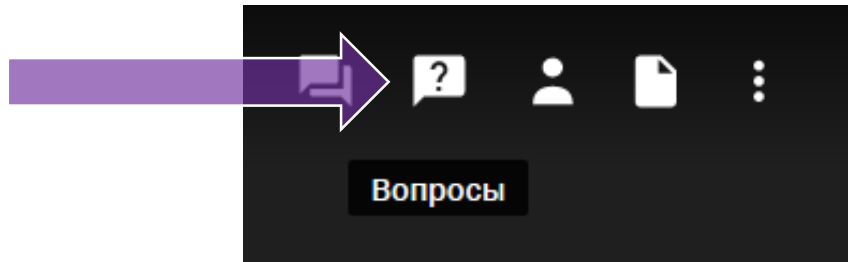
- ит обойти механизм аутентификации, получить доступ код с правами приложения.
- сто в рейтинге уязвимостей web-приложений «OWASP e Top 10 2014». Уровень возможного ущерба от такой ввода и механизмов защиты файлов.
- нных формируется на основе данных из ненадёжного лем). При отсутствии правильной валидации

Как возможно познакомиться с решением?

1. Получить доступ к демостенду Solar appScreener, написав на presale@rt-solar.ru
2. Совместно оценить потребности организации в анализе кода
3. Инициировать **пилотный проект**
4. Успешно **реализовать пилот**



Ваши вопросы?



Сергей Деев
Менеджер продукта appScreener

s.deev@rt-solar.ru

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru



Ростелеком
Солар

