АО «Научно-исследовательский институт «Вектор»

Вопросы информационной безопасности в автоматизированных системах управления жизненным циклом изделий оборонно-промышленного комплекса

Докладчик: начальник сектора ЦЗИ
к.т.н. Белкин Т.Г.

Цели доклада

1. Публикация результатов решения задач защиты информации на предприятиях ОПК. Основной приоритет – решение вопросов по защите информации при разработке и изготовлении изделий военного и двойного назначения.
2. Выявление задач, решение которых требует отраслевого или государственного регулирования в отличие от тех задач, решение которых осуществляется на уровне предприятий или коопераций.

Государственная политика развития оборонно-промышленного комплекса

Указ Президента РФ от 25 декабря 2014 г. № Пр-2976 «О Военной доктрине Российской Федерации» п. 53:

К задачам развития оборонно-промышленного комплекса относятся:

г) совершенствование системы гарантированного материально-сырьевого обеспечения производства и эксплуатации вооружения, военной и специальной техники **на всех этапах жизненного цикла**, в том числе отечественными комплектующими изделиями и элементной базой;

…

к) разработка и производство перспективных систем и образцов вооружения, военной и специальной техники, повышение качества и конкурентоспособности продукции военного назначения, **создание системы управления полным жизненным циклом вооружения**, военной и специальной техники;

Среда разработки конструкторской документации

- Цель автоматизации - эффективное обеспечение жизненного цикла изделия, включая, но не ограничиваясь разработкой КД.
- Конечная цель автоматизации для Предприятия - сократить сроки разработки КД, передачи ее на производство и внесения изменений в КД за счет отказа от бумажной формы документации.
- Среда разработки КД - информационно-телекоммуникационная структура автоматизированной системы управления жизненным циклом изделия.
- Автоматизированная система управления жизненным циклом изделия (АСУ ЖЦИ) – комплекс взаимоувязанных информационных систем, обеспечивающих выполнение процессов реализации функций информационной поддержки жизненного цикла разрабатываемых изделий.

Факторы доверия к среде

- Наличие исходных текстов на используемое прикладное программное обеспечение (CAD/ CAM, PLM, ERP, MES ...).
- Наличие функций (механизмов, средств) защиты информации на прикладном уровне (управление доступом, управление потоками).
- Наличие доверенных базовых элементов информационно-коммуникационных технологий (ИКТ) – ОС, СУБД, телекоммуникационное оборудование, средства виртуализации и СХД.

Этапы создания АСУ ЖЦИ

Создание АСУ ЖЦИ можно ***условно*** разделить на следующие стадии:

Стадия 1 – Локальная автоматизация

Внедрение различных средств разработки на АРМ предметных специалистов, участвующих в разработке изделий. АРМ могут быть объединены в ЛВС, которая охватывает, как правило, одно подразделение.

Стадия 2 –Взаимодействие разных подразделений на одном Предприятии

Объединение АРМ в ЛВС в пределах подразделения и организация взаимодействия ЛВС разных подразделений между собой. Как правило, создается корпоративная ЛВС, в которой действует единая ИТ-политика, и к которой подключается максимально возможное количество подразделений, участвующих в разработке изделий.

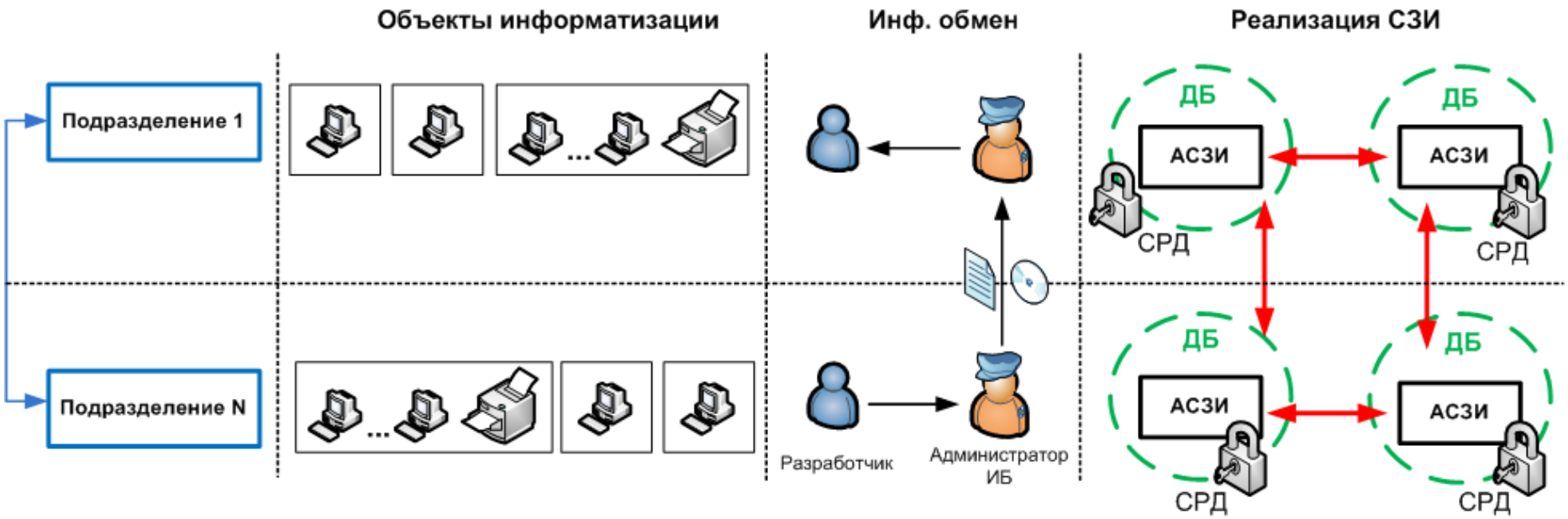
Стадия 3 –Взаимодействие в рамках кооперационных цепочек

Организация информационного обмена между АСЗИ нескольких участников взаимодействия (разных предприятий) в рамках кооперационных цепочек. Передача данных между АСЗИ разных участников может осуществляться как на носителях информации, так и по каналам связи с использованием криптошлюзов.

Стадия 4 – Создание единого информационного пространства (ЕИП) Предприятий при управлении полным жизненным циклом изделий

Внедрение различных информационных систем (ИС) с целью автоматизации бизнес-процессов, в том числе ИС поддержки жизненного цикла изделий. Для стадии характерна интеграция ЕИП нескольких предприятий.

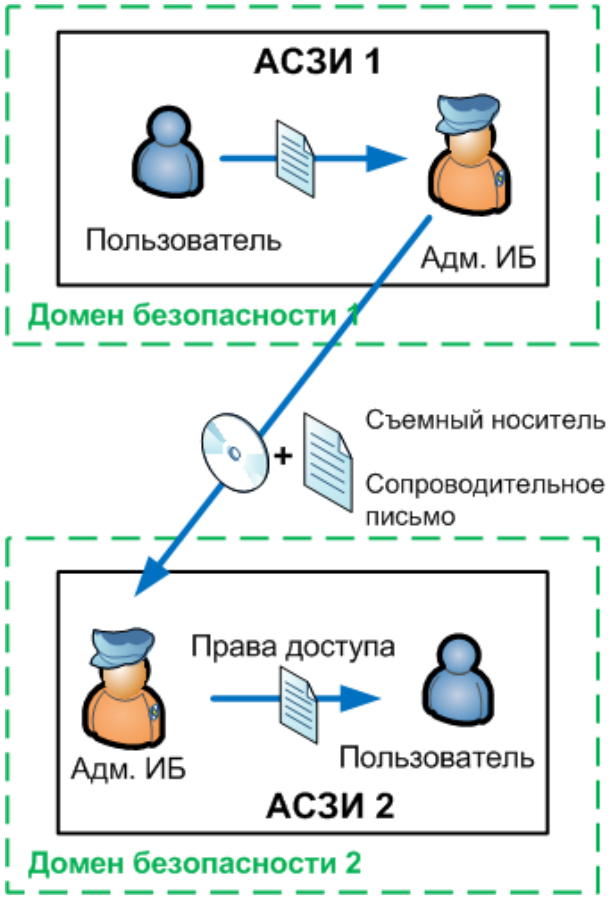
Стадия 1. Локальная автоматизация



На Предприятии функционирует множество не связанных между собой АСЗИ. Каждая АСЗИ имеет собственный домен безопасности и систему разграничения Доступа.

ИБ обеспечивается использованием серийно выпускаемых сертифицированных средств защиты информации.

Ограничения ИБ при обмене данными между разными АСЗИ



Обмен данными между АСЗИ требует обязательного участия администратора информационной безопасности

<u>Причины возникновения ограничения:</u>

1. Каждая АСЗИ является отдельным доменом безопасности со своим пространством субъектов доступа. Каждая АСЗИ имеет собственную систему разграничения доступа (СРД), не пересекающуюся с СРД других АСЗИ.
2. На импортированные файлы должны быть назначены права доступа в соответствии с действующей СРД.
3. Право изменять правила разграничения доступа в соответствии с требованиями РД СВТ предоставляется только выделенным субъектам (администратору ИБ).

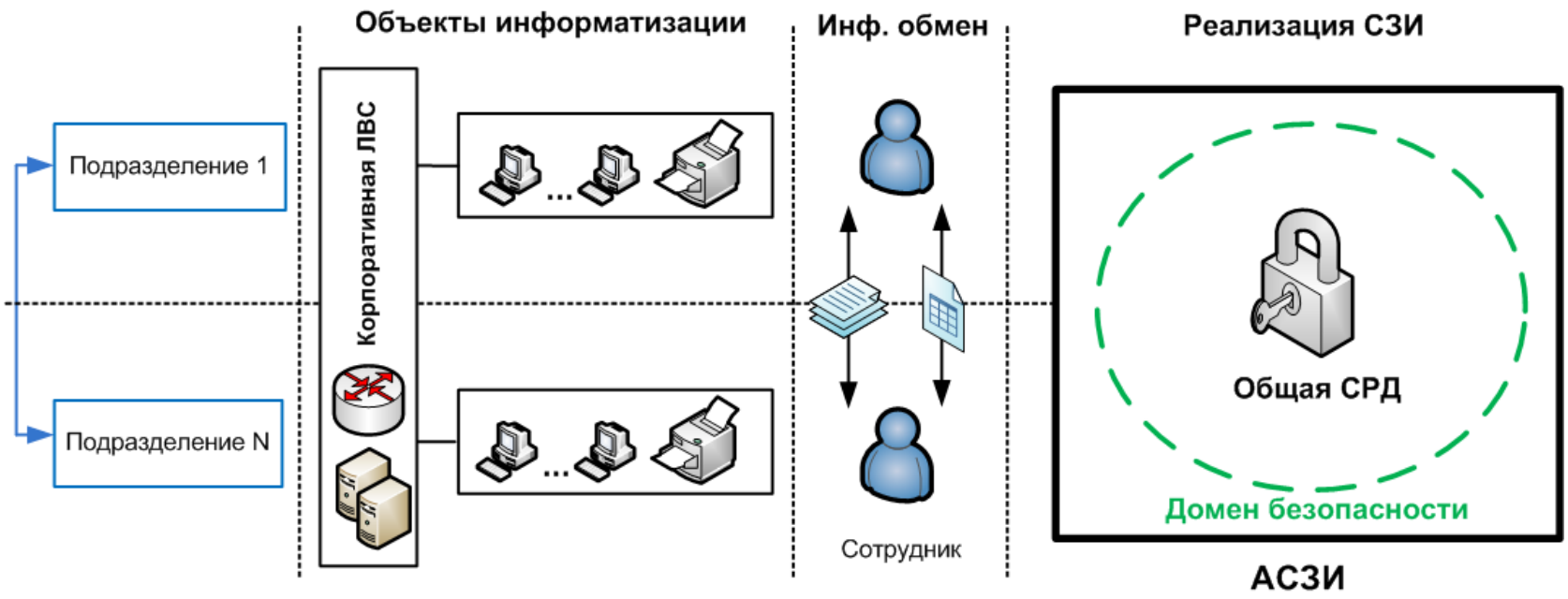
<u>Следствия ограничения:</u>

Невозможность реализации технологического цикла обработки информации, требующего большой частоты обмена данными или автоматического обмена.

<u>Пути обхода ограничения:</u>

Сертификация ППО по требованиям ИБ с интеграцией с СЗИ.

Стадия 2. Взаимодействие разных подразделений на Предприятии

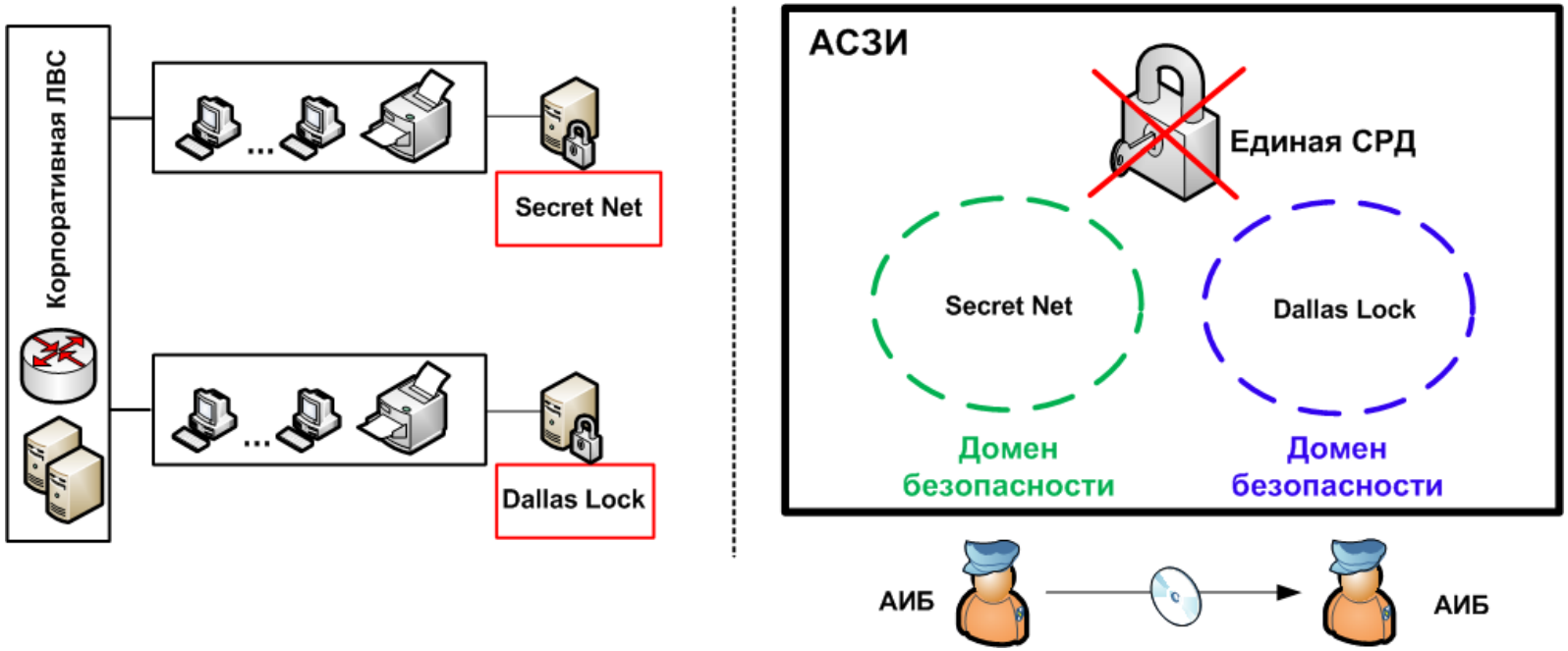


Организация информационного взаимодействия нескольких подразделений, участвующих в разработке изделий, в рамках одной АСЗИ.

Обмен данными в рамках одной АСЗИ не требует участия администраторов ИБ.

Участники обработки информации - сотрудники разных подразделений, в том числе военной приемки; увеличивается территориальная распределенность.

Ограничение по применению разных типов СЗИ от НСД в одной АСЗИ



Причина возникновения:

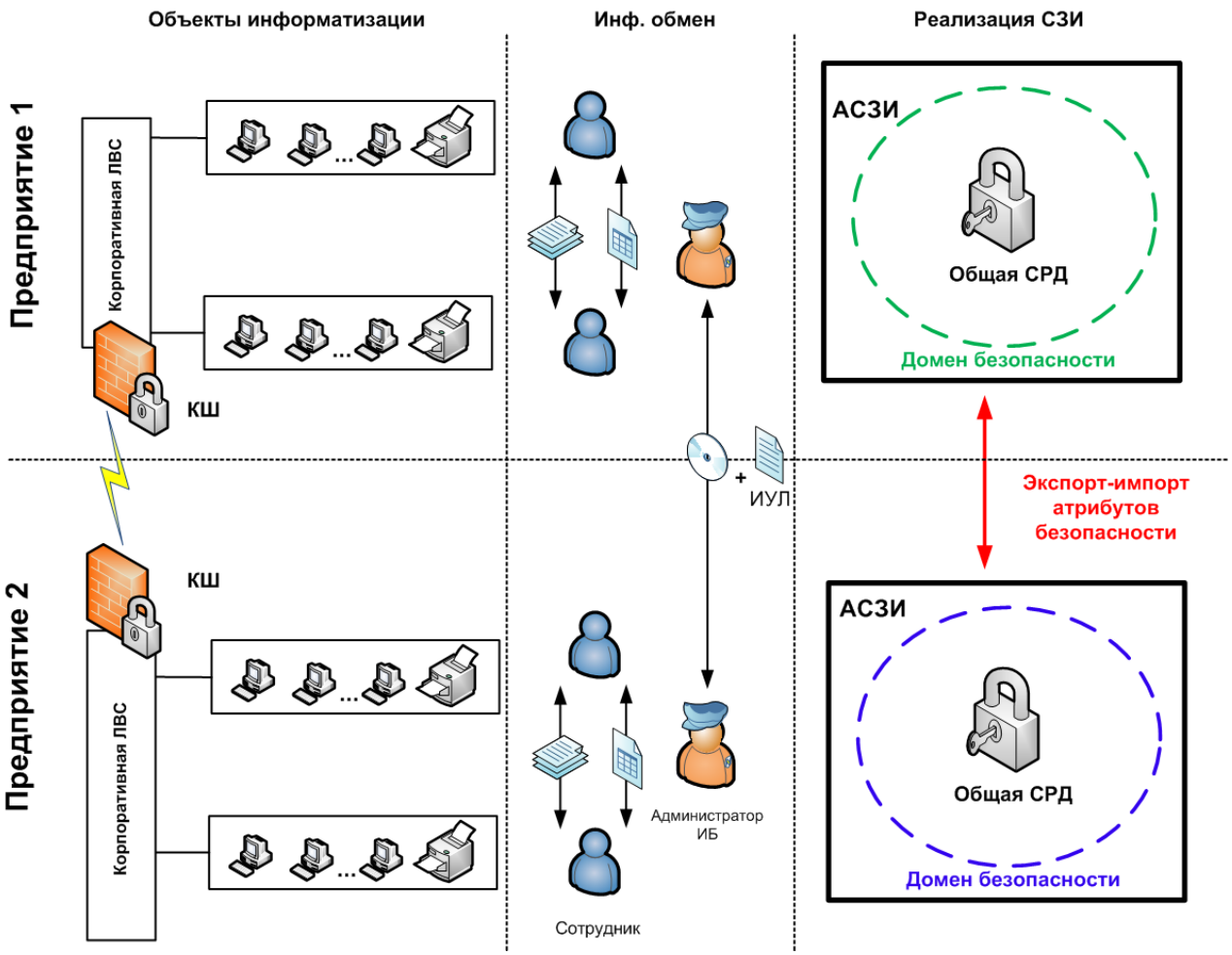
Различные типы средств защиты несовместимы между собой по формату атрибутов безопасности (дискреционные права, мандатные метки) и форме представления имен пользователей.

Следствие ограничения:

Невозможно организовать взаимодействие нескольких подразделений в одной АСЗИ без участия администраторов ИБ.

Стадия 3. Взаимодействие Предприятий в рамках кооперационных цепочек

Организация информационного взаимодействия между несколькими участниками (в т.ч. разной ведомственной принадлежности).



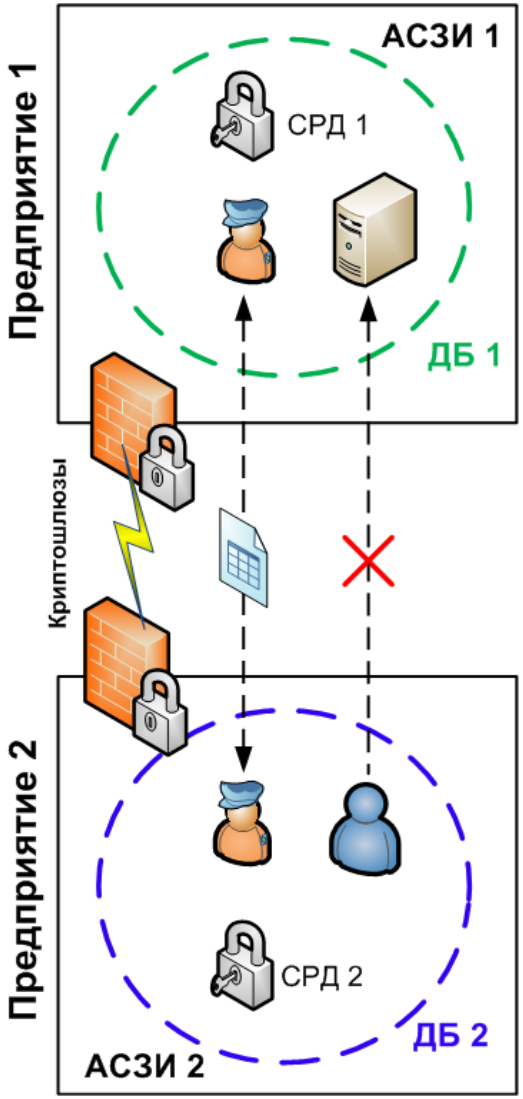
АСЗИ каждого предприятия имеет собственную СРД, не пересекающуюся с СРД других Предприятий.

Способы обмена данными:

1.по каналам связи с использованием криптошлюзов.

2.на носителях информации с информационно-удостоверяющими листами.

Ограничения ИБ при взаимодействии между АСЗИ разных участников обмена



Сложность организации взаимодействия разных предприятий при организации единого технологического цикла обработки информации

<u>Причины ограничения:</u>

1. Значительные организационные сложности в допуске пользователей к АСЗИ, принадлежащей другому юридическому лицу (в т.ч. разной ведомственной принадлежности).

2. Сложность объединения двух аттестованных АСЗИ, принадлежащих разным юридическим лицам (в т.ч. разной ведомственной принадлежности) в одну АСЗИ.

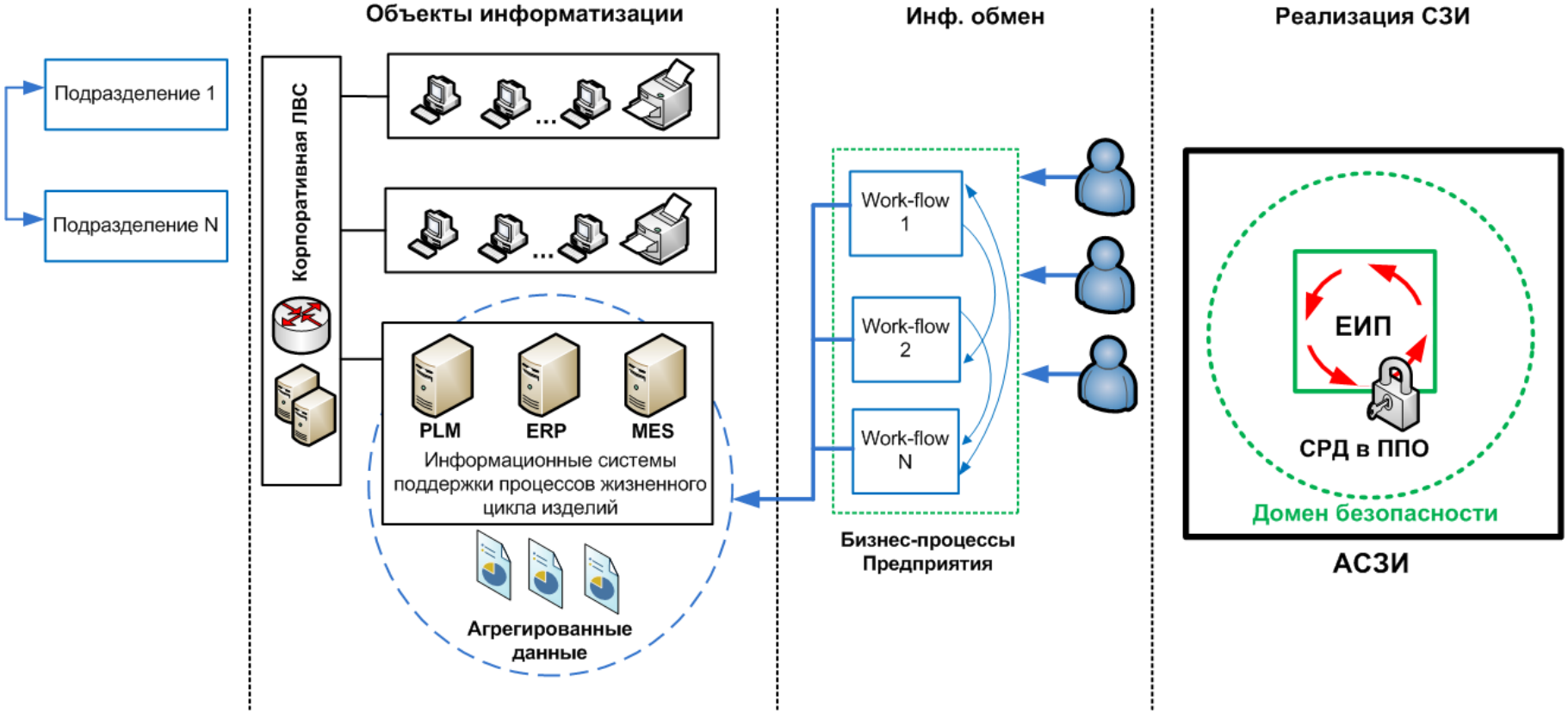
<u>Следствия ограничения аналогичны второй стадии.</u>

<u>Способ обхода ограничения:</u>

1. Требуется уточнение нормативных требований, регламентирующих автоматизированный обмен данными между аттестованными АСЗИ.

2. Требуется разработка и сертификация специализированного ПО, реализующего процедуры полностью автоматизированного обмена. Данное ПО должно обеспечивать передачу атрибутов безопасности между СРД разных АЗСИ.

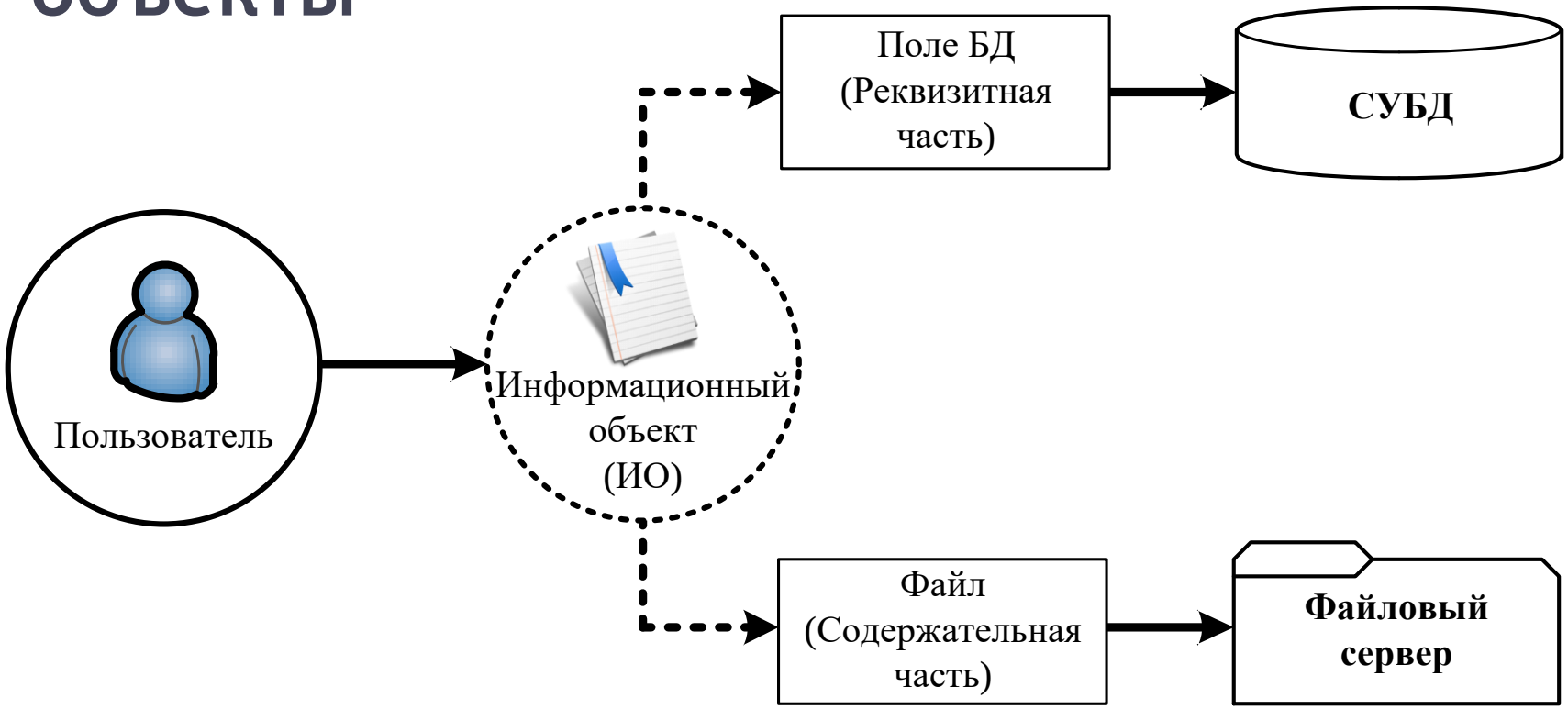
Стадия 4. Внедрение ЕИП на Предприятиях



Внедрение различных ИС с целью автоматизации бизнес-процессов Предприятия, в том числе ИС поддержки процессов жизненного цикла изделий (PLM, ERP, MES и др.).

Осуществляется переход от обработки данных в виде файлов к обработке агрегированных данных (файлы и поля данных в БД). В качестве объекта защиты появляется технологический процесс обработки информации.

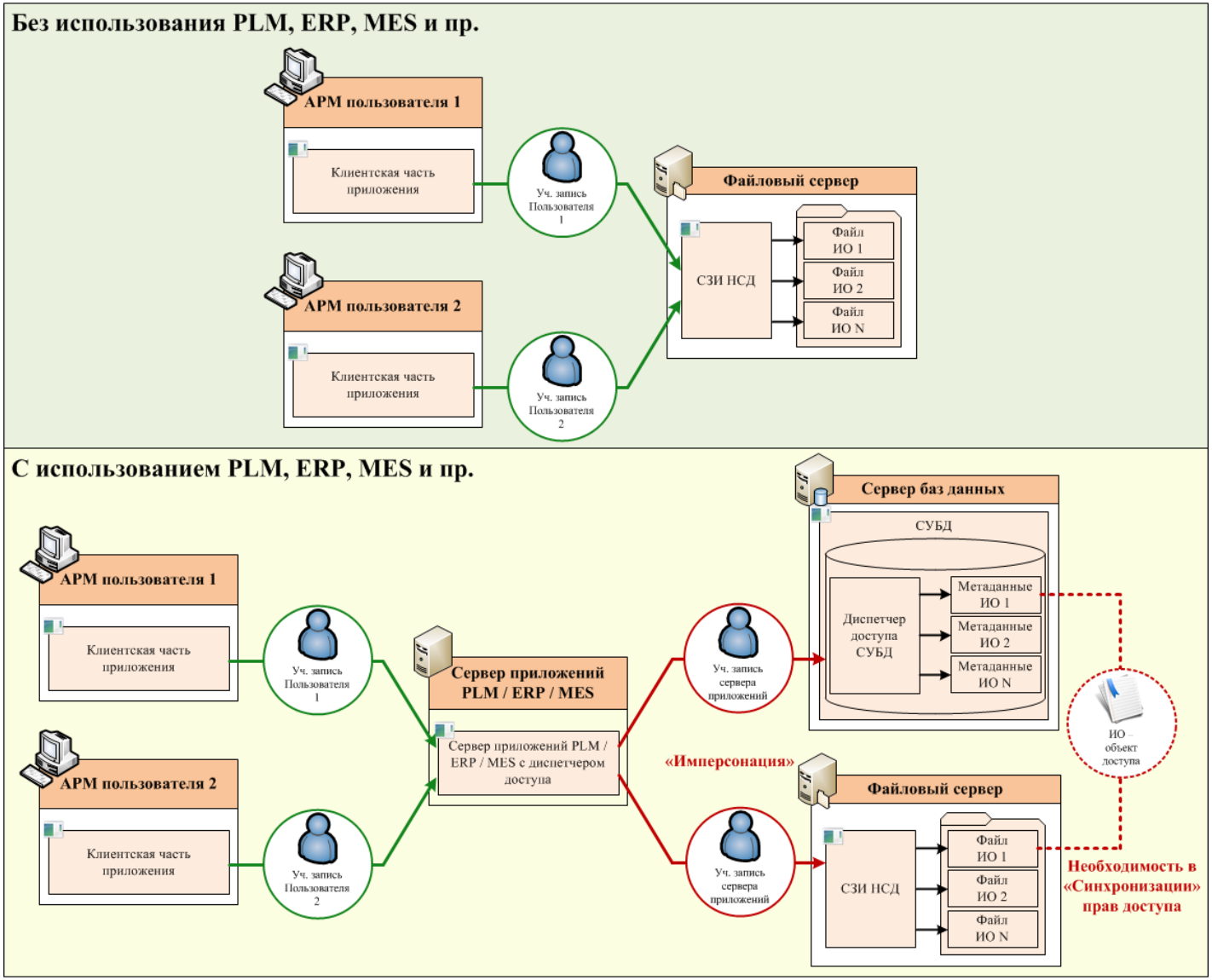
Агрегированные информационные объекты



В PLM-, MES-, ERP-системах в качестве объектов доступа выступает **информационный объект**, состоящий одновременно из полей СУБД и файлов.

Переход к стадии **создания единого информационного пространства** невозможен без использования агрегированных ИО.

СЗИ от НСД не обеспечивает защиту на прикладном уровне



Применение серийно выпускаемых «наложенных» средств защиты информации (СрЗИ) недостаточно для защиты PLM-, MES-, ERP-систем.

Поток данных, который невозможно контролировать «наложенными» СрЗИ.

Поток данных, контролируемый «наложенными» СрЗИ.

Обязательность сертификации прикладного ПО (PLM, ERP, MES и др.) по требованиям безопасности информации

Источник ограничения (приказ ФСТЭК № 31 от 28 февраля 2017 года (пп. 10 и 11):

1. Ввод в действие АСУ ЖЦИ (или ее элементов как ИС) возможен только после создания системы защиты информации и аттестации системы по требованиям безопасности информации.

2. Все механизмы защиты должны соответствовать требованиям к установленному классу защищенности и их надежность должна быть подтверждена в форме сертификационных испытаний всех механизмов защиты, ***включая встроенные в прикладное ПО средства защиты (п. 10 приказа № 31)***.

Причина возникновения:

Развитие технологии обработки информации в части появления объектов доступа прикладного уровня и необходимости управления потоками на прикладном уровне.

Следствия применения несертифицированного ППО:

1. Невозможность обработки информации разных грифов в одной информационной системе (PLM, ERP, MES и т.д.).

2. Формальное отсутствие системы разграничения доступа в АСУ ЖЦИ.

3. Сложности обеспечения юридической значимости документооборота.

Способы обхода ограничения:

1. Отказ от части элементов сквозного цикла (автоматизация только отдельных участков, невозможность автоматизированной обработки полной информации об Изделии, невозможность перехода на электронный документооборот и др.).

2. Реализация сложных архитектурных решений (сегментация АСУ ЖЦИ, отказ от системы разграничения доступа и т.д.) с целью выполнения требований ИБ.

3. Доработка и сертификация ППО.

Ограничения применения ППО импортной разработки

Причина возникновения ограничения:

Нормативными документами по сертификации предусмотрено обязательное предоставление исходных текстов на ПО для обработки ГТ в качестве СрЗИ. По сложившейся практике вендоры крайне редко предоставляют исходные коды.

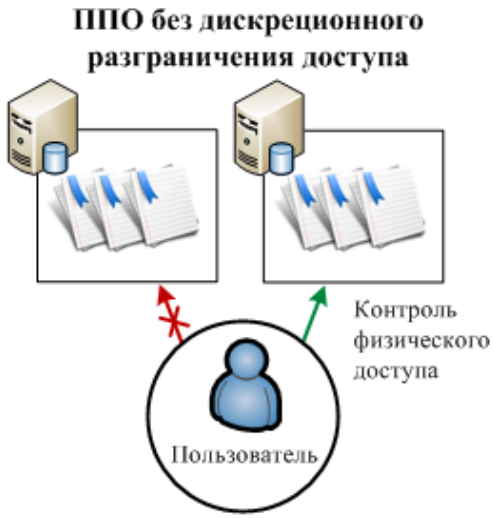
Следствия ограничения:

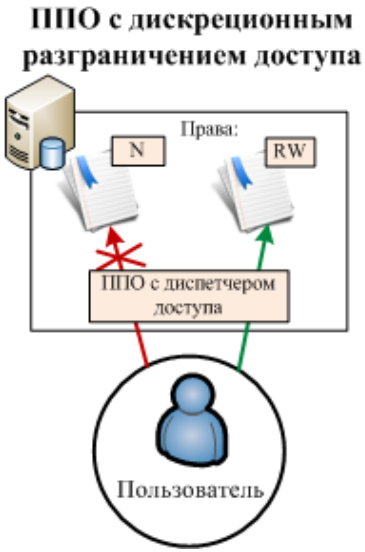
Невозможность использования импортного прикладного и базового ПО (ОС и СУБД), сертифицированного в качестве СрЗИ для создания системы разграничения доступа и управления потоками.

Влияние ограничения на архитектуру АСЗИ:

1. Отсутствует возможность выгрузки данных с учетом мандатной метки (все выгружаемые данные имеют максимальный гриф).
2. Все пользователи допущены ко всему массиву защищаемой информации (фактически система 1В вырождается в совокупность подсистем 2А).

Доступ пользователей ко всем информационным ресурсам в АСУ ЖЦИ





Причина возникновения:

Использование в АСУ ЖЦИ ППО, не имеющего сертифицированной системы дискреционного разграничения доступа.

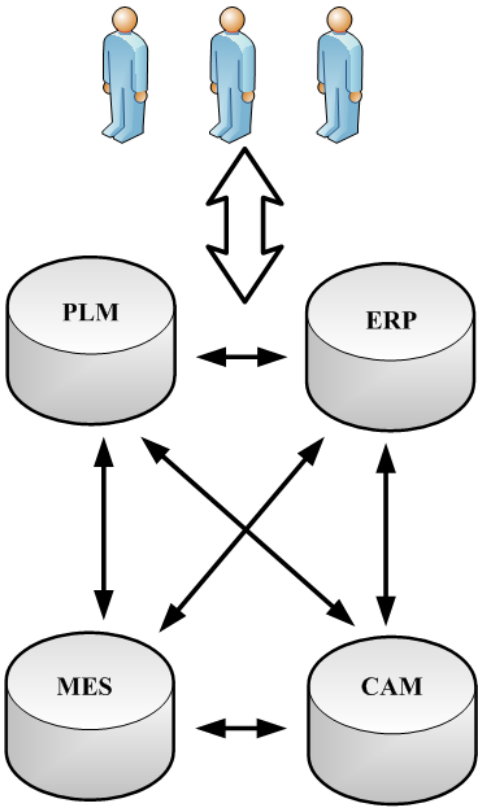
Следствие ограничения:

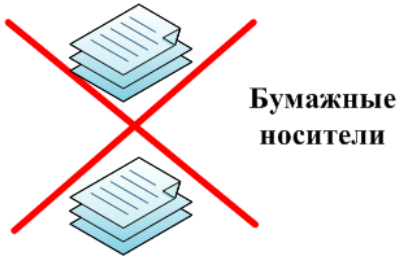
Отсутствие механизма дискреционного разграничения доступа в ППО (по матрице доступа).

Пути обхода ограничения:

Создание нескольких АСЗИ в составе АСУ ЖЦИ и управление доступом пользователей физически.

Ограничения ИБ по обеспечению юридической значимости документооборота в АСУ ЖЦИ





Источник ограничения:

1. Необходимость разработки и согласования всех видов документации в электронной форме.

2. Документация, обрабатываемая в АСУ ЖЦИ должна иметь статус подлинника.

Причина возникновения:

1. Крайне ограниченный выбор сертифицированных решений по применению электронной подписи в контуре ГТ.

2. Для применения ЭП необходимо провести контроль корректности встраивания средств криптографической защиты (СКЗИ) в ППО СРД.

3. Министерством обороны не предусмотрен прием документации в электронной форме как основной вариант приемки и сопровождения изделий.

Следствие ограничения:

1. Сложность перехода на разработку и согласование документации в электронной форме по всему изделию при наличии секретных документов.

2. Невозможность сократить трудовые и временные затраты на разработку в документацию и выпуск изменений.

Способы обхода ограничения:

1. Отказ от юридически значимого документооборота в контуре ГТ.

2. Каждое предприятие ОПК проводит контроль корректности встраивания в индивидуальном порядке.

Эффективное решение вопросов ИБ в АСУ ЖЦИ позволяет существенно снизить затраты, но это требует системного подхода

Применение импортного прикладного ПО связано с ограничениями на реализацию сквозного цикла проектирования и производства изделий.

Сертификация отечественного прикладного ПО по требованиям безопасности информации не имеет широкой практики и связано в свою очередь с другими вопросами системного характера:

Отсутствие тиражируемых решений по применению сертифицированного общесистемного программного обеспечения импортного производства (ОС и СУБД).

Существующее отечественное общесистемное ПО (ОС и СУБД) по мнению разработчиков прикладного ПО **не в полной мере позволяет обеспечить** заданные технологические характеристики информационной системы по производительности и функциональности.

На уровне остальных базовых элементов ИКТ существенно ограничен выбор импортозамещающих элементов среды виртуализации, СХД и телекоммуникационного оборудования, соответствующих требованиям безопасности информации.

Системные вопросы ИБ в АСУ ЖЦИ

1. Вопросы сертификации:

На уровне прикладного ПО есть существенные препятствия для сертификации сложных комплексов, взаимодействующих с промышленными импортными СУБД и средствами защиты от НСД.

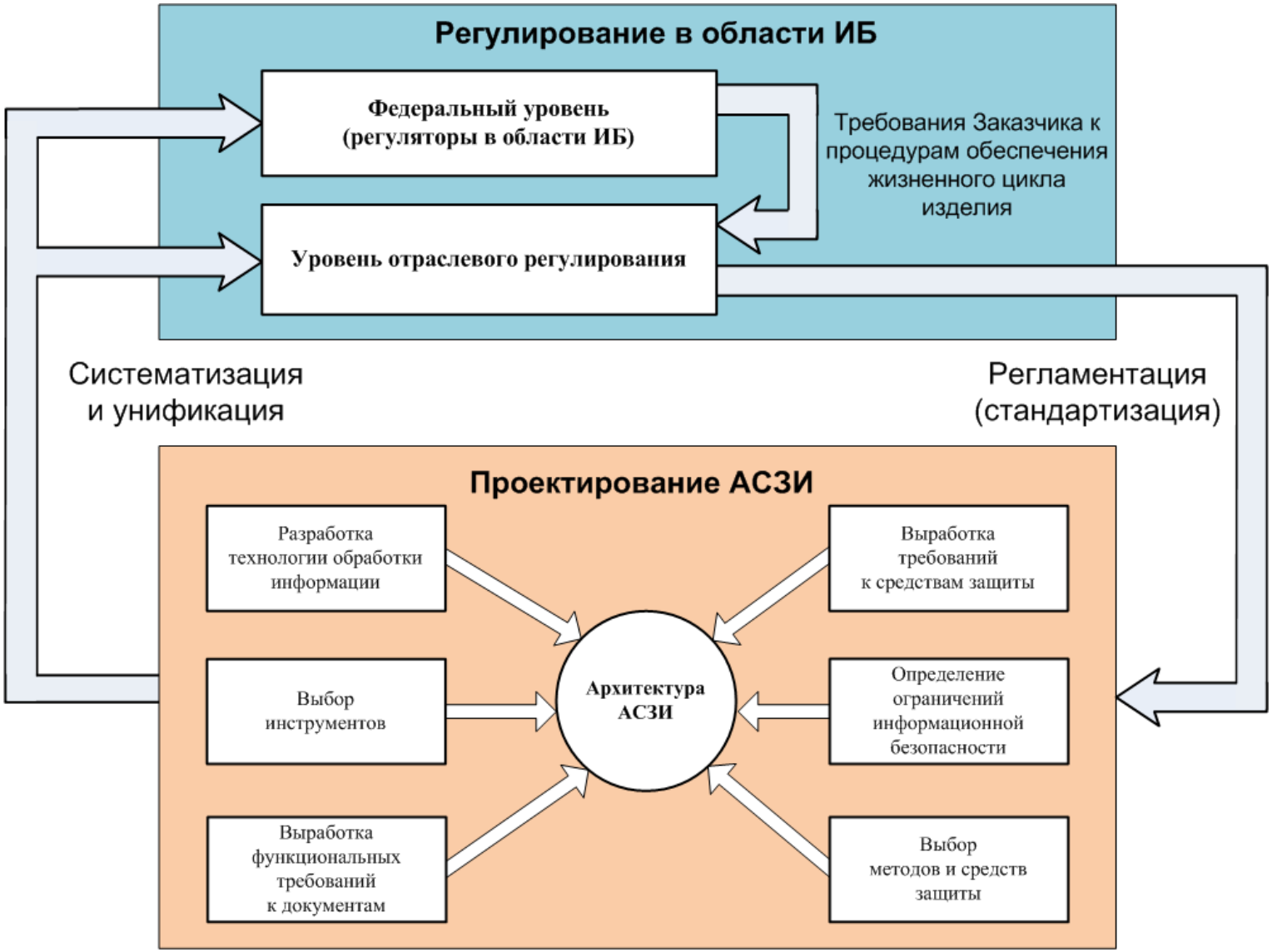
На уровне общесистемного ПО и СУБД есть существенные технологические ограничения по применению отечественных операционных систем и СУБД.

На уровне остальных базовых элементов ИКТ существенно ограничен выбор импортозамещающих элементов среды виртуализации, СХД и телекоммуникационного оборудования.

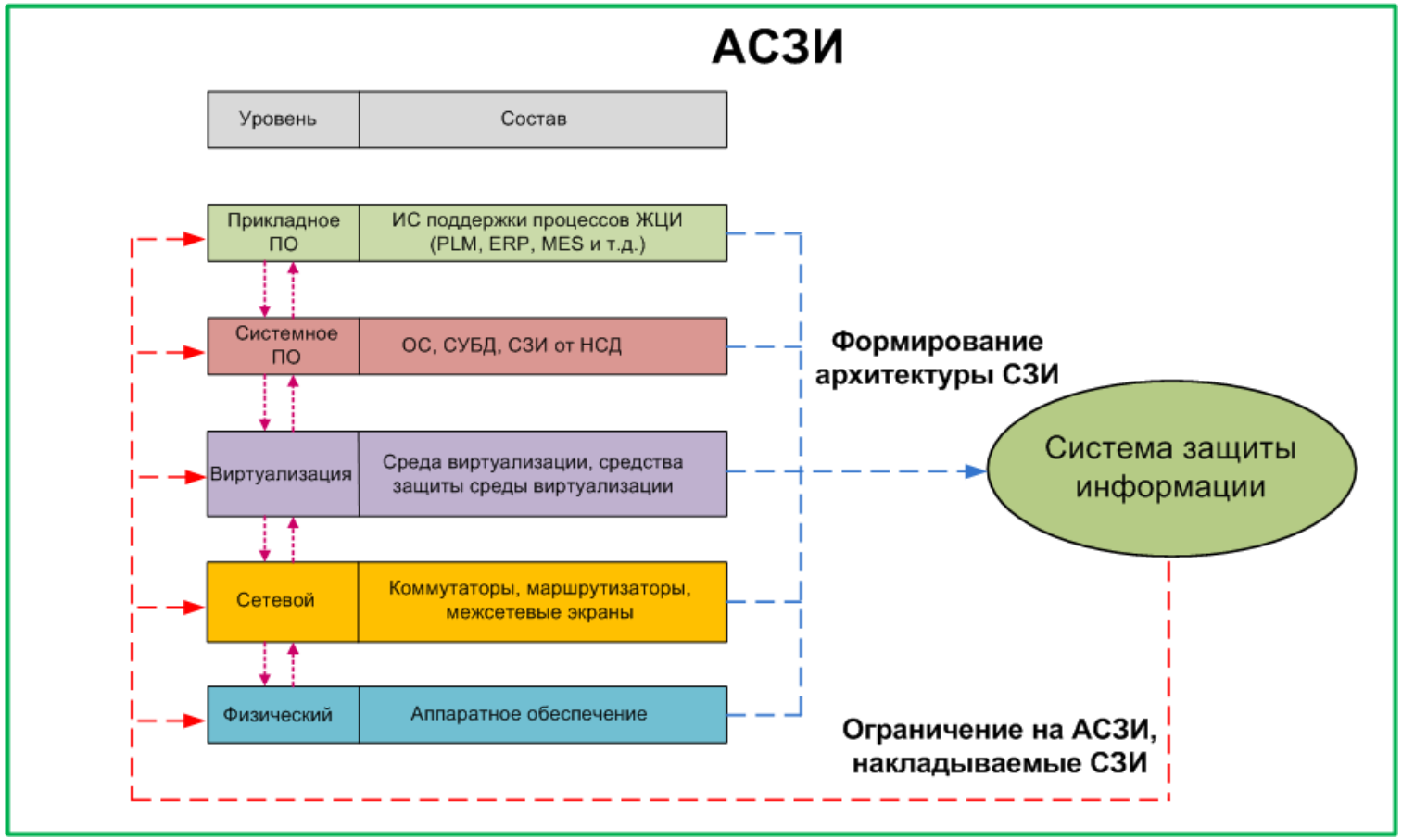
2. Вопросы проектирования:

Как правило, создание АСЗИ ведется «от частных задач» и отталкиваясь от ограничений и функционала заранее выбранных или уже закупленных прикладных комплексов и средств защиты без учета функциональной и информационной моделей АСЗИ.

Проектирование АСУ ЖЦИ



Ограничения, накладываемые СЗИ, на ИКТ



Конкретная реализация архитектуры СЗИ определена только для конкретного взаимоувязанного комплекса компонентов ИКТ АСЗИ.

Изменения состава компонентов ИКТ может повлечь необходимость разработки новой архитектуры СЗИ и переаттестации АСЗИ.

Формат взаимодействия участников

Нормативная база по защите информации должна учитывать изменяющиеся потребности отрасли.