

# **СЕРТИФИКАЦИЯ И ПОДТВЕРЖДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Содокладчик**

**Павел Владимирович Березюк**

Руководитель по информационной  
безопасности ООО «ИНБРЭС»

**Докладчик**

**Ольга Васильевна Димитриева**

Инженер по информационной  
безопасности ООО «ИНБРЭС»



- Производственно-инжиниринговая компания, выполняющая комплексные проекты по внедрению цифровых систем защиты и управления для энергетики и промышленности.
- Центр компетенции в области автоматизации
- Лаборатория по разработке цифровых решений
- Цифровой испытательный полигон



Испытательный полигон «ИНБРЭС» – цифровая модель ПС 500 кВ

# ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ В ЧАСТИ ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Проектирование и внедрение систем информационной безопасности на промышленных объектах критической информационной инфраструктуры (ОКИИ)
- Техническое сопровождение систем информационной безопасности
- Внедрение безопасной разработки программного обеспечения в организации
- Проведение аудита информационной безопасности
- Аттестация объектов информатизации (АРМ, ЗП, ГИС и т.д.)



# ОПРЕДЕЛЕНИЯ

01

**Оценка соответствия требованиям по защите информации** – это прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.\*

02

**Сертификация на соответствие требованиям по безопасности информации** – это форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.\*

03

**Объект защиты информации** — это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.\*

\* - ГОСТ Р 50922-2006 Защита информации.  
Основные термины и определения



# АКТУАЛЬНОСТЬ

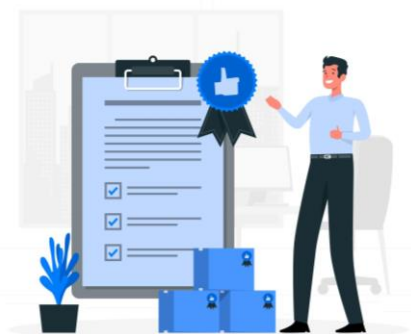
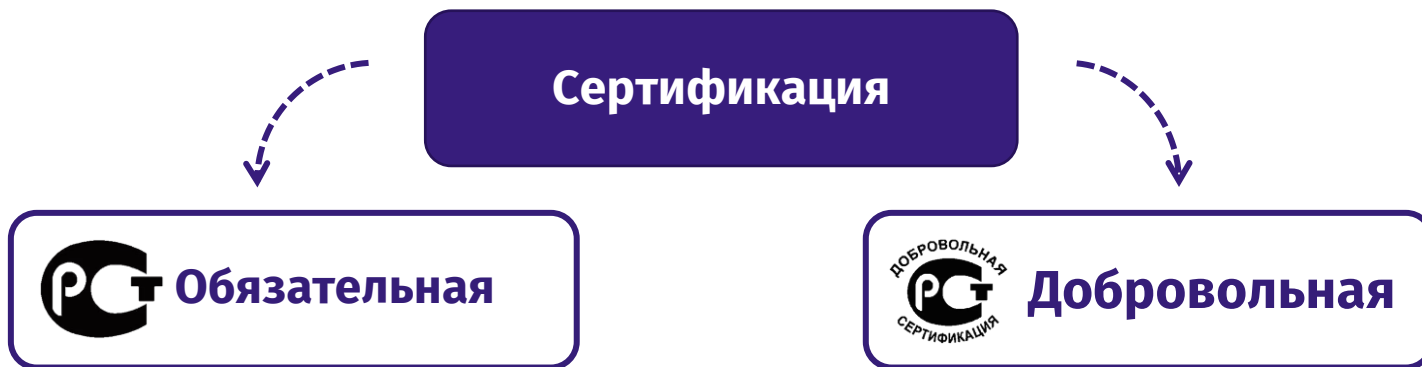


**Доклад актуален** для разработчиков программных продуктов и для организаций, которые разрабатывают *специальное программное обеспечение* в области энергетики и планируют проходить сертификацию или *подтверждение оценки соответствия* требованиям по информационной безопасности.

**Актуальность** настоящего доклада обусловлена необходимостью *подтверждения* со стороны разработчиков программных средств, *наличия функций* информационной безопасности в программном обеспечении, которое управляет технологическими процессами.



# СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ





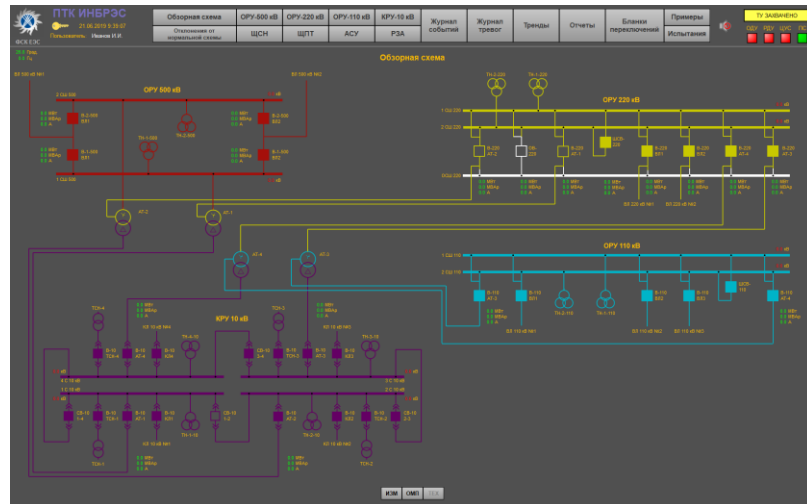
- Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»
- Приказ ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76
- Методика выявления уязвимостей и недеklarированных возможностей в программном обеспечении (ДСП)



# ПОДТВЕРЖДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



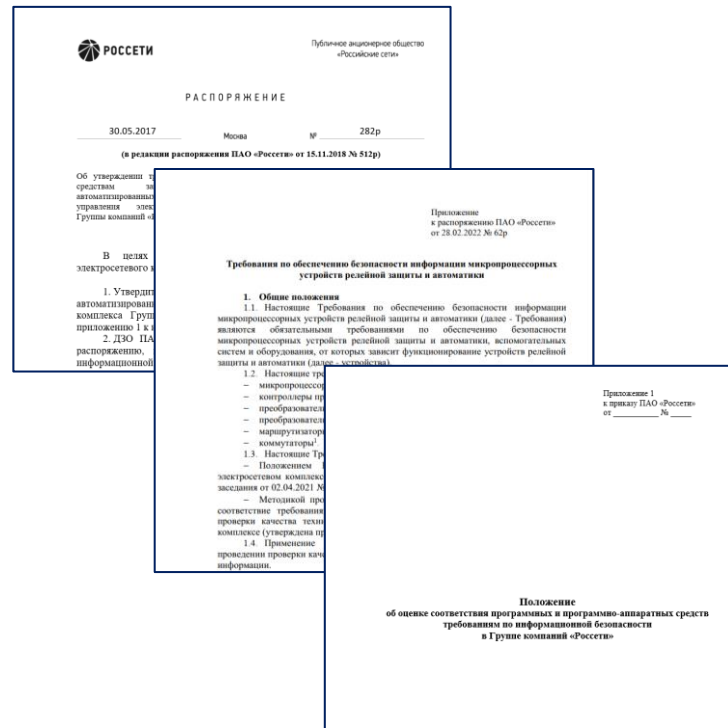
Сертификация является одной из форм оценки соответствия. Принципы прохождения оценки соответствия могут быть адаптированы для разных компаний и ПО.





# ОСНОВНЫЕ ДОКУМЕНТЫ ПАО «РОССЕТИ» ДЛЯ ПОДТВЕРЖДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ ПО ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Распоряжение ПАО «Россети» № 282р от 30 мая 2017 г. «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети»
- Положение об оценке соответствия программных и программно-аппаратных средств требованиям по информационной безопасности в Группе компаний «Россети»
- Требования по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики. Приложение к распоряжению ПАО «Россети» от 28 февраля 2022 г. № 62р



# ПОДТВЕРЖДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

01

Реализация функций информационной безопасности в программном обеспечении

02

Внедрение процессов в организации для прохождения оценки соответствия

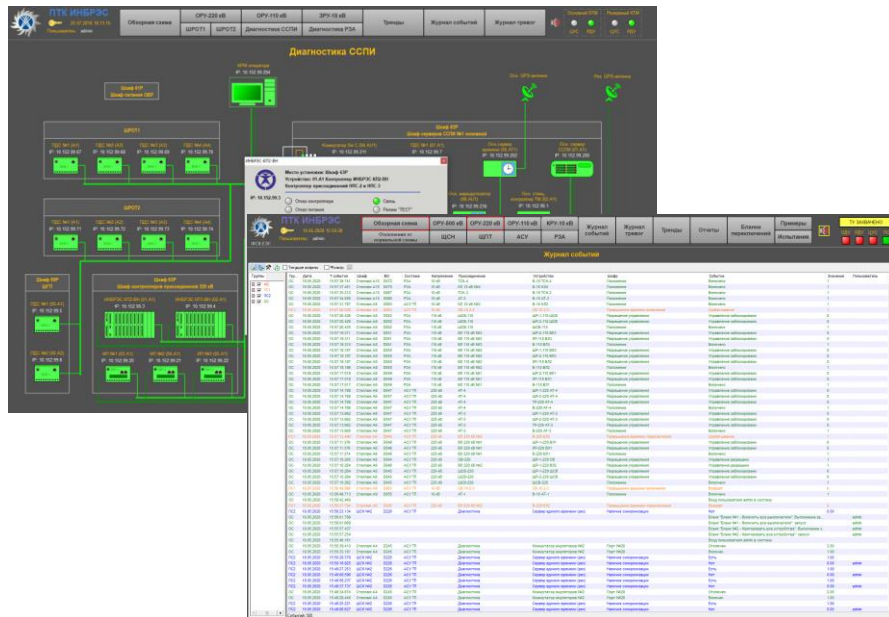
03

Внедрение безопасной разработки программного обеспечения в организации

04

Подтверждение оценки соответствия программного обеспечения требованиям информационной безопасности





На примере ПО «ИНБРЭС»:

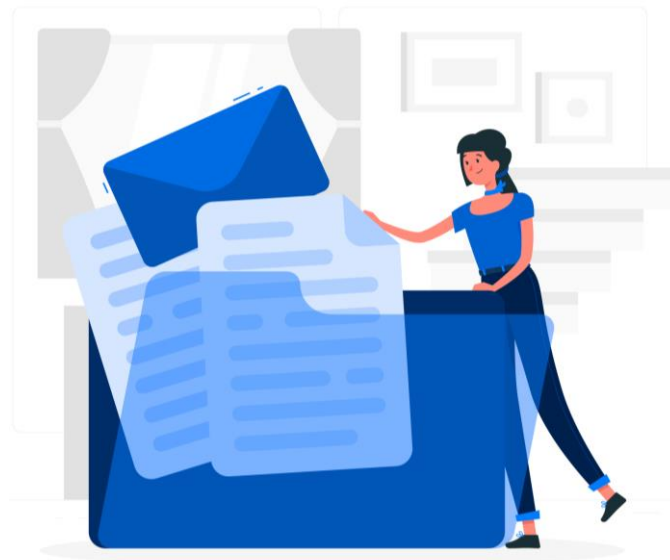
- Управление доступом субъектов доступа к объектам доступа
- Регистрация событий безопасности (аудит)
- Идентификация и аутентификация
- Откат к исходному состоянию
- Контроль целостности



*Входит в Единый реестр российского ПО.  
Запись №5271 от 26.02.2019*

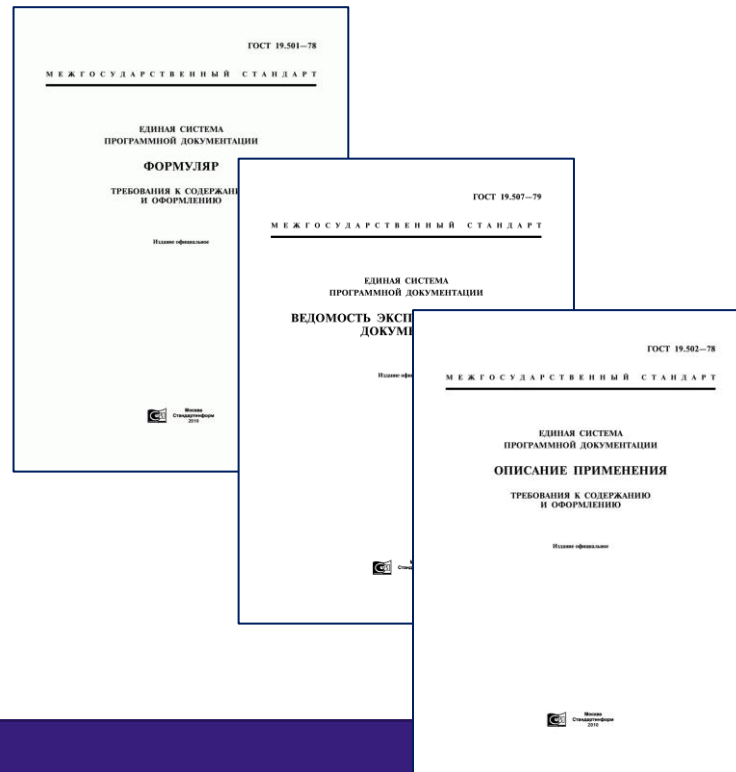
# ПРОГРАММНАЯ ДОКУМЕНТАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ПОДТВЕРЖДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ

- Технические условия
- Описание архитектуры безопасности разрабатываемого ПО
- Базовый модульный проект (функциональная спецификация)
- Модель безопасности разрабатываемого ПО
- Задание на безопасность
- Описание инструментальных средств разработки
- Описание программы
- Программа и методика испытаний
- Спецификация
- Текст программы



# ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ПОДТВЕРЖДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ

- Формуляр
- Ведомость эксплуатационных документов
- Описание применения
- Руководство пользователя по эксплуатации
- Руководство администратора по безопасности

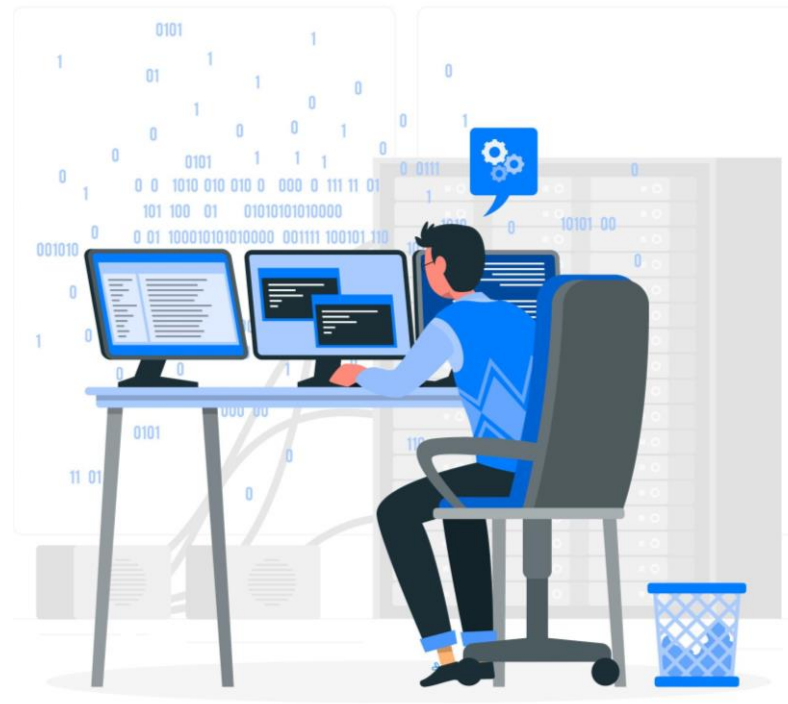


# ВНЕДРЕНИЕ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ





- Наличие стенда для изготовления ПО
- Определён порядок тиражирования
- Определён порядок изготовления и испытаний
- Определены требования к транспортировке
- Определён порядок маркировки и упаковки
- Регулярный контроль мероприятий по выпуску программного обеспечения



# СОПРОВОЖДЕНИЕ ПО НА ВСЁМ ЭТАПЕ ЖИЗНЕННОГО ЦИКЛА

02  
процесс

01

Тестирование ПО на наличие уязвимостей



02

Устранение недостатков и уязвимостей в ПО



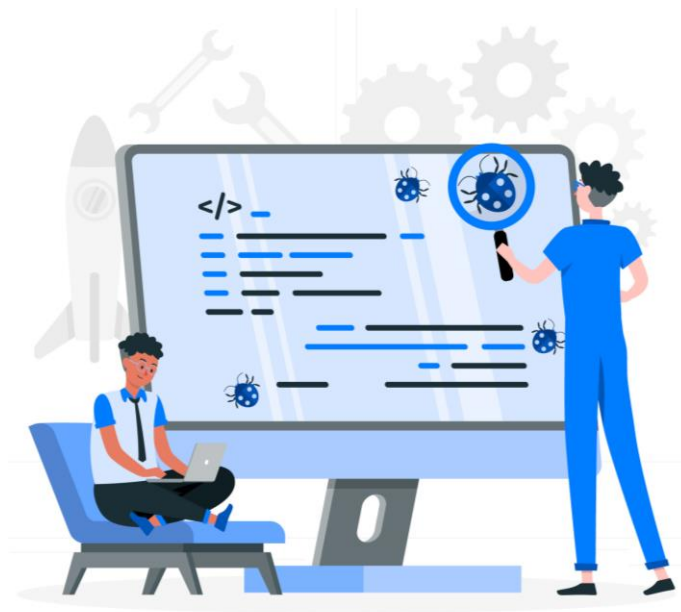
03

Выпуск обновлений ПО



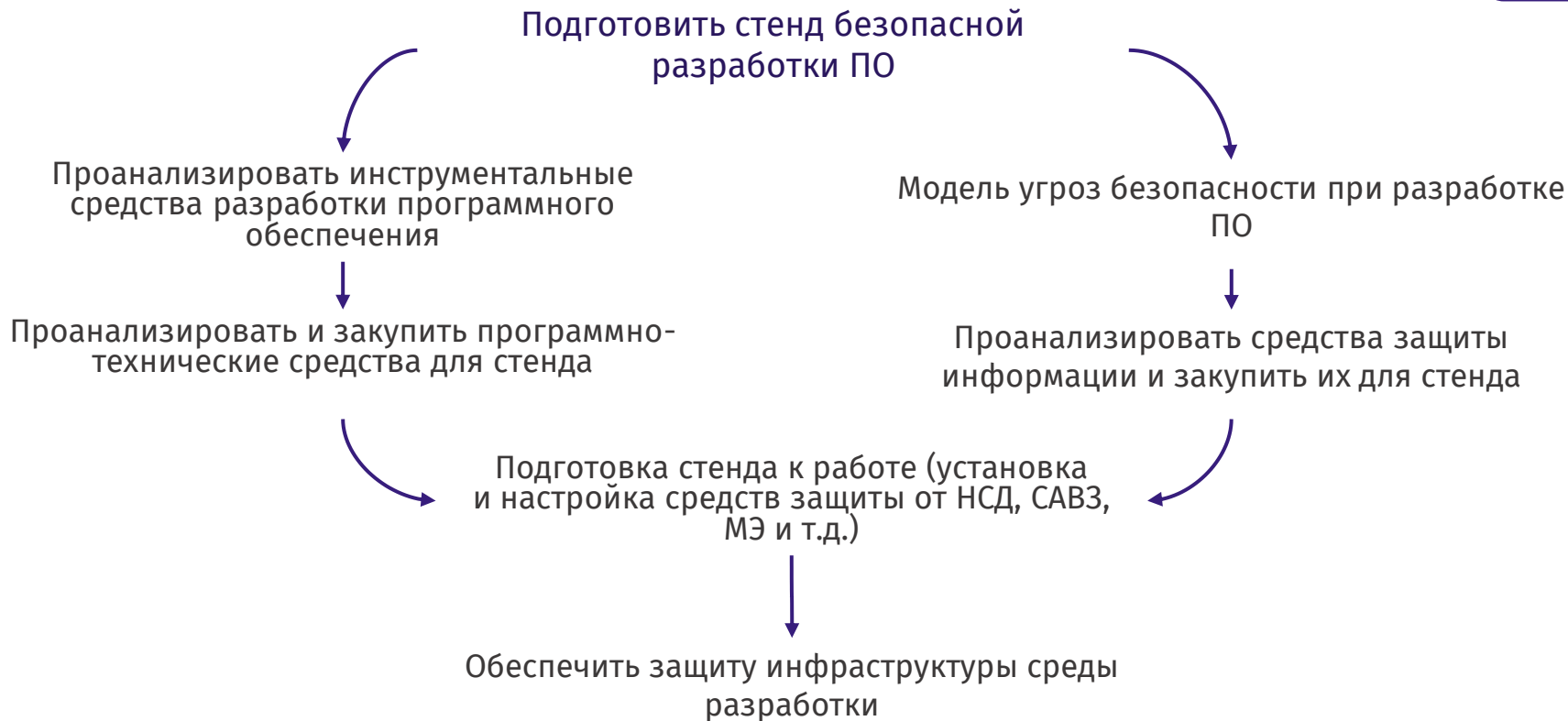
04

Доведение обновлений до пользователей



# БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

03  
процесс



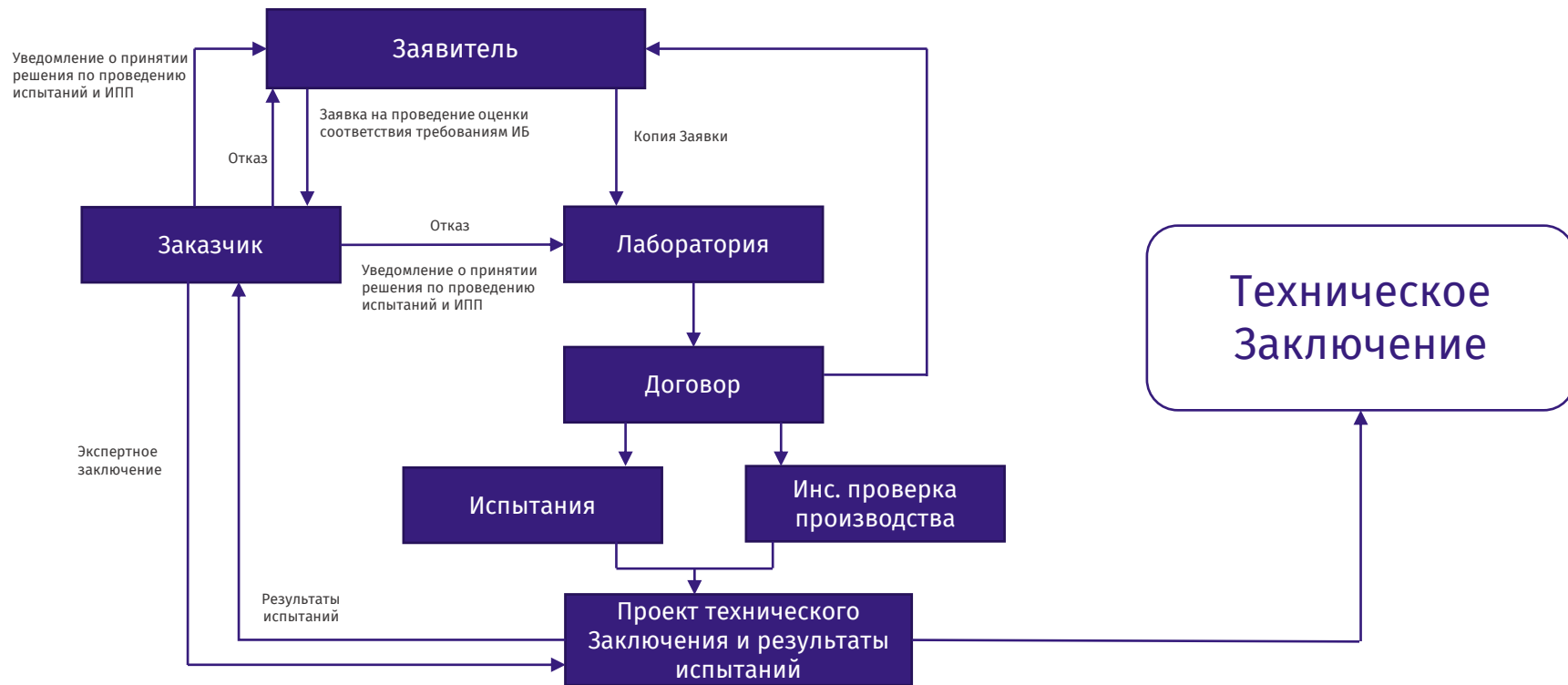
# БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- Регламент по проведению статического анализа кода
- Регламент по проведению динамического анализа
- Регламент по проведению фаззинг-тестирования
- Регламент по проведению экспертизы исходного кода
- Регламент по проведению тестирования на проникновение
- Регламент по проведению тестирования на наличие уязвимостей



# ПОДТВЕРЖДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**04**  
процесс



# ПОДТВЕРЖДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

04  
процесс





# БЛАГОДАРИМ ЗА ВНИМАНИЕ

Приглашаем к взаимовыгодному  
сотрудничеству в проектах  
по строительству  
и реконструкции объектов энергетики и  
инфраструктуры!



[inbres.ru](http://inbres.ru)



[info@inbres.ru](mailto:info@inbres.ru)

