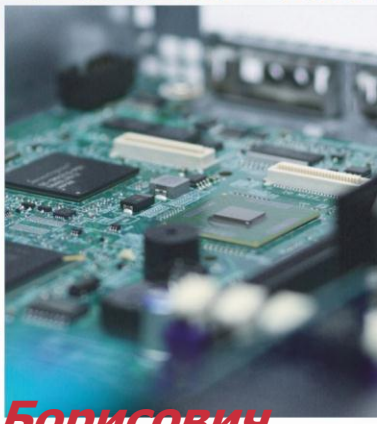
RTSoft
средства и системы автоматизации

Применение технологии встраиваемых периметров защиты в критически важных информационно-управляющих системах






Здирук Константин Борисович
главный специалист Технической дирекции АИУС ПП ЗАО «РТСофт», кандидат технических наук

Предлагаемая классификация используемого программного обеспечения КВИУС на основе критериев доверия

Обобщенные критерии доверия (ОКД) D[3]:

d_1 - авторизация кода (авторы/правообладатели – резиденты РФ, независимое подтверждение авторства и лицензионной чистоты кода)

d_2 – представление комплекта конструкторской и эксплуатационной документации в соответствии с ГОСТ ЕСКД (ЕСПД) РФ

d_3 - контроль (внешним) уполномоченным органом (ФСТЭК РФ, ФСБ РФ) всех этапов жизненного цикла программных изделий

Классы ПО:

АД – *(абсолютно) доверенные* (полное соответствие ОКД)

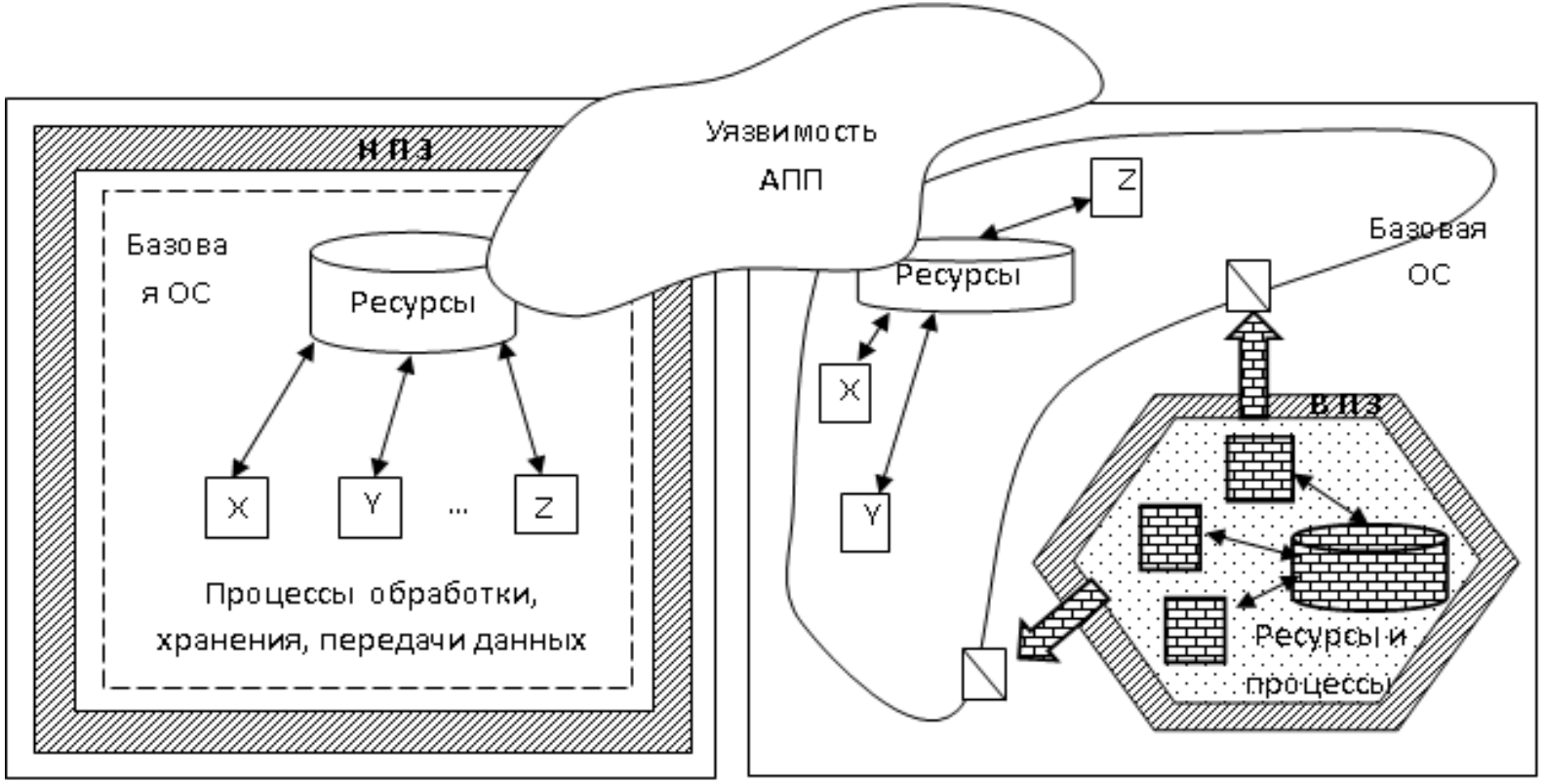
УД- *условно доверенные* (невыполнение хотя бы одного из ОКД)

НД- *недоверенные* (невыполнение всех ОКД, при этом, *показатель качества* ПО может превосходить аналогичные значения элементов других классов)

Общий методический подход:

Встраиваемые периметры защиты (ВПЗ) реализуются (только) АД-средствами !

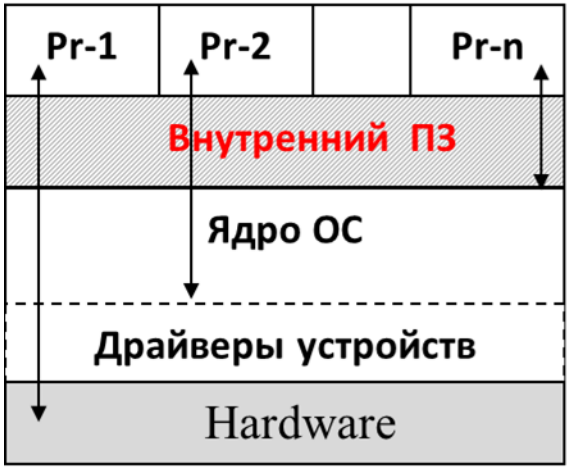
Совмещение встраиваемых (внутреннего и наложенного) периметров защиты в составе АПП

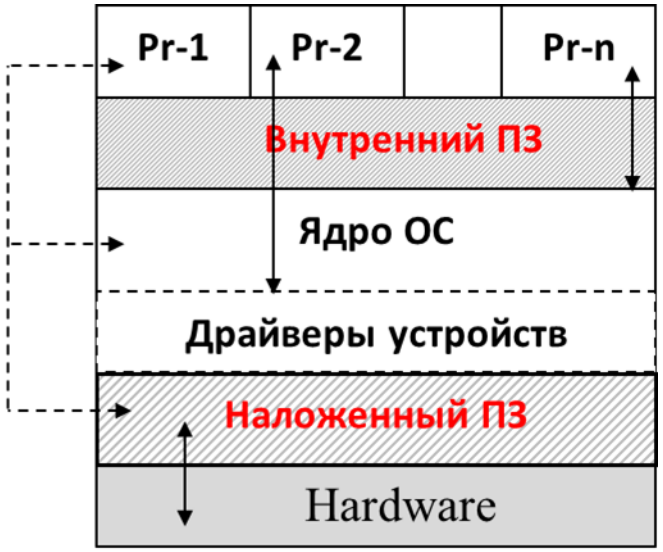


Особенности реализации:

1) организация на каждом узле изолированной от угроз со стороны базовой ОС защищенной области бескомпроматного хранения и передачи данных
2) объективный контроль и управление исполнением недоверенных приложений, помещенных в контейнер

Проблемы гарантированной нейтрализации актуальных угроз ИБ для современных АПП





Недостаточность внутреннего периметра защиты (ПЗ) для современных аппаратно-программных платформ:

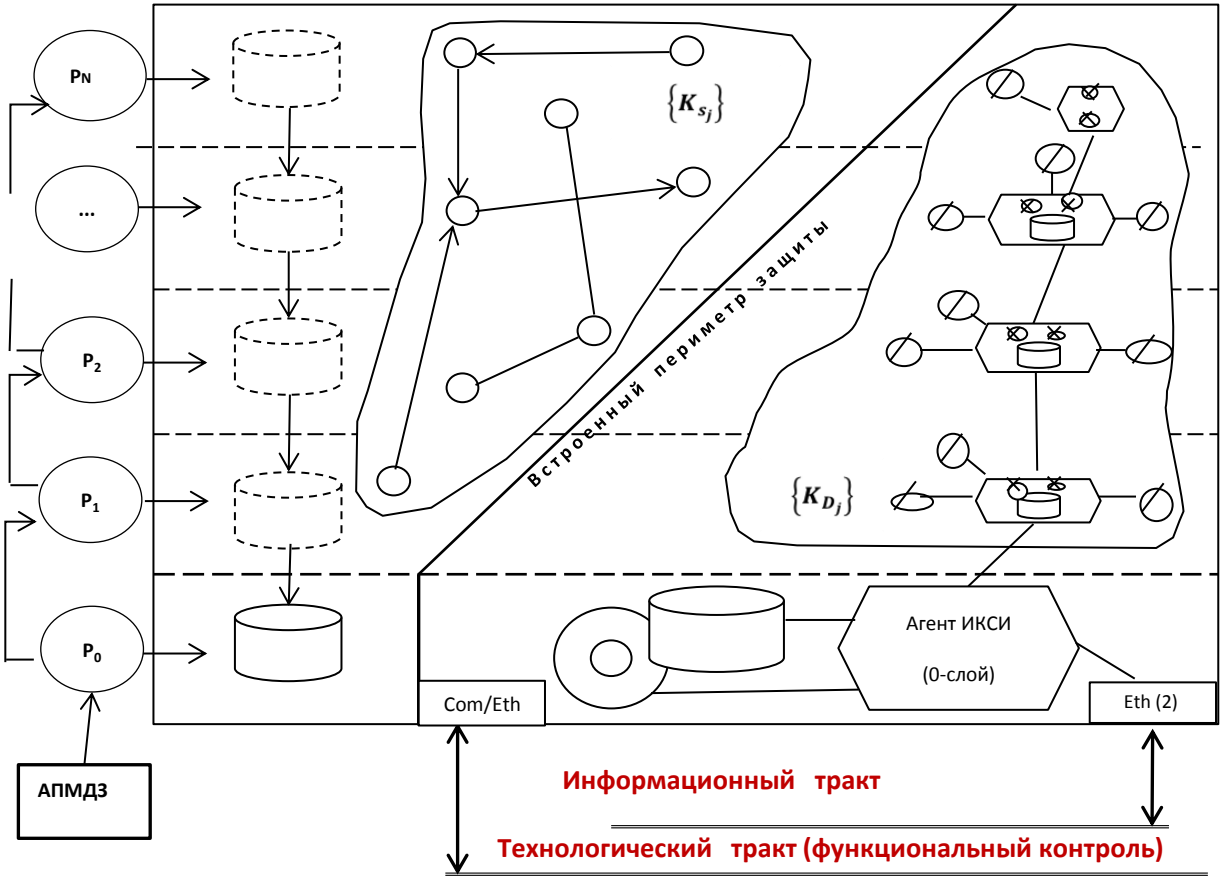
- **НД / УД код ядра ОС является *нейтральным* по отношению к функциональной системе** (возможно, включающим устраняемые *уязвимости*, но не содержащим *вредоносных,* относительно целевой системы, вложений*)*;
- ***все* запросы субъектов доступа (Pr) к объектам защиты *могут быть* перехвачены** наложенными средствами защиты либо ядром ОС.

Проблемы гарантированной нейтрализации актуальных угроз ИБ для современных АПП

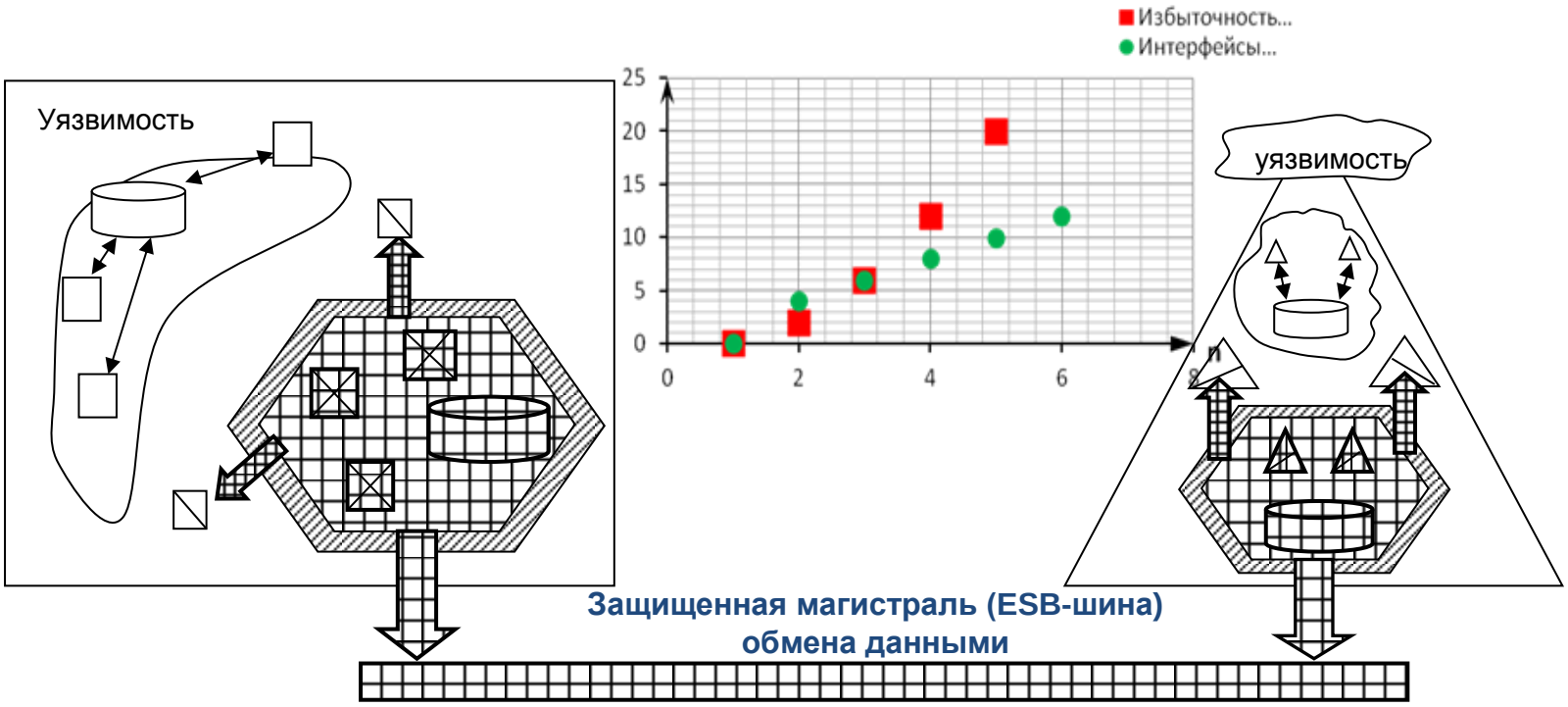
Внутренний периметр защиты изолирует множество недоверенных процессов K_S от доверенных K_D, при этом сетевые интерфейсы разделены и доступны только доверенной области.

Независимый канал внешнего управления (технологический тракт) обеспечивает регистрацию инцидентов и контроль состояния АПП и критически важных процессов обработки данных.

ИКСИ – доверенное ПО организации ВПЗ



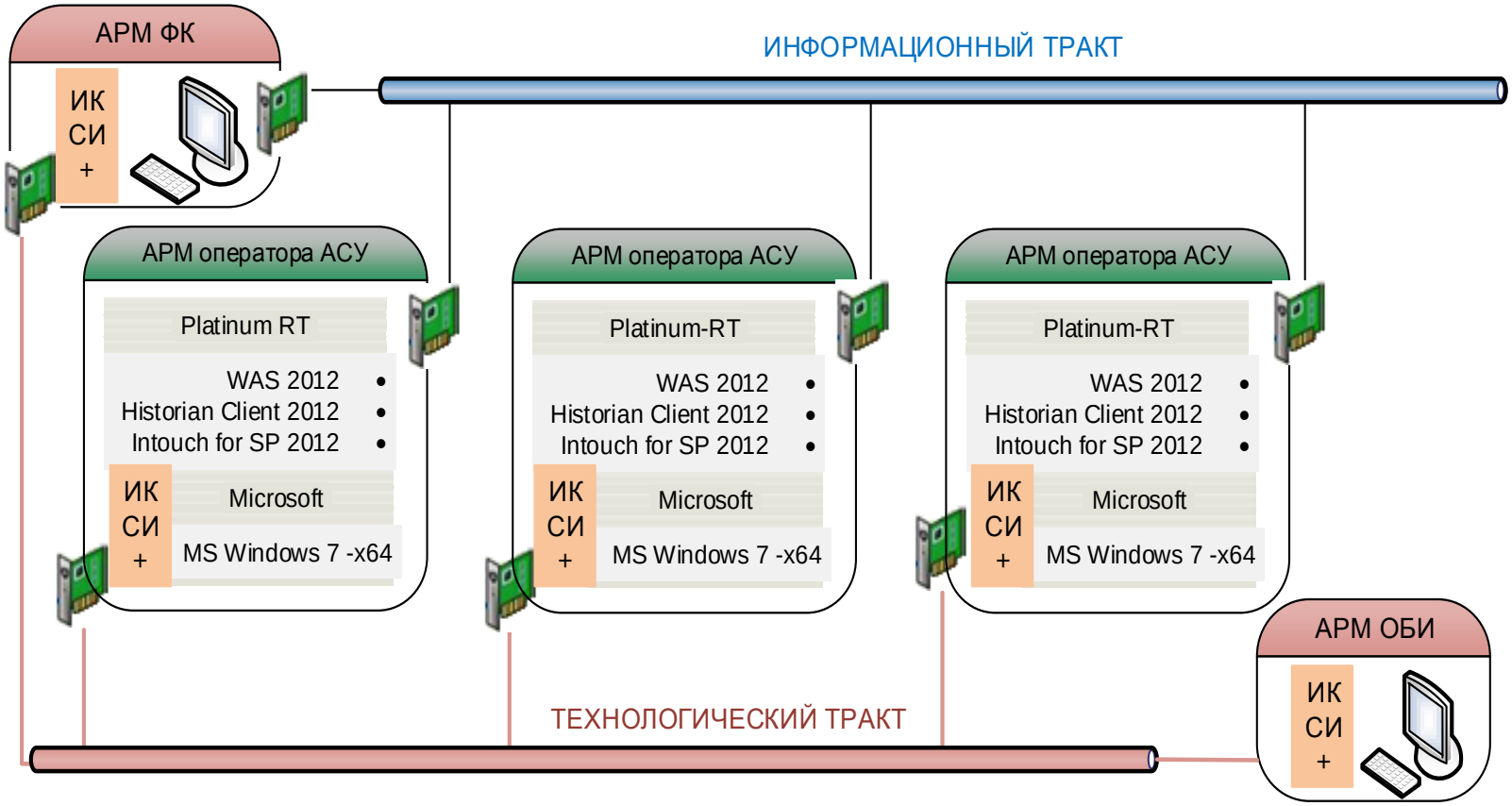
Унификация взаимодействия доверенных процессов разнородных АПП на основе использования свойств интероперабельности встраиваемых периметров защиты



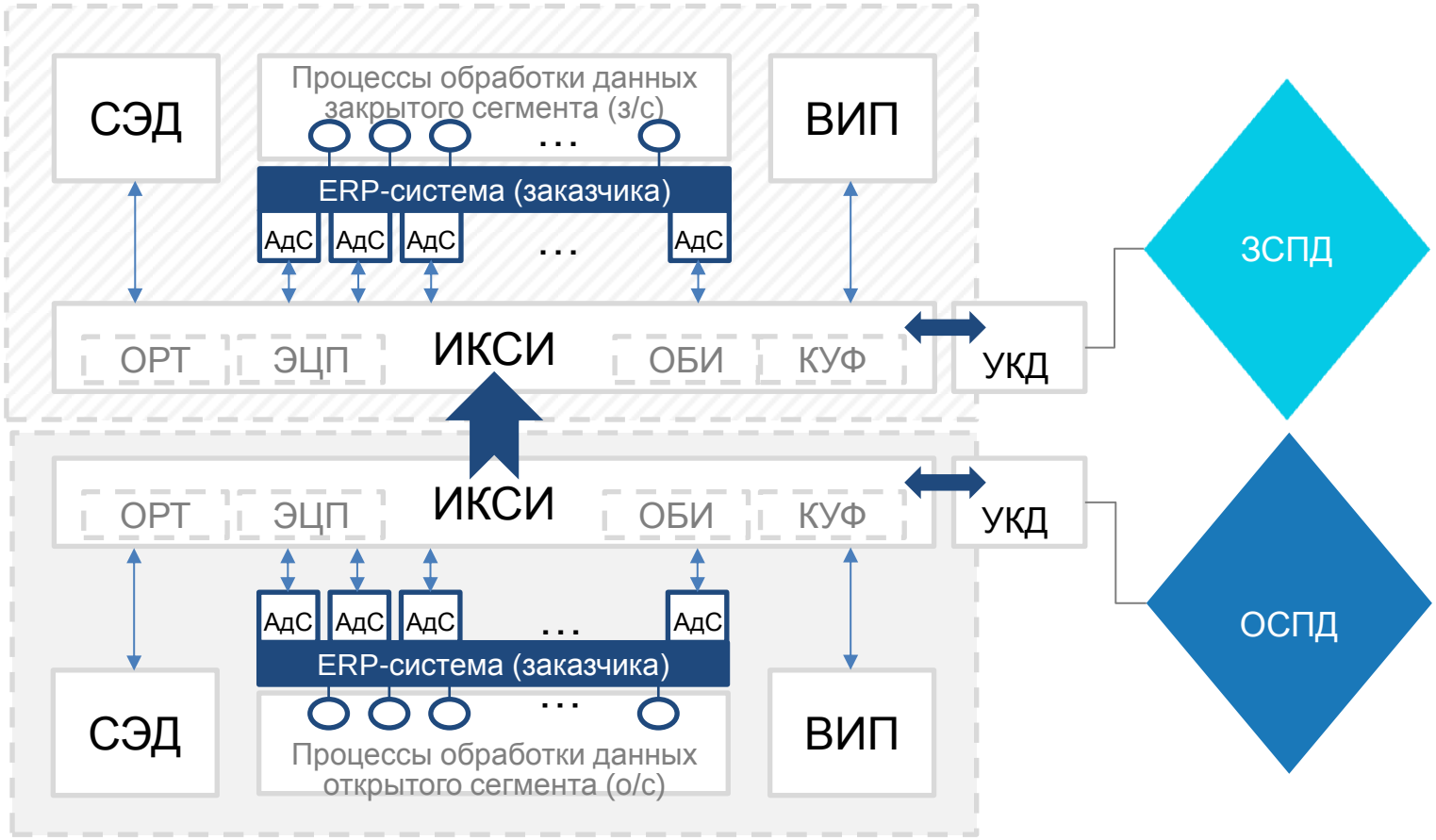
Классы защищаемых ресурсов:

ОП, файловая система, доверенные процессы, устройства I/O

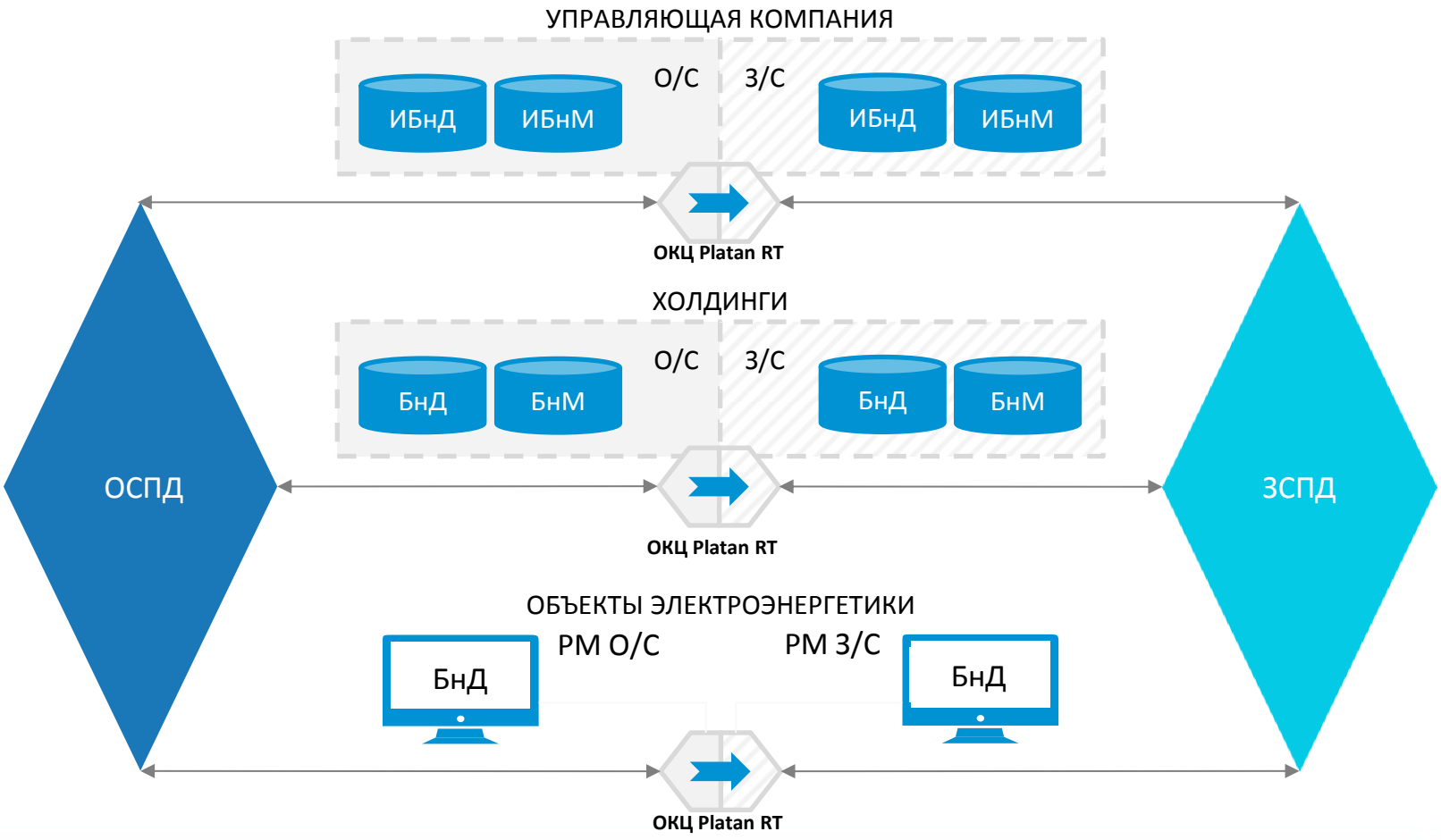
Раздельное применение технологического и информационного трактов обмена информацией в составе защищенного комплекта программ (ЗКП) «Plato RT»



Взаимодействие сегментов КВИУС, обрабатывающих информацию различных уровней конфиденциальности, посредством ОКЦ «Platan RT»



Взаимодействие объектов КВИУС, обрабатывающих информацию различных уровней конфиденциальности, посредством ОКЦ «Platan RT»



Спасибо за внимание!

Автор:

Здирук К.Б.

ЗАО «РТСофт»

Тел: (495) 742-68-28, 967-15-05

Факс: (495) 742-68-29

E-mail: rtsoft@rtsoft.msk.ru

http://www.rtsoft.ru