Ростелеком
Солар

Современные подходы к контролю безопасности ПО:

от минимального набора мер (для среднего уровня компаний) до глубокой экспертизы (для крупных организаций)

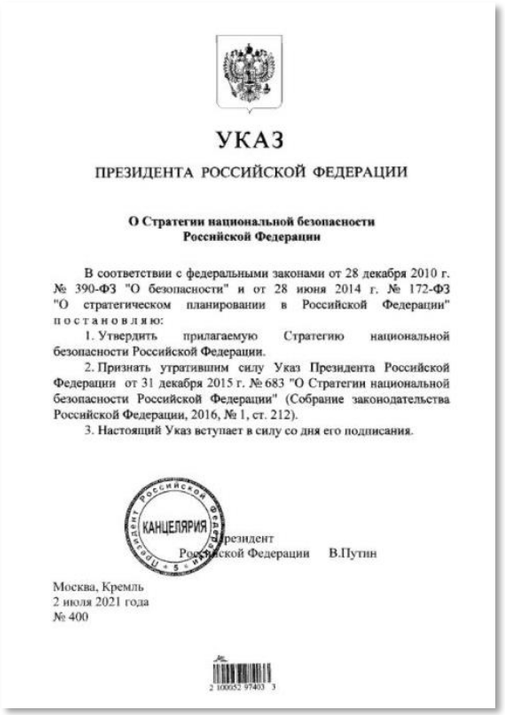
Деев Сергей
Менеджер продукта Solar appScreener

Ростелеком
Солар

Актуальность вопроса анализа безопасности ПО

Мировое информационное пространство создает новые вызовы для ИТ-инфраструктуры РФ

Угрозы о проведении возможных атак на инфраструктуру РФ уже звучат на публичных трибунах из уст руководителей других стран.



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О Стратегии национальной безопасности Российской Федерации

В соответствии с федеральными законами от 28 декабря 2010 г. № 390-ФЗ "О безопасности" и от 28 июня 2014 г. № 172-ФЗ "О стратегическом планировании в Российской Федерации" п о с т а н о в л я ю:

1. Утвердить прилагаемую Стратегию национальной безопасности Российской Федерации.

2. Признать утратившим силу Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации" (Собрание законодательства Российской Федерации, 2016, № 1, ст. 212).

3. Настоящий Указ вступает в силу со дня его подписания.

КАНЦЕЛЯРИЯ

Президент Российской Федерации В.Путин

Москва, Кремль
2 июля 2021 года
№ 400

The New York Times

Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China

The proliferation of cyberattacks by rivals is presenting a challenge to the Biden administration as it seeks to deter intrusions on government and corporate systems.

Мировая обстановка обостряется. При этом формируются новые виды ведения боевых действий, которые теперь могут затрагивать ИТ-инфраструктуры противников.

Ростелеком Солар

В РФ определены требования к обеспечению ИБ организаций электроэнергетики

Для ОКИИ

187ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

Приказ ФСТЭК N239

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" января 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Приказ Минэнерго N1015

Министерство энергетики Российской Федерации
(Минэнерго России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 53815
от "15" февраля 2019 г.

ПРИКАЗ

6 ноября 2018 г. № 1015

Москва

Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования

В соответствии с подпунктом «б» пункта 1 постановления Правительства Российской Федерации от 2 марта 2017 г. № 244 «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты Правительства Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 11, ст. 1562; 2018, № 34, ст. 5483) п р и к а з ы в а ю:

1. Утвердить прилагаемые требования в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования.

2. Настоящий приказ вступает в силу по истечении шести месяцев со дня его официального опубликования.

Министр А.В. Новак

Департамент оперативного контроля и управления в электроэнергетике
Медведева Елена Анатольевна
(495) 631-08-71

Для АСУ ТП

Приказ ФСТЭК N31

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 31919
от "10" июня 2014 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ПРИКАЗ

«14» марта 2014 г. Москва № 31

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137), **П Р И К А З Ы В А Ю:**

Утвердить прилагаемые Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Ростелеком Солар

Устоявшиеся меры по обеспечению ИБ в организациях

I этап
Аудит ИС и процессов в организации

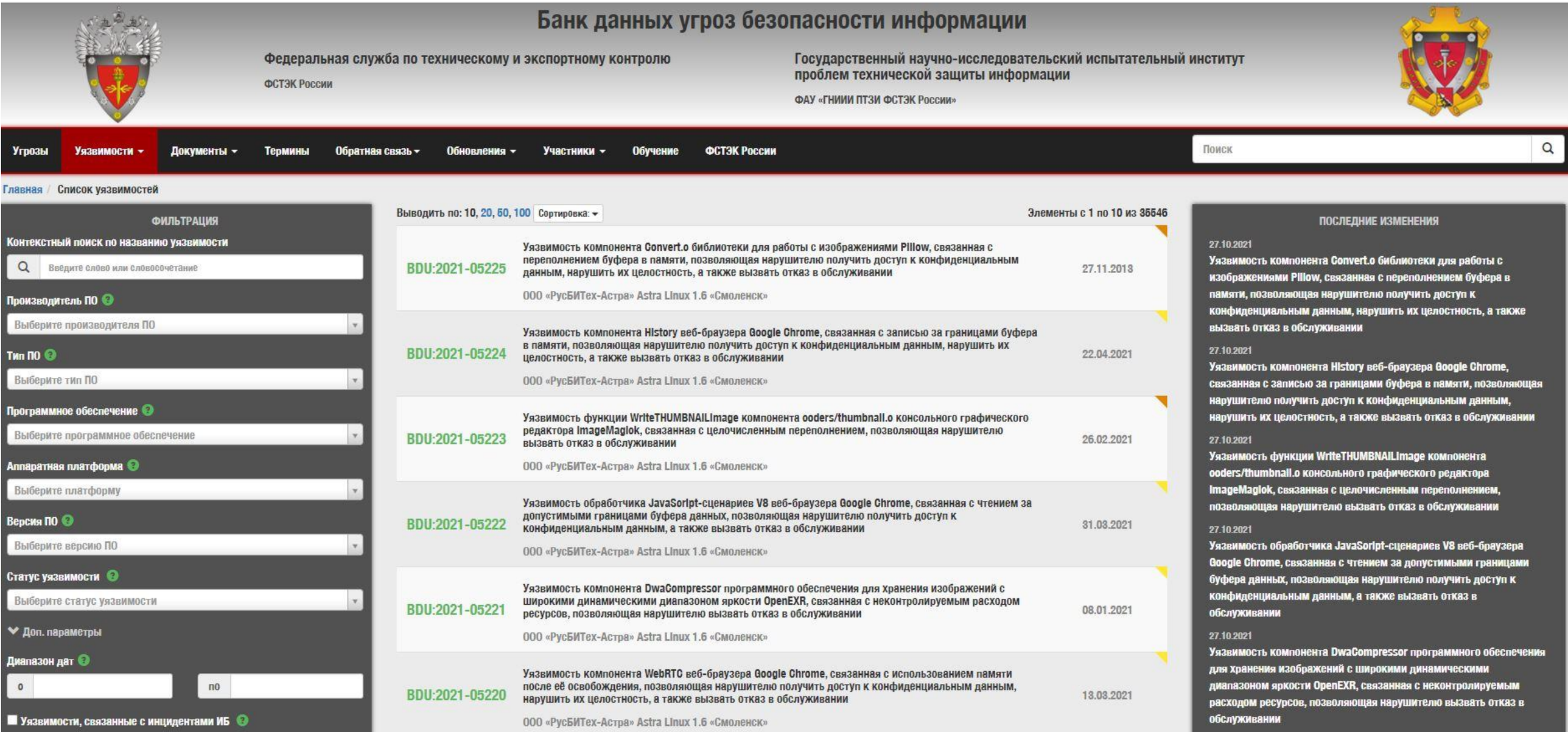
II этап

- Моделирование угроз и формирование рекомендаций по их нейтрализации
- Формирование перечня мер по обеспечению ИБ

III этап
Построение и ввод в эксплуатацию подсистемы защиты информации

Ростелеком Солар

Информация об уязвимостях в ПО БДУ ФСТЭК



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Документы | Термины | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Поиск

Главная / Список уязвимостей

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО

Выберите производителя ПО

Тип ПО

Выберите тип ПО

Программное обеспечение

Выберите программное обеспечение

Аппаратная платформа

Выберите платформу

Версия ПО

Выберите версию ПО

Статус уязвимости

Выберите статус уязвимости

Доп. параметры

Диапазон дат

с

по

Уязвимости, связанные с инцидентами ИБ

Выводить по: 10, 20, 50, 100 Сортировка:

Элементы с 1 по 10 из 35546

BDU:2021-05225	Уязвимость компонента Convert.o библиотеки для работы с изображениями Pillow, связанная с переполнением буфера в памяти, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	27.11.2013
BDU:2021-05224	Уязвимость компонента History веб-браузера Google Chrome, связанная с записью за границами буфера в памяти, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	22.04.2021
BDU:2021-05223	Уязвимость функции WriteTHUMBNAILImage компонента ooders/thumbnail.o консольного графического редактора ImageMaglok, связанная с целочисленным переполнением, позволяющая нарушителю вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	26.02.2021
BDU:2021-05222	Уязвимость обработчика JavaScript-сценариев V8 веб-браузера Google Chrome, связанная с чтением за допустимыми границами буфера данных, позволяющая нарушителю получить доступ к конфиденциальным данным, а также вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	31.03.2021
BDU:2021-05221	Уязвимость компонента DwaCompressor программного обеспечения для хранения изображений с широкими динамическими диапазоном яркости OpenEXR, связанная с неконтролируемым расходом ресурсов, позволяющая нарушителю вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	08.01.2021
BDU:2021-05220	Уязвимость компонента WebRTC веб-браузера Google Chrome, связанная с использованием памяти после её освобождения, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании ООО «РусБИТех-Астра» Astra Linux 1.6 «Смоленск»	13.03.2021

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

27.10.2021
Уязвимость компонента Convert.o библиотеки для работы с изображениями Pillow, связанная с переполнением буфера в памяти, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании

27.10.2021
Уязвимость компонента History веб-браузера Google Chrome, связанная с записью за границами буфера в памяти, позволяющая нарушителю получить доступ к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании

27.10.2021
Уязвимость функции WriteTHUMBNAILImage компонента ooders/thumbnail.o консольного графического редактора ImageMaglok, связанная с целочисленным переполнением, позволяющая нарушителю вызвать отказ в обслуживании

27.10.2021
Уязвимость обработчика JavaScript-сценариев V8 веб-браузера Google Chrome, связанная с чтением за допустимыми границами буфера данных, позволяющая нарушителю получить доступ к конфиденциальным данным, а также вызвать отказ в обслуживании

27.10.2021
Уязвимость компонента DwaCompressor программного обеспечения для хранения изображений с широкими динамическими диапазоном яркости OpenEXR, связанная с неконтролируемым расходом ресурсов, позволяющая нарушителю вызвать отказ в обслуживании

Меры по обеспечению ИБ в ИС

Меры по обеспечению ИБ

Построение подсистемы защиты информации

Анализ защищенности ИС и ПО

Ростелеком Солар

Анализ защищенности

Анализ защищенности ПО
(объект оценки: ПО)

Поиск уязвимостей в ПО:

- **Статический анализ кода**
- Динамический анализ кода (включая фаззинг-тестирование)
- Поиск уязвимостей в сторонних компонентах кода на основе данных из открытых источников
- Верификация выявленных и известных уязвимостей в ПО

Анализ защищенности ИС
(объект оценки: ИС)

Оценка инфраструктуры на наличие:

- Известных уязвимостей в компонентах используемого ПО
- Уязвимостей в веб-интерфейсах доступных сервисов (методом черного ящика)
- Уязвимостей конфигурации в серверном и сетевом ПО и оборудовании

Ростелеком Солар

Ростелеком
Солар

Нормативно-правовые предпосылки анализа безопасности ПО

Требования 239 Приказа ФСТЭК России к применяемым СЗИ, вступающие в силу с 1 января 2023 года.

«28. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся **субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций**, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.»

Ростелеком Солар

Требования 239 Приказа ФСТЭК России к применяемому ПО, вступающие в силу с 1 января 2023 года.

«29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее - программное обеспечение), должно соответствовать следующим требованиям по безопасности:
29.3.1. Требования по безопасной разработке программного обеспечения:
наличие руководства по безопасной разработке программного обеспечения ... (и прочих документов)
29.3.2. Требования к испытаниям по выявлению уязвимостей в программном обеспечении:
проведение статического анализа исходного кода программы ... (и прочих проверок иными методами).
29.3.3. Требования к поддержке безопасности программного обеспечения:
наличие процедур отслеживания и исправления обнаруженных ошибок ... (и прочих процедур, с этим связанных).»

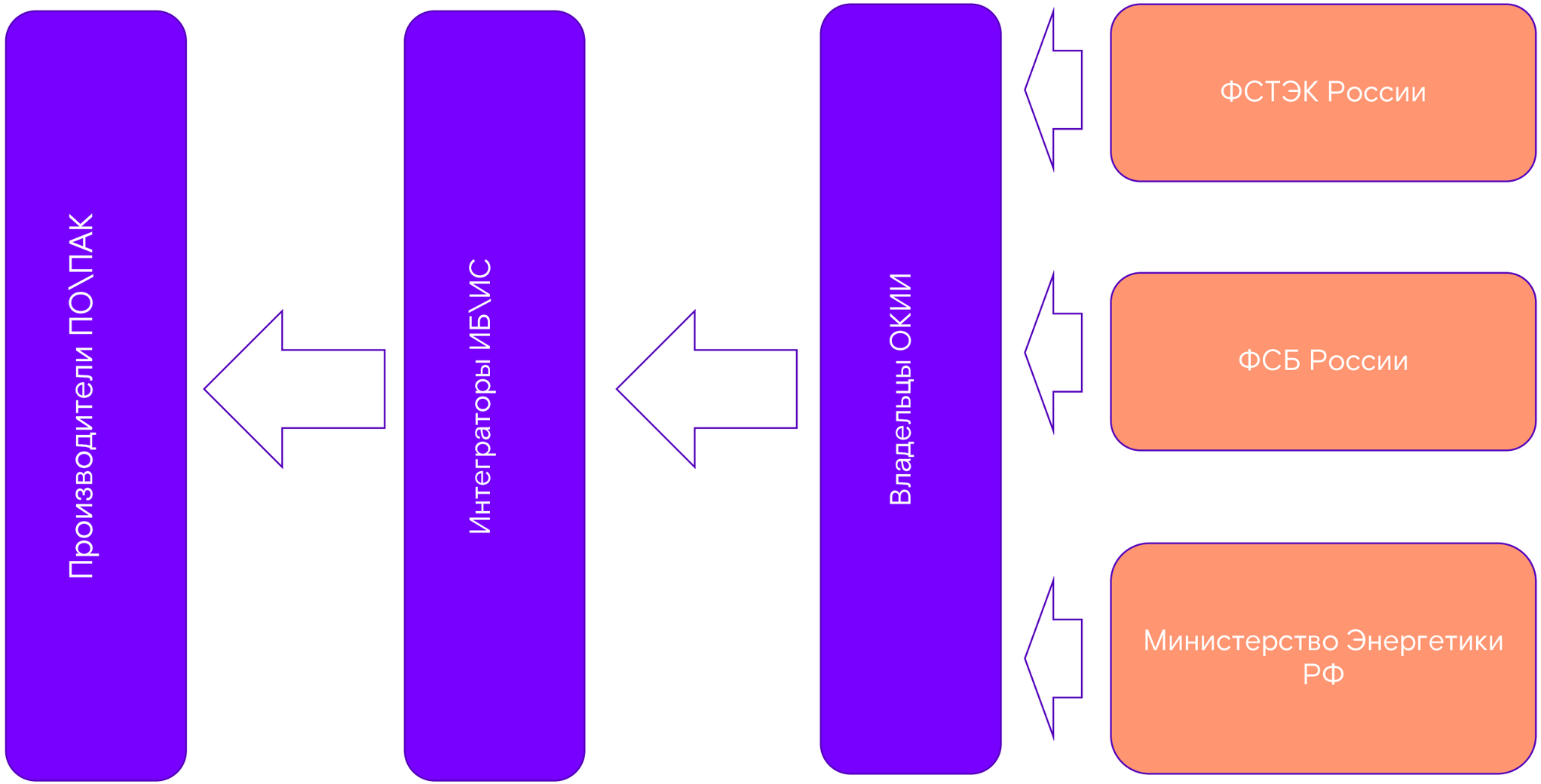
«29.4. Выполнение требований по безопасности, указанных в подпунктах 29.3.1 - 29.3.3 пункта 29.3 настоящих Требований, **оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции или ремонту) значимого объекта и (или) обеспечению его безопасности**, на этапе проектирования значимого объекта на основе результатов анализа материалов и документов, представляемых разработчиком (производителем) программного обеспечения в соответствии с техническим заданием (частным техническим заданием), разрабатываемым в соответствии с пунктом 10 настоящих Требований.»

Ростелеком Солар

Ростелеком
Солар

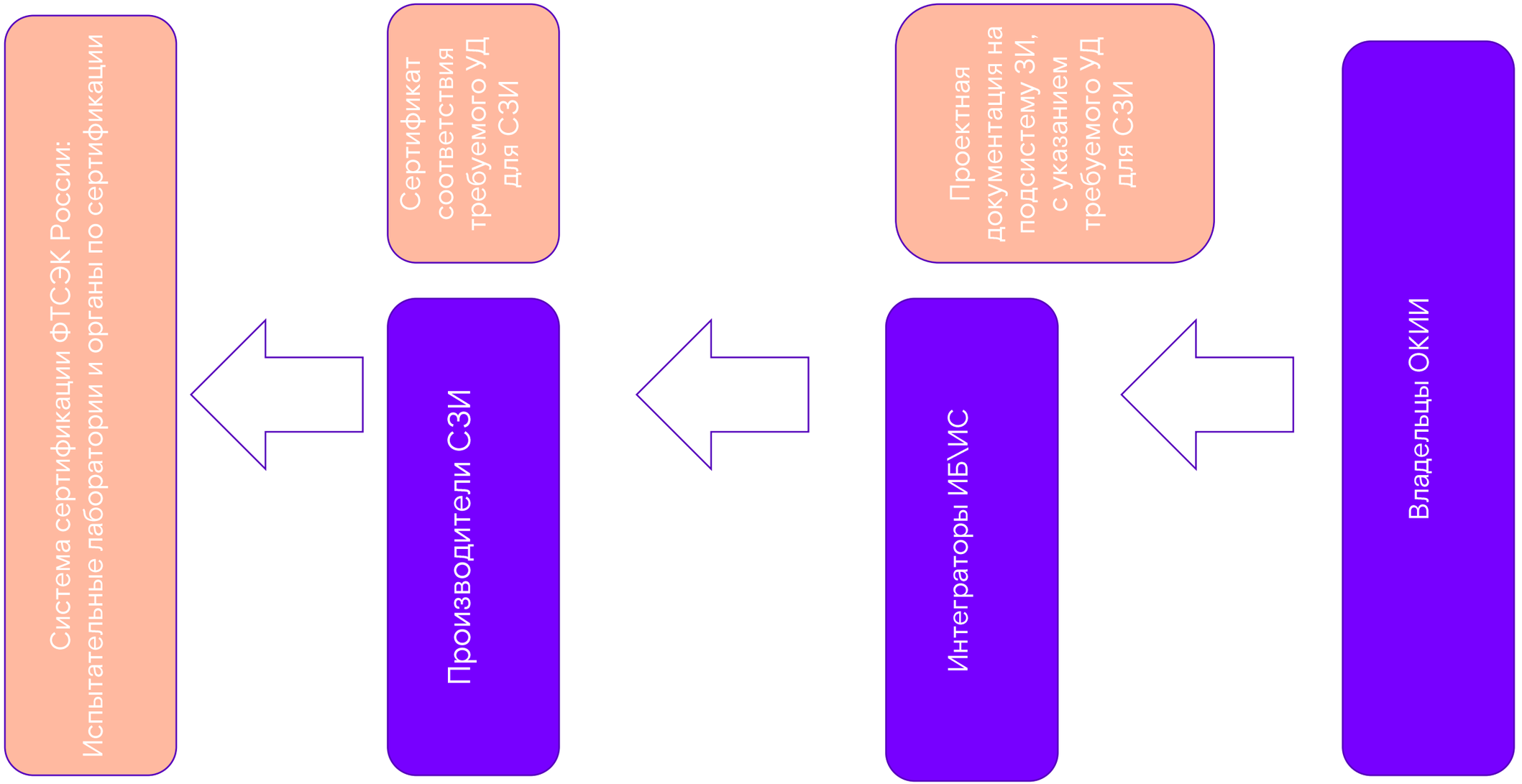
Практики выполнения мер по соответствию новым требованиям по анализу безопасности ПО

Как выставляются требования к участникам отрасли ОКИИ при приемке?



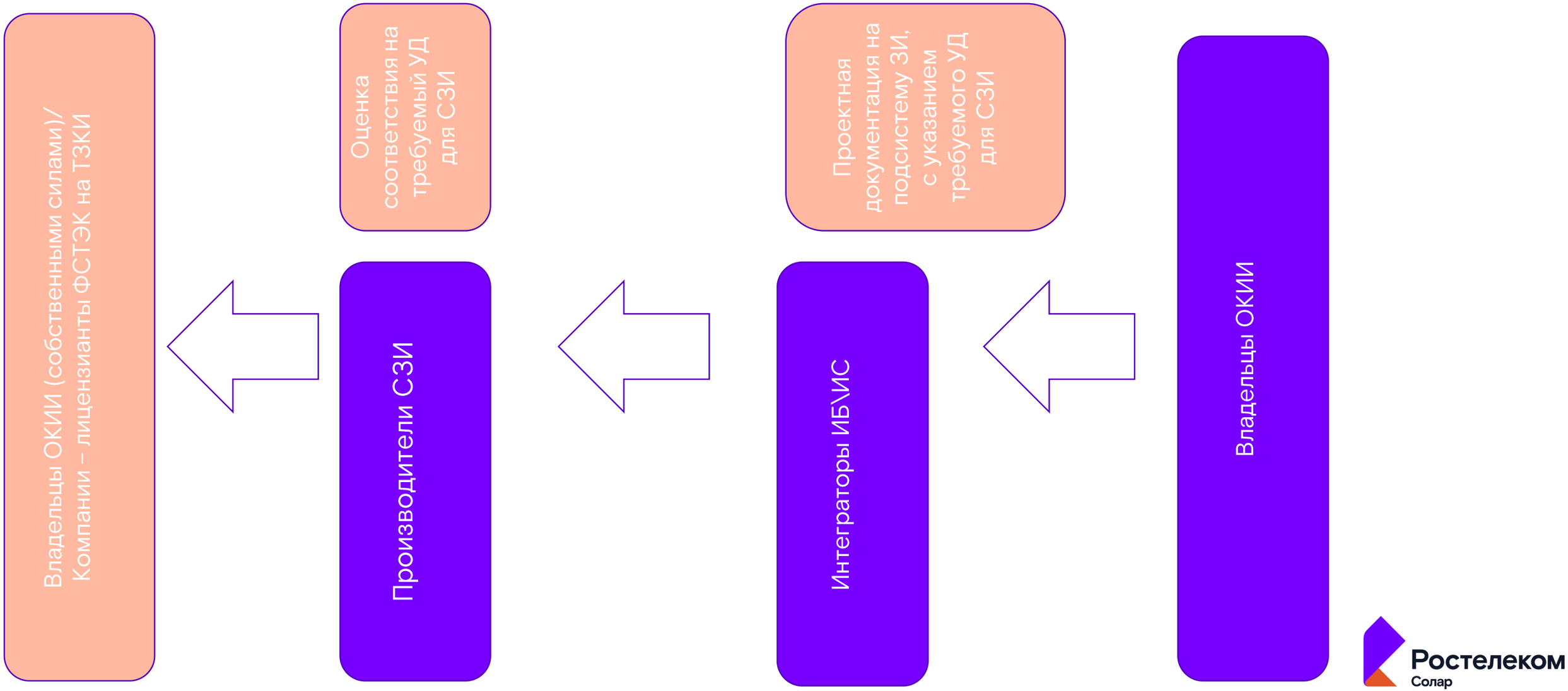
Ростелеком Солар

Как выполняется проверка выполнения требований к сертифицированным СЗИ?



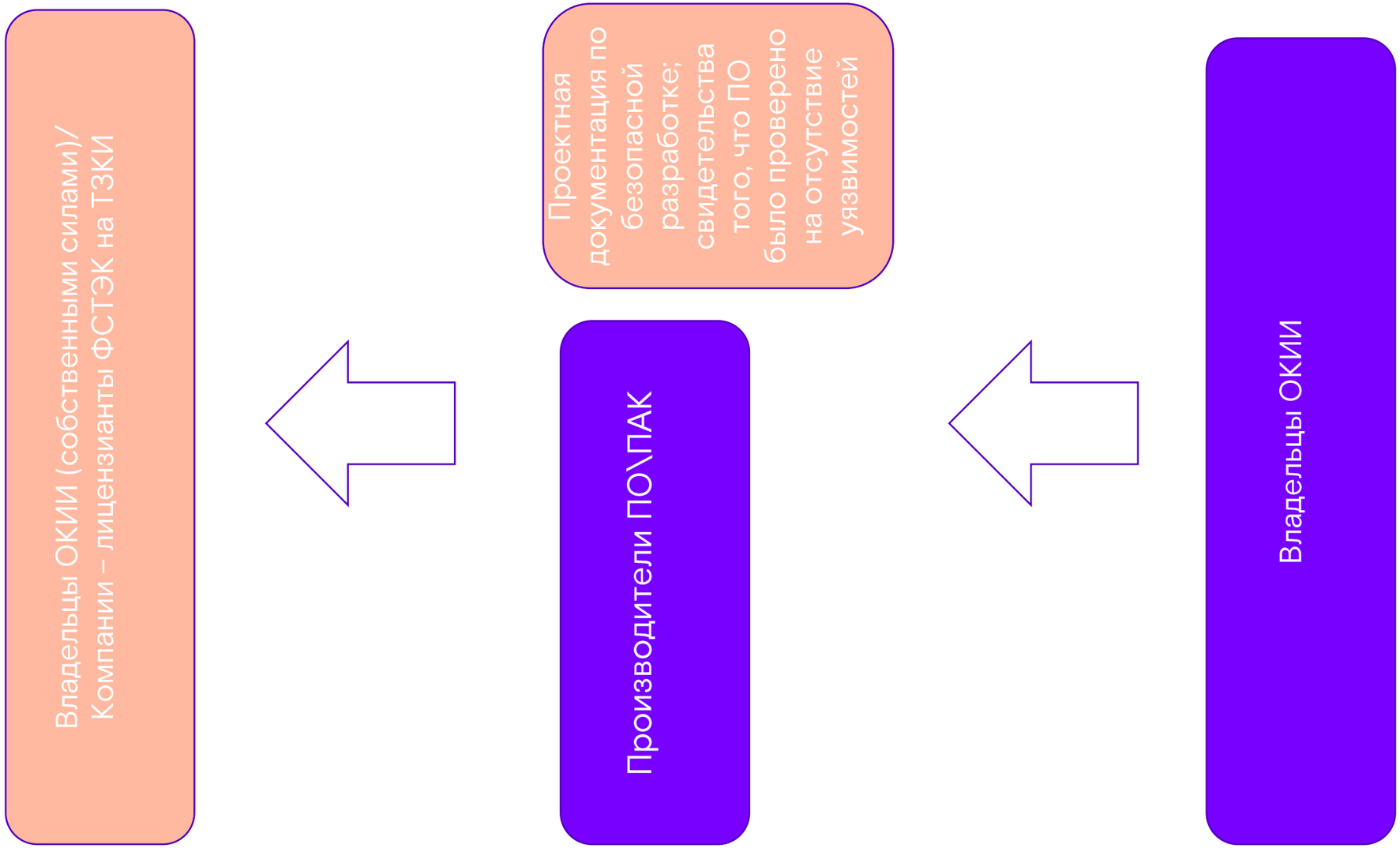
Ростелеком Солар

Как выполняется проверка выполнения требований к несертифицированным СЗИ?



Ростелеком Солар

Как выполняется проверка выполнения требований по безопасной разработки?



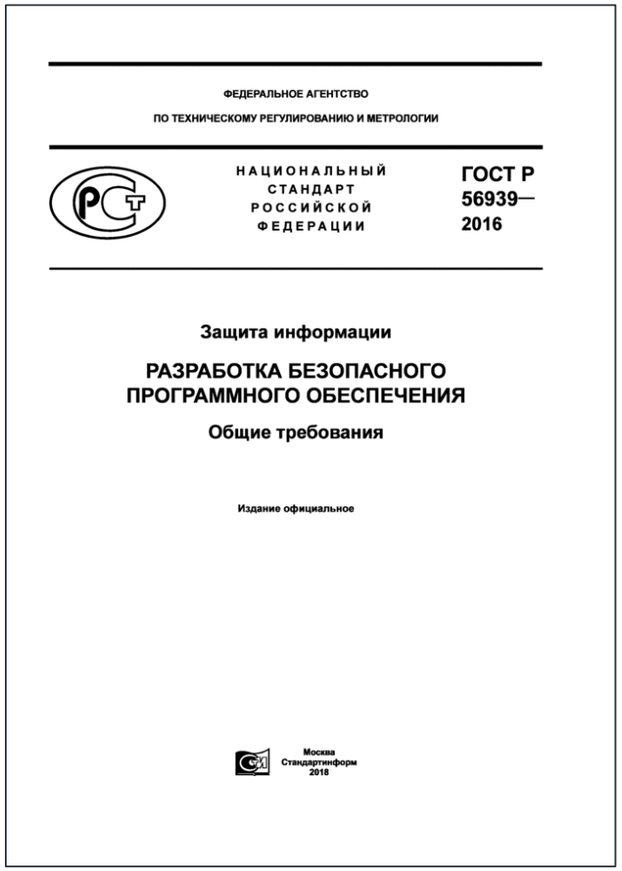
Ростелеком Солар

Как выполняется приведение в соответствие требованиям по безопасной разработки?

Производители ПО\ПАК,
Компании – лицензианты ФСТЭК на ТЗКИ

Проектная документация по безопасной разработке; свидетельства того, что ПО было проверено на отсутствие уязвимостей

Производители ПО\ПАК



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2018

Ростелеком
Солар

Ростелеком
Солар

Что же делать организациям отрасли в первую очередь?

Как выполнить требования 239 Приказа ФСТЭК России к применяемым СЗИ, вступающие в силу с 1 января 23 года?

Производители ПО\ПАК и СЗИ

Владельцы ОКИИ, Интеграторы ИТ\ИБ

Определить Вашу роль

Обеспечить условия для успешного прохождения контролей

Реализовать контролирующие меры

Какая Ваша задача?

Стоить процесс Сразу при партнерстве с экспертной компании.

Разбить процесс внедрения практик на несколько лет:
1) описать процессы;
2) Выстроить процедуру анализа кода;
3) Для прочих прове-рок привлечь экспертную организацию

Растить в себе экспертизу: Закупать инструменталь-ные средства; Нанимать экспертов.

Обратиться за услугой к др. организации

Исходя из ресурсов определить решение

Ростелеком Солар

Почему статический анализ внедряется в первую очередь?

Полное покрытие кода

Показывает все потенциальные ошибки схожего типа.

Простая интеграция

Может быть интегрирован в сборочную инфраструктуру на разных этапах разработки ПО в рамках внедрения практик безопасной разработки.

Конкретные выводы

Указывает, где конкретно находится ошибка в коде, и описывает, к чему она может привести.

Выявление 0-day

Сохраняется возможность обнаружения уязвимостей нулевого дня.

Ростелеком Солар

Почему важно обращаться к команде экспертов по анализу защищенности ПО?

Разные инструменты для разных стеков технологий

Инструменты динамического анализа (в том числе и фаззеры) работают только с определенным стеком технологий. И если у Вас в разработке находится несколько решений реализованных на разных стеках, то потребуются и разные инструменты. Которые смогут подобрать эксперты.

Требуется подтверждение применимости уязвимости

Эксперты смогут описать методику или подготовить эксплойт, успешно эксплуатирующий уязвимость, что позволит получить более точный результат.

Не всегда просто обеспечить интеграцию

Эксперты могут подсказать с какими настройками наиболее эффективно будет интегрировать и автоматизировать процесс динамической проверки кода.

Требуется интерпретация результатов технических отчетов

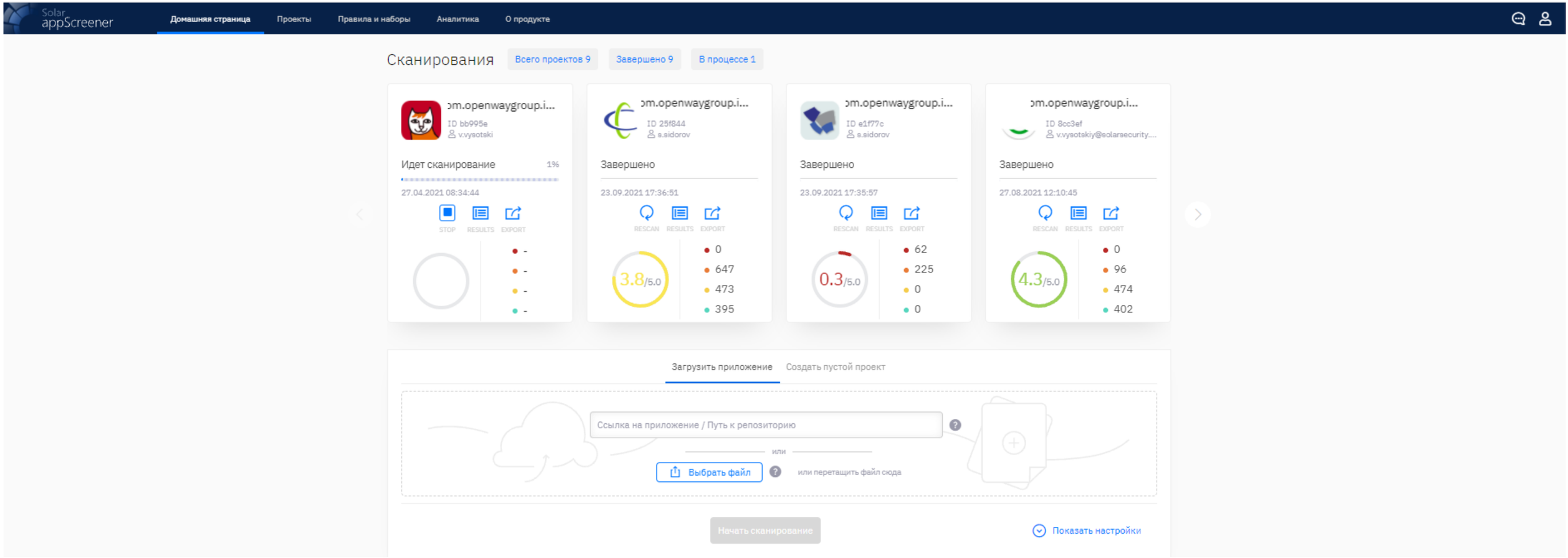
Динамические анализаторы за частую представляют неполную информацию об уязвимости и требуются дополнительные комментарии экспертов чтобы понять какие дальше шаги требуется выполнить.

Ростелеком Солар

Ростелеком
Солар

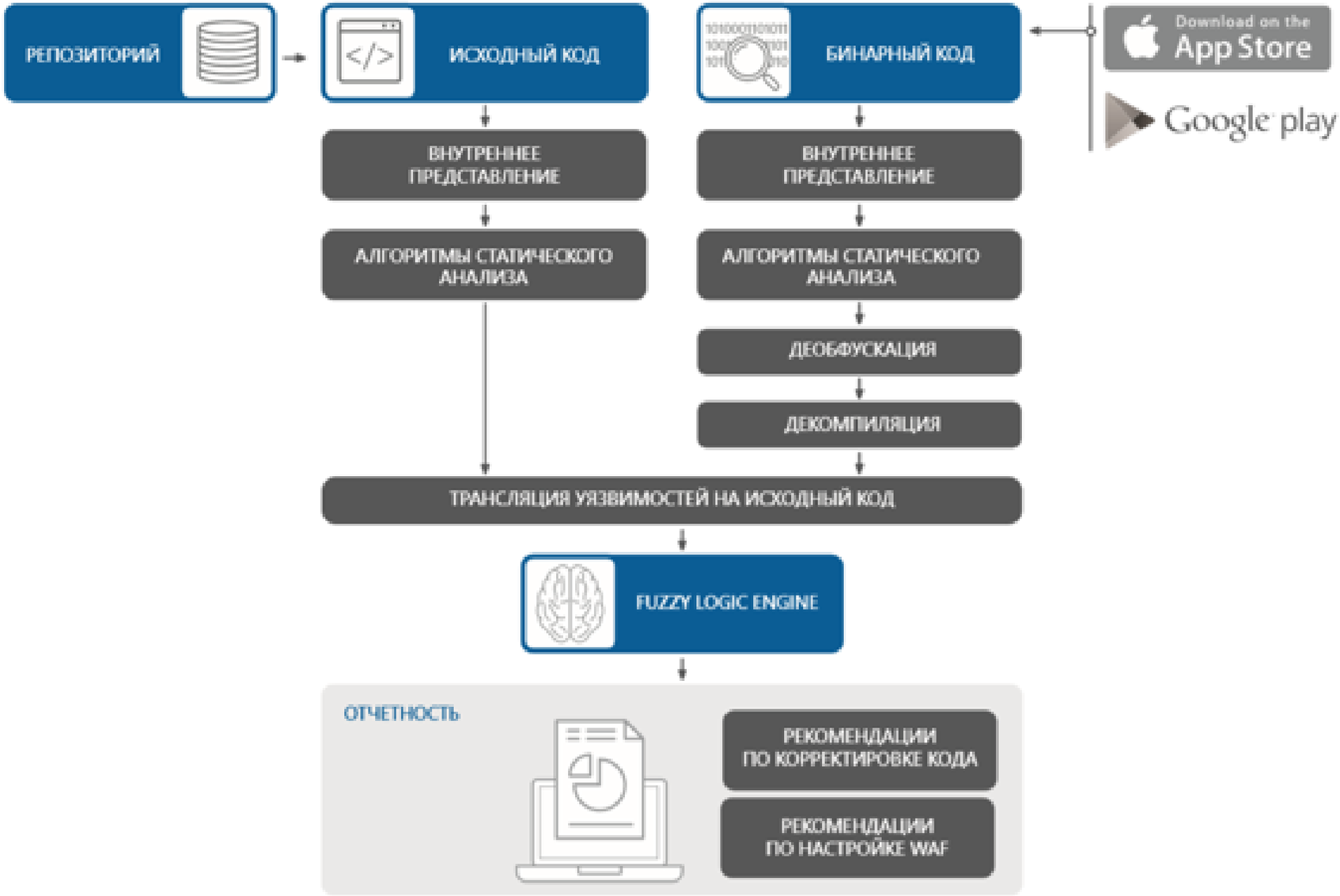
Чем могут помочь экспертные организации по ИБ участникам Энергетической отрасли? (На примере Ростелеком-солар)

Solar appScreener – анализатор кода с простым и понятным интерфейсом



Ростелеком
Солар

Принципы работы Solar appScreener



Ростелеком Солар

Преимущества Solar appScreener:

36 языков программирования

Включая возможность выполнения анализа мобильного ПО, размещенного в магазинах приложений Google Play и App Store.

9 типов бинарных файлов

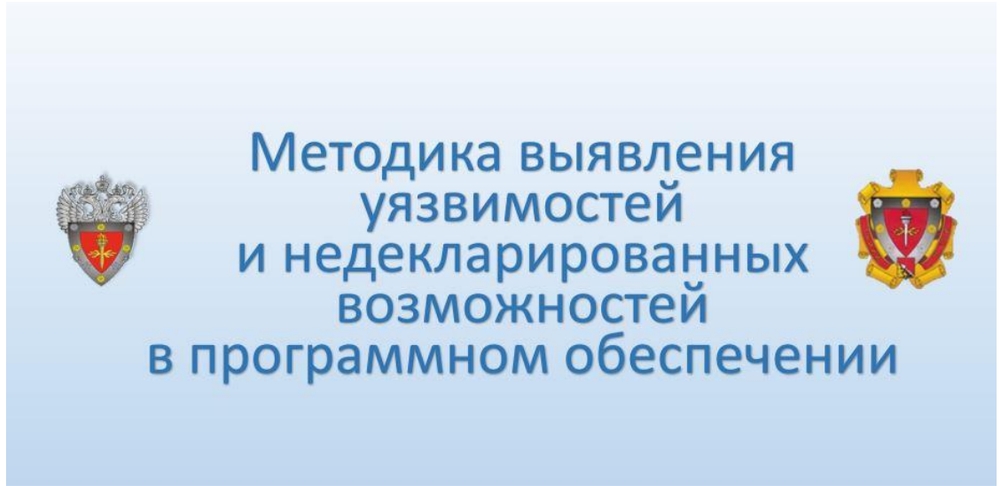
Ростелеком
Солар

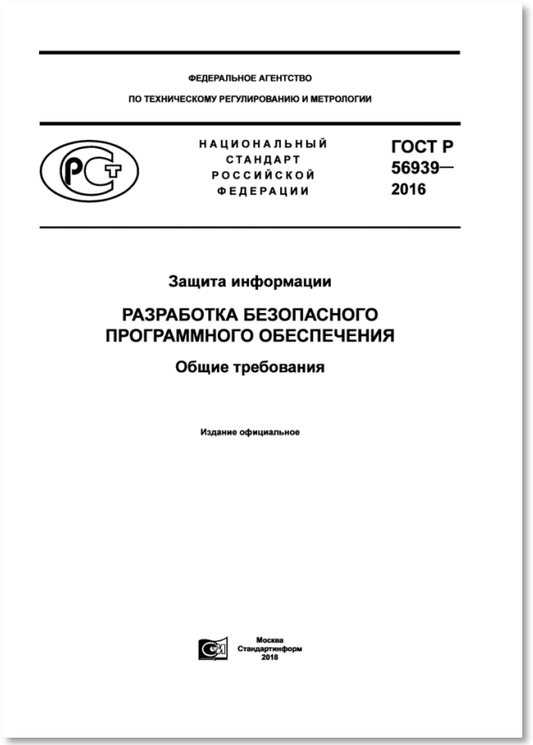
Поддерживается интеграция со следующими инструментами разработки

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

Ростелеком Солар

Solar appScreener может применяться как инструмент (сервис) проверки безопасности кода, так и как инструмент, используемый в рамках безопасной разработки.





ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2016

Ростелеком
Солар

Эксперты в области анализа защищенности ПО Ростелеком-солар:

- Богатый опыт поиска уязвимостей нулевого дня в различном ПО (в том числе и АСУТП). Первое место среди исследователей на сайте БДУ ФСТЭК.

- Богатый опыт ведения методологической деятельности (как в рамках частных проектов, так и на базе Киберполигона Ростелеком-Солар).

Ростелеком
Солар

Спасибо за внимание!

Деев Сергей
Менеджер продукта Solar appScreener

rt-solar.ru

rt-solar.ru/products/solar_appscreener/capabilities/