

# Опыт и планы по сертификации инженерного ПО АСКОН в ФСТЭК РФ в 2008 - 2019 годах

Иван Трохалин, АСКОН



АССОЦИАЦИЯ  
ЛИГА СОДЕЙСТВИЯ  
ОБОРОННЫМ  
ПРЕДПРИЯТИЯМ

# Предыстория



Решения компании АСКОН «родились» и «вышли» из KBM в 1989 году. Поэтому с самого начала требования информационной безопасности для ПО нашей разработки заказчики озвучивали, как важную составляющую использования систем на предприятиях ОПК.

# Этапы работы:

Работы по сертификации ПО в ФСТЭК проводились в несколько этапов:

**I этап, 2008-2009 год.** Сертификация ПО для контура ДСП.

**II этап, 2012-2015 год.** Сертификация ПО для контура ГТ.

**III этап, 2017-2018 год.** НИР по целевой модели, обеспечивающей мандатный контроль доступа с учетом эффективной работы ИТР.

**IV этап, 2018 - ...**

# I этап работы. 2008 - 2009

В рамках добровольной сертификации выполнен комплекс внутренних работ:

1. Разработана детальная документация по описанию принципов работы ПО АСКОН.
2. Подробно описаны механизмы взаимодействия программных инструментов между собой.

# I этап работы. 2008 - 2009

## Результат этапа:

1. Сертификат соответствия ЛОЦМАН:PLM РД СВТ по 5-му классу защищённости и соответствия РД НДС по 4 уровню контроля.
2. Сертификат соответствия КОМПАС-3D РД НДС по 4 уровню контроля.
3. Сертификаты ФСТЭК получили Гемма-3D и АПМ FEM

## II этап работы. 2012 - 2015

Одними из ключевых требований к проекту Типовой Информационной Системы Ядерно-оружейного комплекса (ТИС ЯОК) и создаваемой в рамках проекта автоматизированной системы были требования по информационной безопасности.

## II этап работы. 2012 - 2015

Выполненные работы (совместно с ФГУП «РФЯЦ-ВНИИЭФ», «Информационная» и НПО «Эшелон»):

1. Доработка ПО в части встраивания средств защиты:

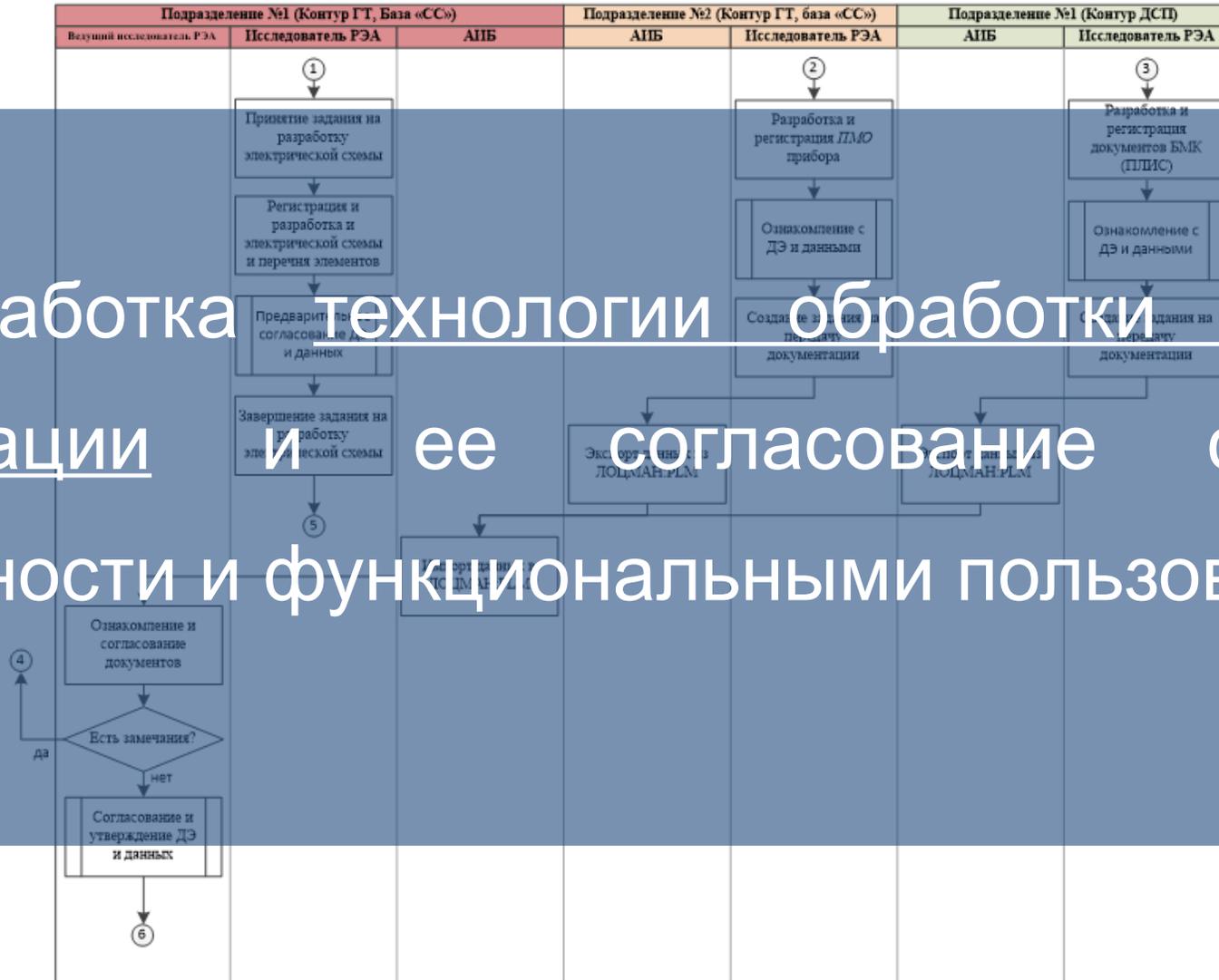
- доработана интеграция с СрЗИ НСД SecretNet;
- переработан механизм базовой аутентификации;
- доработан контроль доступа субъектов к защищаемым информационным объектам в соответствии с матрицей доступа;

## II этап работы. 2012 - 2015

- расширена реализация подсистемы регистрации событий ИБ;
- полностью исключена избыточность программного кода;
- выполнена замена программных компонентов сторонних разработчиков для обеспечения полного предоставления исходных кодов всех используемых компонентов;

# II этап работы. 2012 - 2015

2. Разработка технологий обработки защищаемой информации и ее согласование со службой безопасности и функциональными пользователями.



# II этап работы. 2012 - 2015



3. Разработка технических условий применения РДМ-системы в качестве средства защиты информации совместно с СрЗИ SecretNet.

## II этап работы. 2012 - 2015

4. Разработка полного комплекта документации с учетом требований сертификации, в том числе:

- предоставлен для испытаний полный комплект исходных текстов программ, входящих в объект сертификации;
- предоставлены стенды для компиляции программ, а также для сборки дистрибутива ПО

5. Проведение сертификационных испытаний совместно с испытательной лабораторией

## II этап работы. 2012 - 2015

**Результат этапа:**

Комплекс ПО АСКОН, единственный на рынке инженерного ПО в РФ, был сертифицирован для применения в АСЗИ до класса 1Б включительно.



## III этап работы. 2017 - 2018

Проведена НИР для определения целевой модели защиты информации, обеспечивающей мандатный контроль доступа на уровне информационных объектов с приемлемой для функциональных пользователей методикой применения инженерного ПО.

# III этап работы. 2017 - 2018

## Результаты НИР:

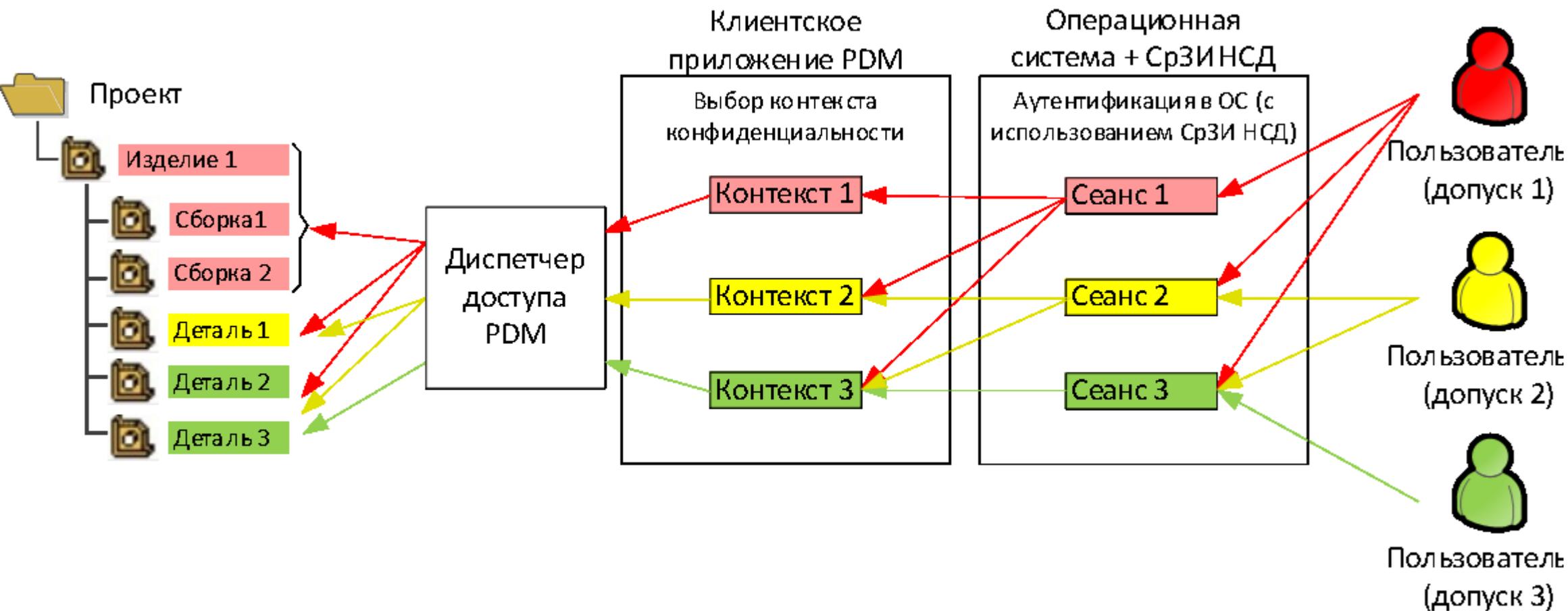
1. Целевая технология выполнения процессов предполагает возможность назначения пользователем уровня конфиденциальности создаваемой информации (в пределах допуска) без осуществления смены сеанса конфиденциальности (без перезапуска ОС и программы - инструмента)

# III этап работы. 2017 - 2018

Результаты НИР:

2. Обеспечение целевой технологии работы требует реализации контекстной модели назначения меток конфиденциальности во всех клиентских приложениях PLM системы, а также во всех программах-инструментах, которые работают с агрегированными (состоящими из нескольких ассоциативно связанных файлов) документами.

# III этап работы. 2017 - 2018



# IV этап работы. 2018 - ...

## Перспективы:

### 1. Поддержка импортонезависимых СУБД:

- СУБД PostgreSQL. Начались работы по портированию.
- СУБД Линтер. НИР по поддержке в справочниках



# IV этап работы. 2018 - ...

## 2. Поддержка импортонезависимых ОС:

- разработан прототип просмотрщика САD-документов на базе КОМПАС-3D, работающий под управлением



- дальнейшие работы приостановлены, так как не ясны перспективы (какие ОС считаются импортонезависимыми, будет ли господдержка одной из них или нескольких, как обеспечить работу всего комплекса инженерного ПО на базе импортонезависимых ОС)

# Выводы:

**1. Жизненный цикл сертифицированного продукта не заканчивается сертификацией.**

Необходима организация комплекса работ по сопровождению, минимум:

- Контроль уязвимостей систем защиты;
- Инспекционный контроль ПО в случае устранения уязвимостей и исправления ошибок;
- Работы по пересертификации.

## Выводы:

2. Эксперты понимают, как на основе данного опыта, достичь целевого варианта защищенной PLM/PDM-системы, которая будет при этом сохранять свои основные показатели эффективности применения для ИТР. Целевого варианта нет ни у кого на сегодняшний день.

## Выводы:

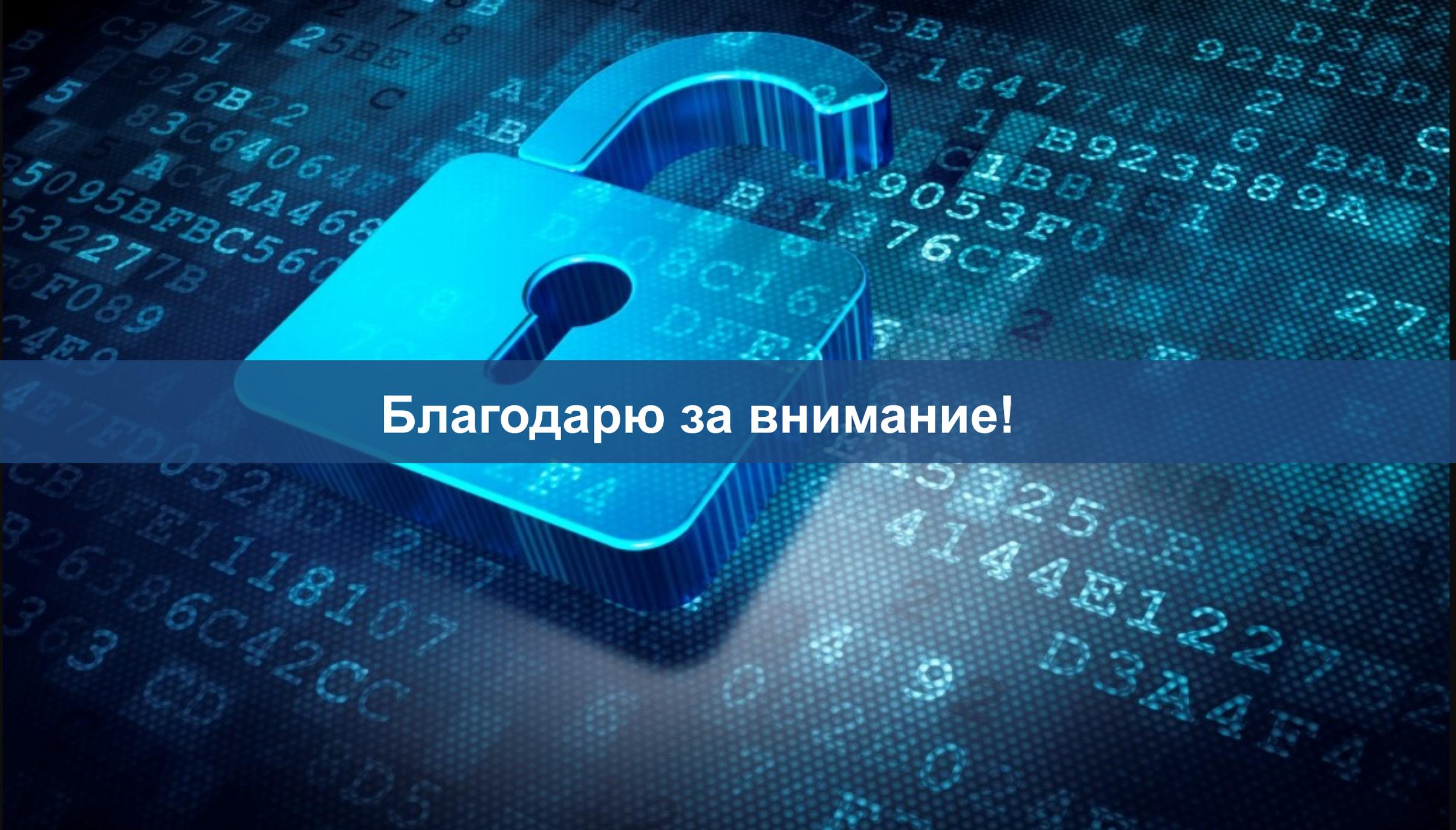
3. Перевод отдельных компонентов инженерного ПО (например, PLM и CAD) на «импортонезависимые» ОС недостаточен. Должны быть конкурентоспособные отечественные системы CAE/CFD/eCAD/CAM, так же работающие на этих ОС. Участники консорциума «Развитие» частично решает эту задачу.

## Выводы:

4. В целевой модели САД-система из-за ее специфики становится частью средств защиты информации и она должна быть также сертифицирована и, поэтому не должна содержать покупных компонентов (в том числе иностранных математических ядер, модулей визуализации и т. п. компонентов).

## Выводы:

5. Важно, чтобы от заказчика(ов) было четкое и согласованное техническое задание на конкретную защищенную ОС и СУБД. Данное ПО должно начинаться использоваться на предприятиях промышленности, должна быть обеспечена совместимость «железа» и других КОМПОНЕНТОВ ЭКОСИСТЕМЫ.

A blue padlock is the central focus, set against a dark blue background filled with glowing binary code (0s and 1s). The padlock is open, with the shackle raised. The lighting is dramatic, highlighting the metallic texture of the padlock.

**Благодарю за внимание!**