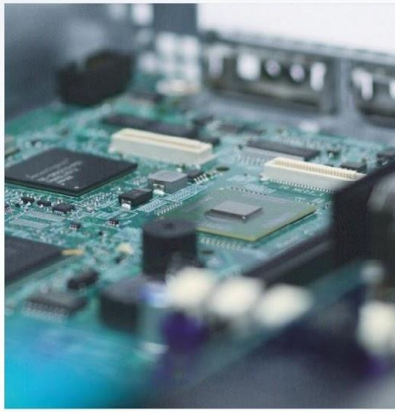
RTSoft
средства и системы автоматизации

Нейтрализация инсайдерских угроз функционированию программных компонентов на основе применения двухконтурной архитектуры безопасности PLATO-RT®.



Назначение и область применения «Plato RT»

Назначение:

Защищенный комплект программ (ЗКП) «Plato RT» предназначен для организации защищенной обработки конфиденциальных данных на объектах критически важных информационно-управляющих систем

Область применения:

- Автоматизированные системы управления технологическими процессами (АСУ ТП)
- Автоматизированные системы диспетчерского управления (АСОДУ)
- Автоматизированные систему управления производственными процессами (MES)
- Системы управления предприятием (ERP – системы)
- Информационно – аналитические системы, Информационно – управляющие системы

Состав ЗКП «Plato RT»

Состав ЗКП «Plato RT»:

- Комплект программ (КП) базовой версии программной инструментальной платформы (ПИП) «Wonderware System Platform»;
- Программный продукт (ПП) «PowerFactory»;
- Программный продукт компании GE «PowerOn™ Fusion»
- Программный продукт SAP HANA
- Программный комплекс средств защиты (КСЗ) ЗКП «Plato RT», включающий (Internal-IT):

  а) программный комплекс обеспечения безопасности информации (ПК ОБИ);

  б) программный комплекс функционального контроля (ПК ФК);

  в) программные интерфейсы (API) взаимодействия с функциональными подсистемами КСЗ ЗКП «Plato RT» (управления доступом, регистрации и учета, обеспечения целостности, технологического преобразования информации);

  г) подсистема хранения данных КСЗ;

  д) общесистемное программное обеспечение (ОСПО) – доверенная программная среда функционирования КСЗ, организуемая с использованием Инструментального комплекта средств интеграции БИГЕ.466451.099-01 (далее ИКСИ);

  е) комплект эксплуатационной документации на изделие.

Состав компонентов «Plato RT»

Доверенная защищенная платформа исполнения критически важных процессов «Plato-RT»

Системообразующие компоненты и решения

1. **Инструментальный комплект сервисов интеграции (ИКСИ)**

- **1.1. Транспортная служба гарантированной доставки данных (GRAF)**
- **1.2 Служба защищенного темпорального хранения M/D/T (SLON)**
- **1.3 Технологическая платформа интеграции приложений (CAPI)**
- **1.4 Платформа автоматизации процессов документооборота (Ъ)**

Вспомогательные компоненты

- **2. Контейнеры для защищенного функционирования программных продуктов (Wonderware System Platform)**
- **3. Агентство доступа к защищенной мобильно-стационарной сети передачи данных A-PORT**

Обеспечивающие подсистемы

4. Крипто-временной тоннель ТРОПА

4.1. «Машина времени» #- CHRONOSCOPE
4.2. Крипто-сервер #-ENIGMA

5. Интерактивный анализ ALBA-ВИП

5.1. Экспресс-анализ серий данных ALBA
5.2. Конструктор ВИП-анализа

- **6. Средства гарантированной изоляции БД и процессов CRM НЕЙТРИНО**

7.Система операционного управления ПРОКУРАТОР

7.1. Служба управления инфраструктурой СКИФ
7.2 Служба мониторинга критических процессов ОКО

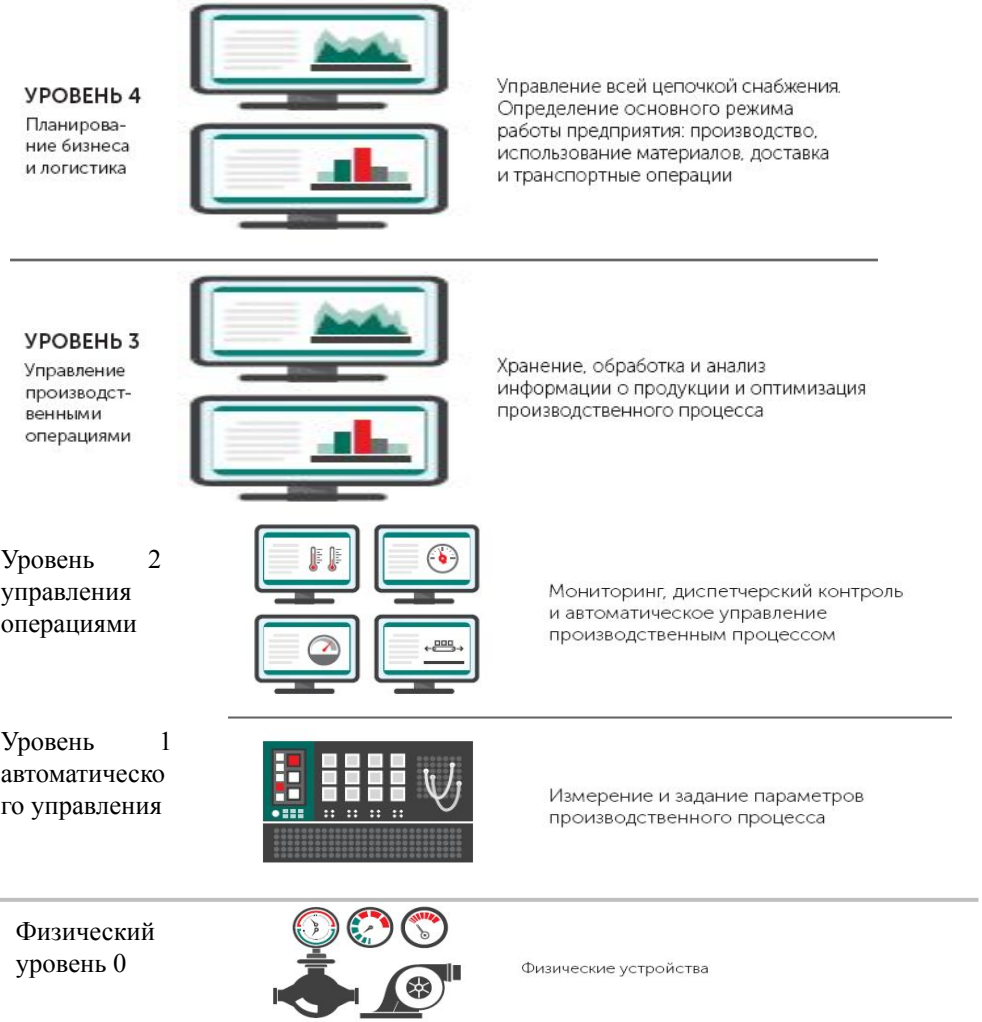
8. ПОЛИКУБ
Банк многомерных цифровых моделей объектов предметной области

ВОЗМОЖНОСТИ ПЛАТО-РТ

1. На уровне архитектуры изолируются все критически важные данные и процессы их обработки от любых деструктивных воздействий, как со стороны программных «закладок», вирусов, так и злоумышленников (информационных террористов, инсайдеров и др.).
2. Решение встраивается в существующую у заказчика вычислительную инфраструктуру и/или функционирует в отдельном (скрытом) сегменте сети.
3. Обеспечена возможность реализации на объектах заказчика консолидированной обработки сведений как открытого, так и ограниченного доступа с организацией взаимодействия изолированных информационных контуров (сегментов ЛВС), предназначенных для хранения и обработки данных различных уровней конфиденциальности.
4. В составе продукта реализовано 106 требований (63%) из 167, содержащихся в базовом наборе, определенном Приказом №31 2014г. ФСТЭК РФ).
5. Входящие в состав продукта технологии «бесшовной» интеграции гетерогенных процессов и БД, а также Банк цифровых моделей объектов предметной области (планируется к поставке с 02.2018 г.) реализуют соответствие концепции «Индустрии 4.0».

В целом, продукт применяется для построения высоконадежных, гарантированно защищенных сегментов критически важных систем в составе широкого класса систем: АСУ ТП, САЦ, ERP…

Подход к обеспечению промышленной информационной безопасности



ЗКП Plato_RT’

Модель угроз

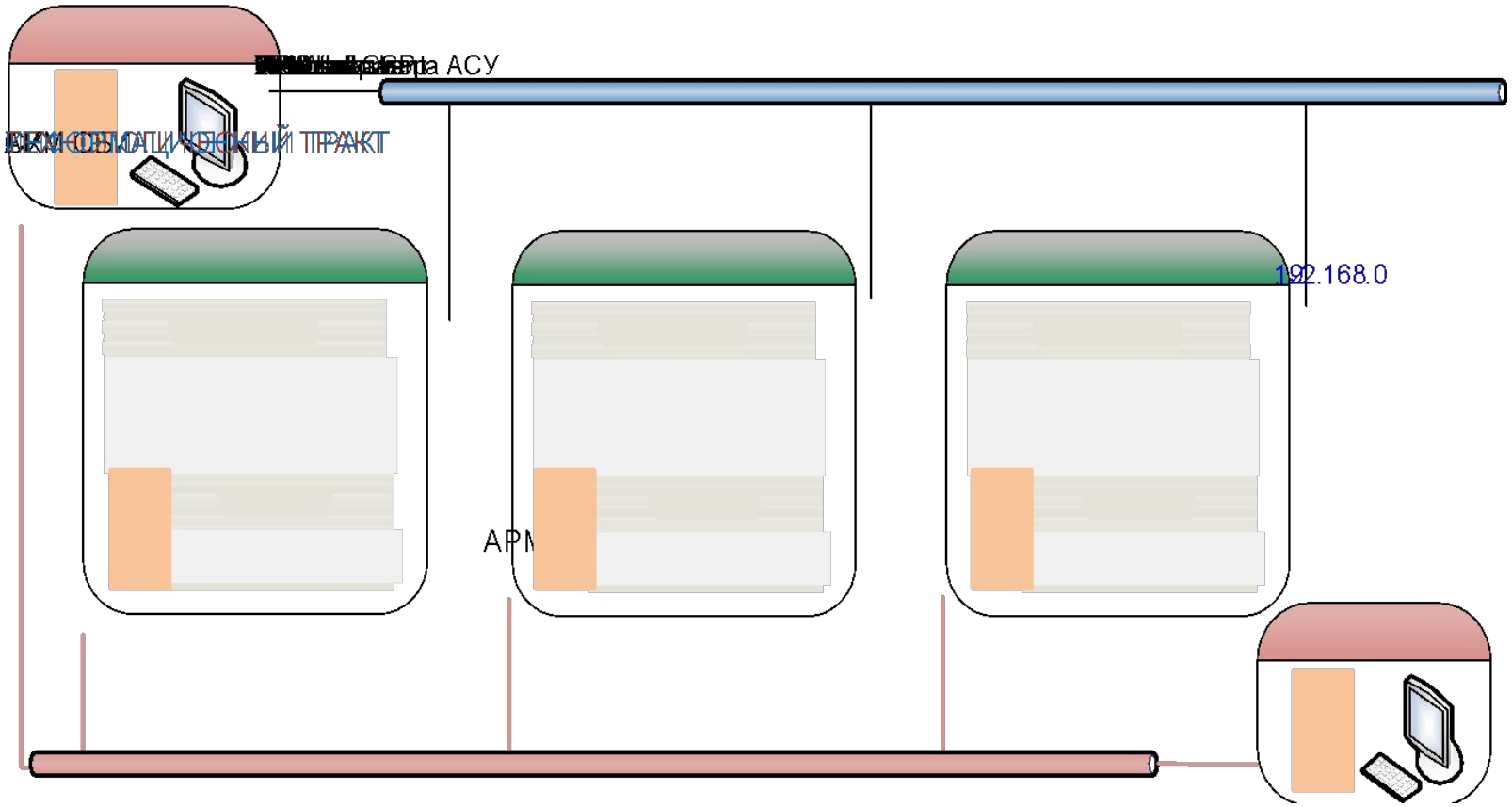
- **Внешний нарушитель:**
  - Вызов сбоев и внесение неисправностей в каналы передачи данных;
  - Несанкционированный доступ к защищаемой информации, передаваемой по каналам связи.
  - Добывание защищаемой информации за счет использования электронных устройств негласного получения информации,
  - Осуществление компьютерных атак в отношении оборудования и информационных ресурсов.

- **Организационно – технические мероприятия:**
  - размещение оборудования в строгом соответствии с требованиями предписаний;
  - Оборудование помещений в соответствии требованиями по защите информации
  - Физическая защита оборудования
  - Регламентация доступа персонала

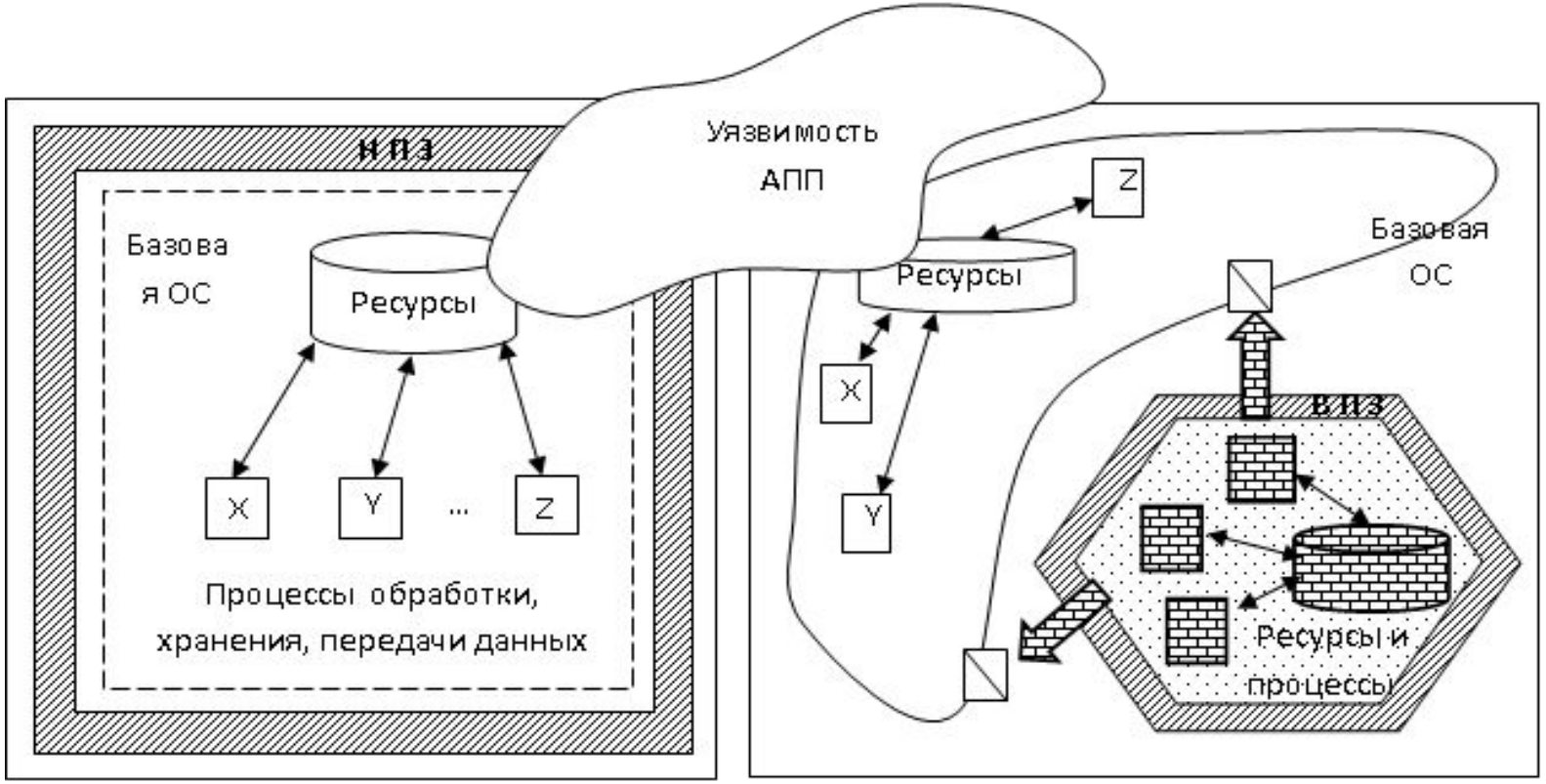
- **Внутренний нарушитель:**
  - Несанкционированное изъятие съемных носителей
  - Копирование защищаемой информации
  - Захват (копирование) машинных носителей защищаемой информации
  - Несанкционированное изменение состава технических средств изделия
  - Несанкционированная установка посторонних программных средств
  - Модификация ведущихся в электронном виде регистрационных протоколов
  - Внедрение вредоносного программного обеспечения
  - Скрытое (несанкционированное) использование вредоносным ПО привилегированных инструкций процессоров, поддерживающих аппаратную виртуализацию (AB),
  - Попытки преодоления системы защиты
  - Попытки несанкционированного доступа «внешних» объектов автоматизации к защищаемым ресурсам

1. **Организационно – технические мероприятия**
2. **Использование программно – аппаратных средств - Plato_RT**

Раздельное применение технологического и информационного трактов обмена информацией в составе ЗКП «Plato RT»



Совмещение встраиваемых периметров защиты - внутреннего (ВПЗ) и внешнего (НПЗ) в составе СВТ



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

Дополнительные функциональные возможности Плато-РТ

Что дает применение продукта различным категориям пользователей

Категория- I (руководство предприятия / организации)

Бескомпроматность хранения и передачи чувствительных для бизнеса (критических) данных, реализация организационно-распорядительных функций, доверенный (защищенный) обмен сообщениями и документами, вскрытие вредоносной активности и гарантированную (на уровне архитектуры) объективную регистрацию инцидентов безопасности. Организация дополнительного (встроенного) информационного контура, гарантированно защищенного как от внешних угроз (в лице любознательных искателей брешей в программном обеспечении), так и от внутренних - в лице инсайдеров.

Категория –II (оперативно-диспетчерская служба / конечные пользователи)

Минимизация количества ручных операций по авторизации абонентов и их работе в соответствии с заданным профилем, автоматический запуск/завершение технологических (регламентных) процессов, подготовка и рассылка итоговых отчетных документов о функционировании системы, реализации организационно-распорядительных функций.

Категория – III (специалисты подразделений автоматизации)

Оптимизация ресурсов (прежде всего – временны*х*) на реализацию полнофункционального объективного контроля текущего состояния и сопровождение территориально-распределенного вычислительного процесса на объектах заказчика (объективный контроль целостности технических и программных средств, смена версий, оперативность локализации сбоев/отказов и их устранения).

Категория IV (специалисты по ИБ /администраторы ОБИ)

Обеспечение службы ИБ сертифицированными (РД ФСТЭК) средствами, исключение каналов утечки чувствительной информации, разделение трактов управления функциональной и информационной безопасностью, гарантированное обнаружение и проактивная нейтрализация угроз, регламентированных моделью нарушителя (в том числе – инсайдерских угроз).

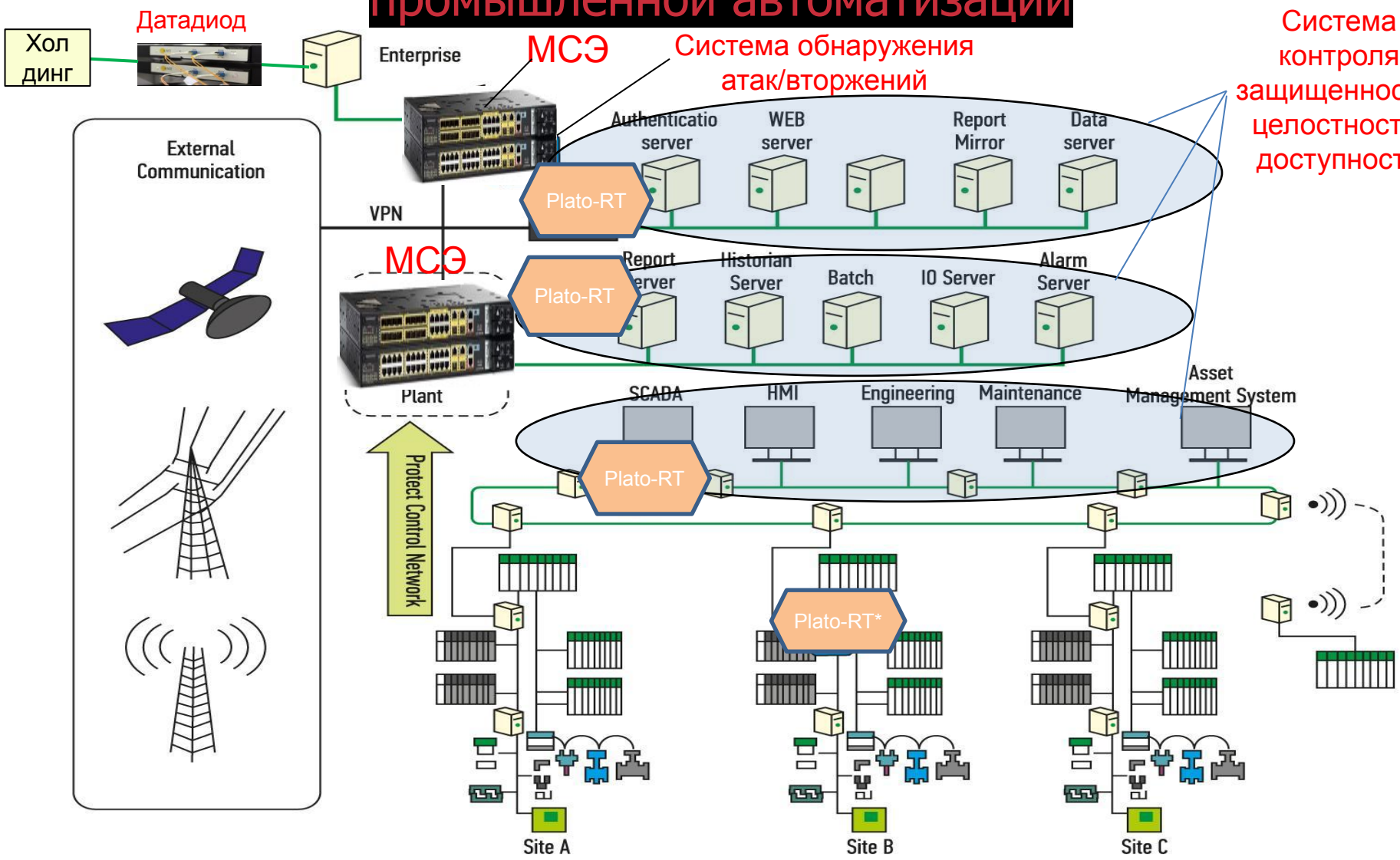
В целом, продукт применяется для построения высоконадежных, гарантированно защищенных сегментов критически важных систем в составе широкого класса систем: АСУ ТП, САЦ, ERP…

Особенности внедрения Плато-РТ

- Разумное применение аппаратных и программных средств: дооснащается уже существующая инфраструктура
- Комплексное решение задач безопасности, контроля и управления функционированием вычислительной инфраструктурой

- Отечественное, доверенное, защищенное программное обеспечение
- Сертификат ФСТЭК
- Основные системотехнические решения внедрены и подтвердили надежность в системе федерального масштаба

Позиционирование Плато-РТ в ландшафте защиты систем промышленной автоматизации

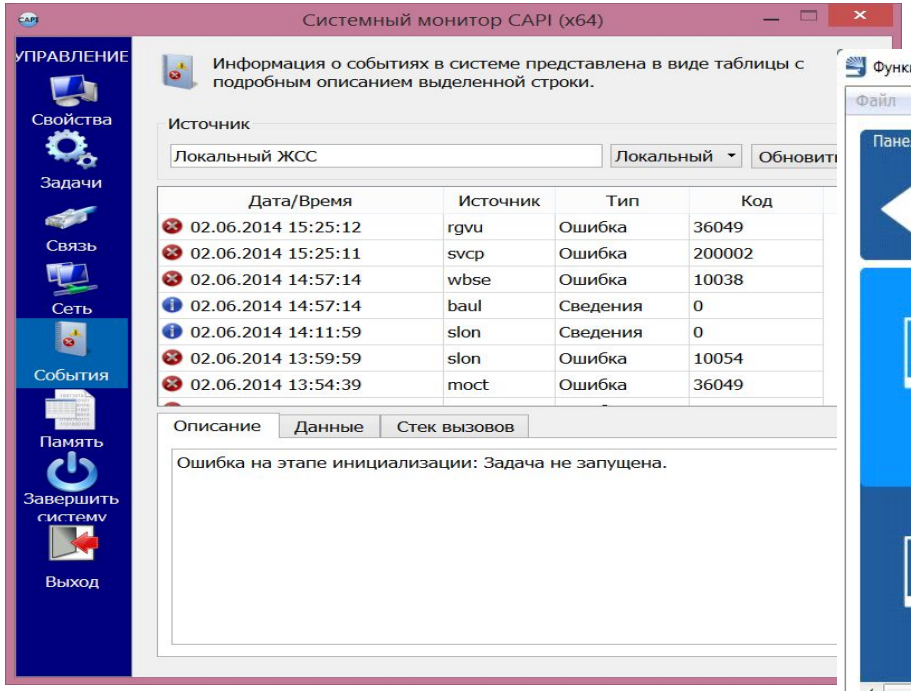


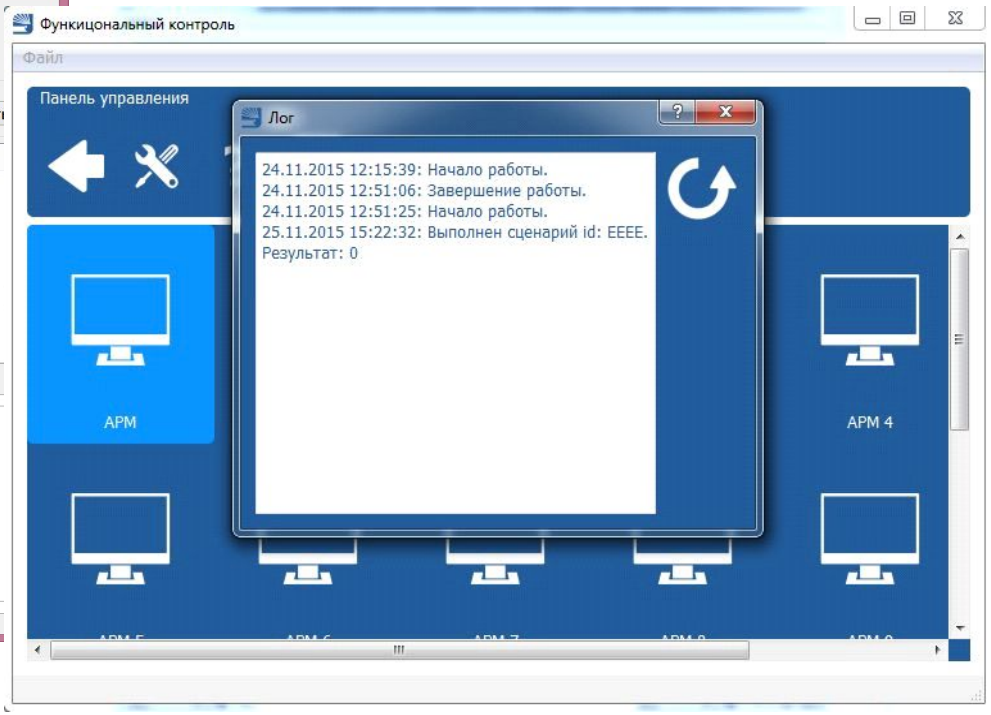
Примечание: Plato-RT* - требуется разработка

Варианты компонентов защиты

Компонент защиты	Вариант
Межсетевой экран (МСЭ)	Cisco CGR 2000 Cisco CGS 2500 Cisco ASA 5506H-X Cisco IE-3000-8TC 
	Symanitron SEWM-DF-S300, DF-S200, SEWM-DF-S500, ViPNet 100 
Система обнаружения атак/вторжений	Check Point UTM-1 Edge N Industrial Appliance Check Point 1200R, 
	FortiGate Rugged-100C, Rugged-60D, Rugged-90D 
	АПК «ЩИТ» SECURE OUTLINE 
Однонаправленные шлюзы	Fox DataDiode InfoDiode SECURE DIODE Waterfall Security Solutions 
Система контроля защищенности, целостности, доступности	**ПЛАТО-РТ** Honeywell Industrial Cyber Security Risk Manager Kaspersky Industrial CyberSecurity   InfoWatch Automated System Advanced Protector (InfoWatch ASAP)  MaxPatrol SCADA-аудитор  

Контроль целостности вычислительной инфраструктуры в ЗКП «Plato RT» вер.1.1

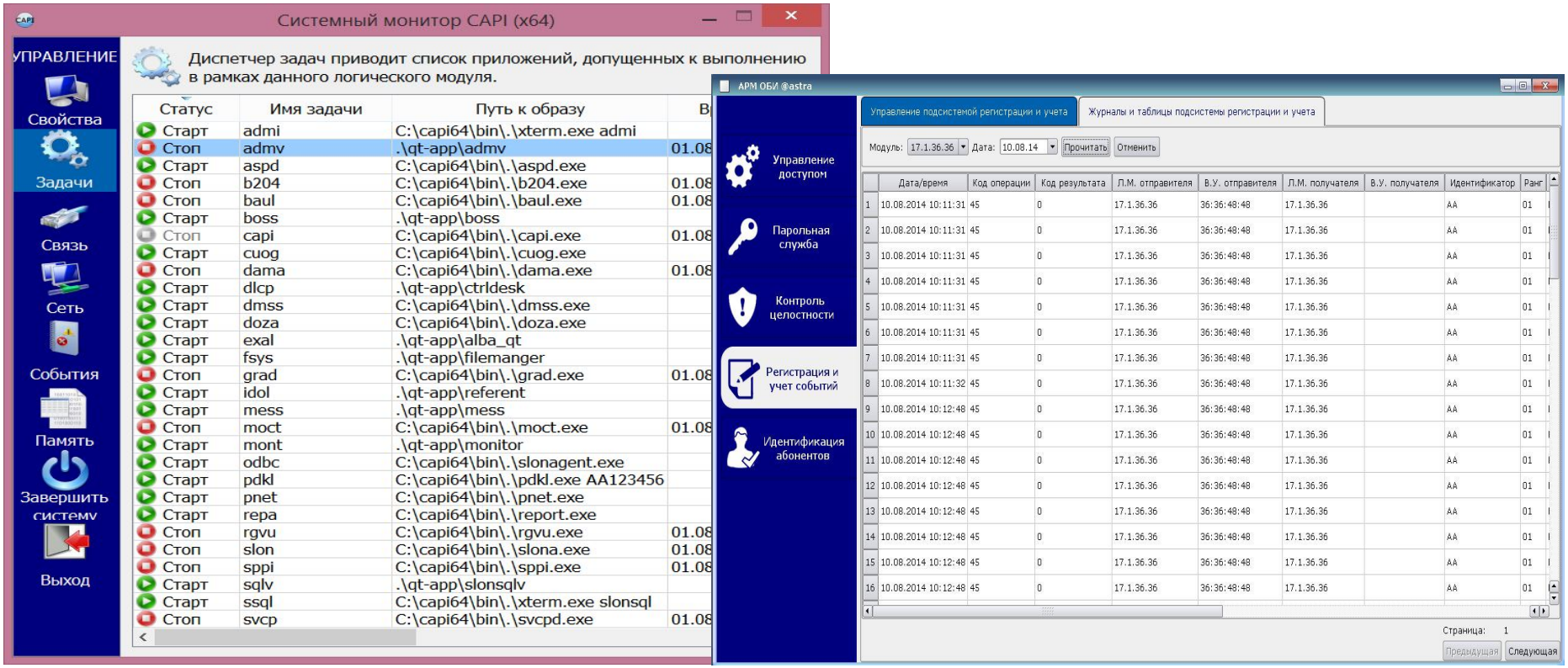




Особенности реализации:

1) Контроль производится на каждом узле средствами ЗКП «Plato RT» с хранением результатов (инцидентов) в независимой области под управлением гипервизора безопасности и представлением данных на АРМ функционального контроля (ФК) по технологическому тракту.
2) Управление функционированием производится с АРМ ФК в автоматическом (посредством сценариев) и/или автоматизированном режиме

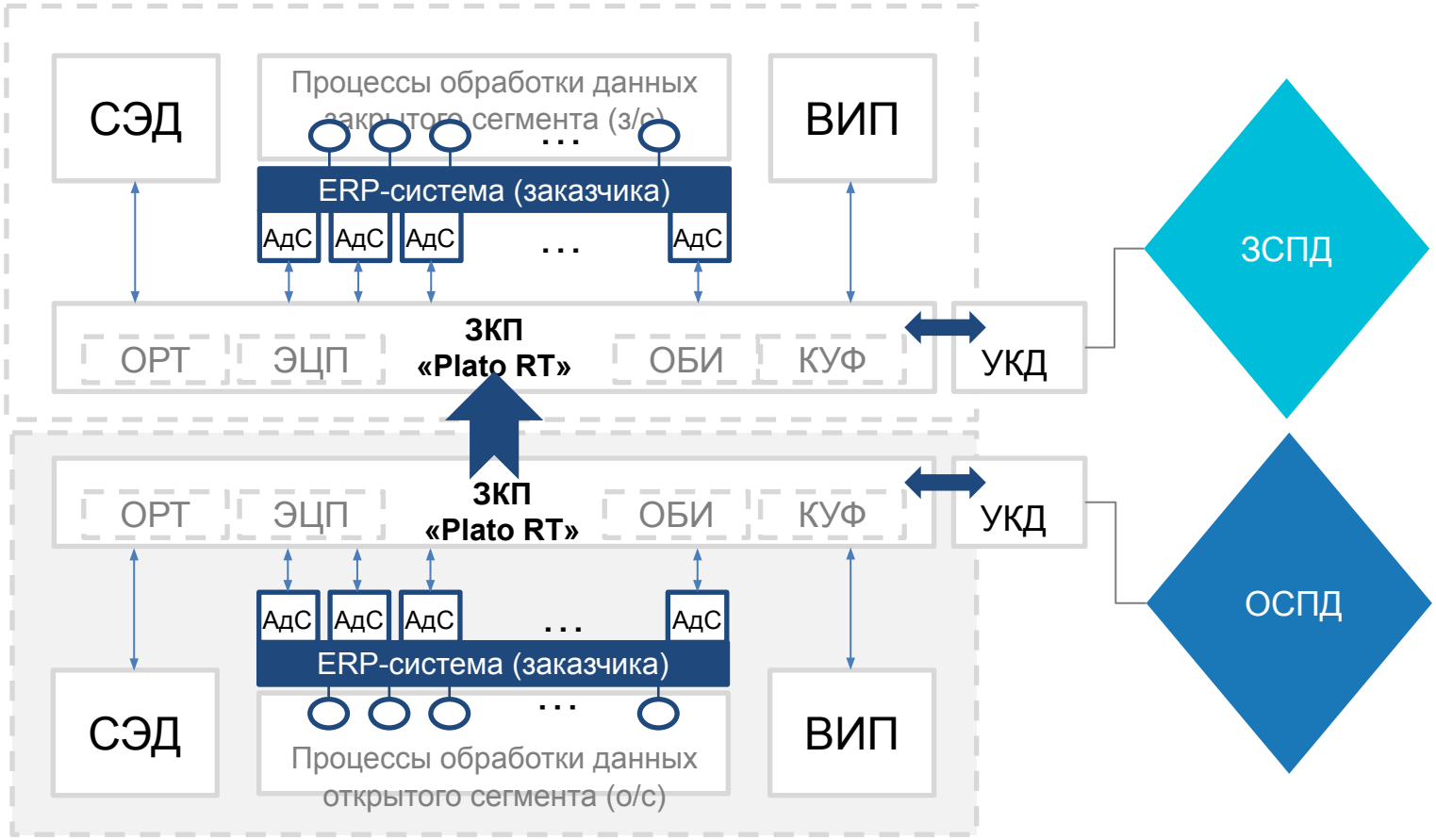
Контроль и управление средствами защиты ЗКП «Plato RT» вер.1.1



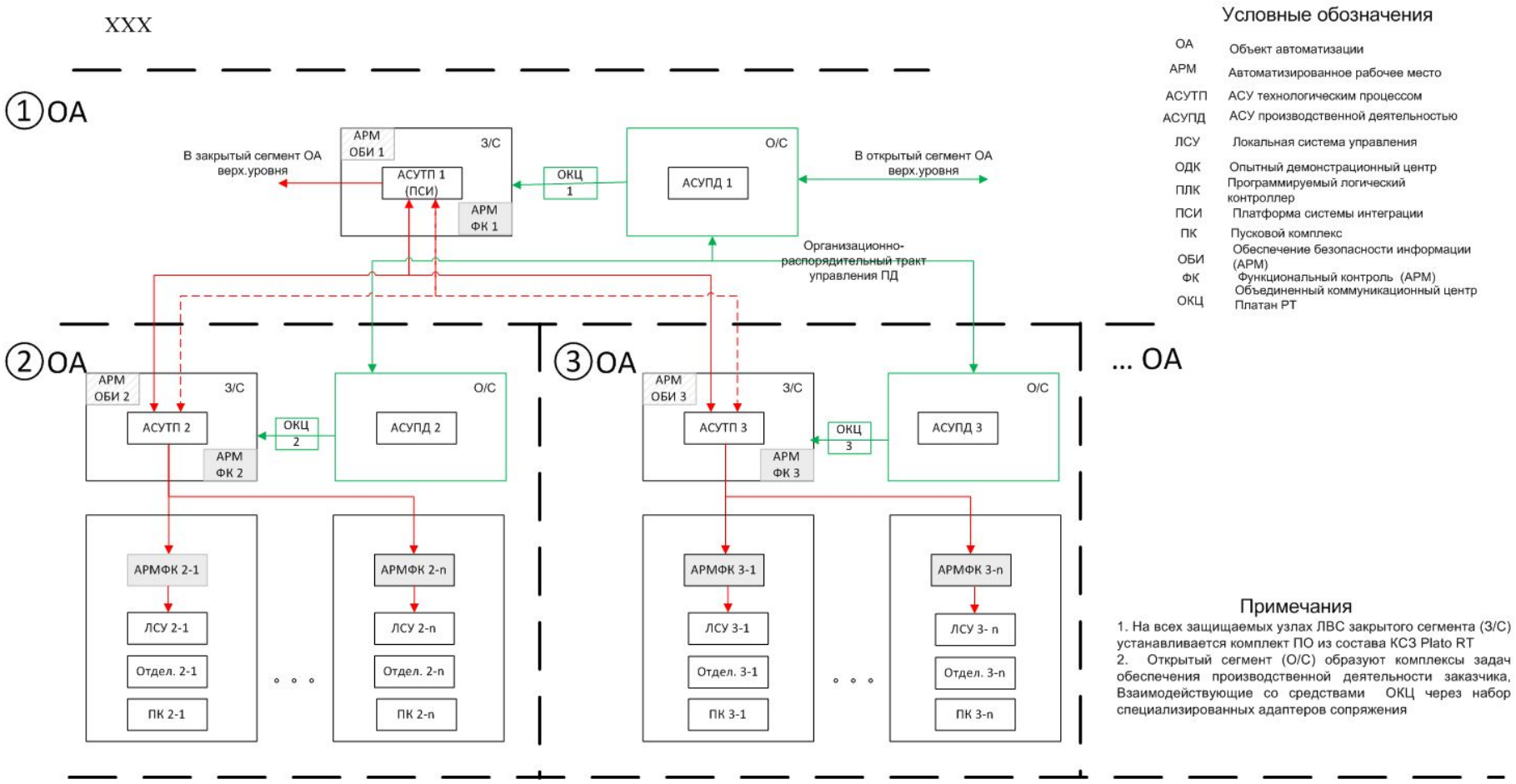
Особенности реализации:

1) Контроль ограничений конфиденциальности, заданных настройками политики безопасности производится на каждом узле с хранением результатов (инцидентов) в независимой области.
2) Управление безопасностью в рамках объекта (включая АРМ ФК) производится с АРМ ОБИ по отдельному (выделенному) каналу.

Взаимодействие сегментов ЗКП «Plato RT», обрабатывающих информацию различных уровней конфиденциальности, (в составе изделия ОКЦ «Platan RT»)



Структура Системы Защиты Информации на объекте Заказчика



Условные обозначения

ОА	Объект автоматизации
АРМ	Автоматизированное рабочее место
АСУТП	АСУ технологическим процессом
АСУПД	АСУ производственной деятельностью
ЛСУ	Локальная система управления
ОДК	Опытный демонстрационный центр
ПЛК	Программируемый логический контроллер
ПСИ	Платформа системы интеграции
ПК	Пусковой комплекс
ОБИ	Обеспечение безопасности информации (АРМ)
ФК	Функциональный контроль (АРМ)
ОКЦ	Объединенный коммуникационный центр Платан РТ

Примечания

1. На всех защищаемых узлах ЛВС закрытого сегмента (З/С) устанавливается комплект ПО из состава КСЗ Plato RT
2. Открытый сегмент (О/С) образуют комплексы задач обеспечения производственной деятельности заказчика, Взаимодействующие со средствами ОКЦ через набор специализированных адаптеров сопряжения

RTSoft

Замысел построения Системы Защиты Информации на объекте Заказчика

Основные архитектурные решения построения системы защиты информации (СЗИ):

- 1. Каждая ЛСУ представляет собой отдельный закрытый сегмент (З/С) в составе объекта автоматизации (ОА), на всех защищаемых узлах ЛСУ устанавливается клиентский комплект ПО из состава ЗКП «Плато РТ». Локальный контроль и управление функционированием системы защиты каждой ЛСУ обеспечивается соответствующим АРМ ФК из состава ЗКП «Плато РТ».
- 2. Каждый ОА состоит из закрытого сегмента, включающего одну и более защищенную ЛСУ (см. п.1), и условно-открытого сегмента (О/С), содержащего АРМ из состава АСУ предприятия, реализующей организационно-распорядительные функции. Однонаправленное информационное взаимодействие сегментов (от канального до прикладного уровней) реализуется средствами ОКЦ «Платан РТ», оснащенного комплектом ПО - Адаптеров сопряжения . На каждом ОА (в закрытом сегменте) организуется отдельный АРМ ОБИ.
- Масштабированию (по горизонтали) подлежат все ОА, построенные в соответствии с пп.1, 2. При этом, для контроля и управления состоянием всех ОА Заказчика, а также их взаимодействия (по вертикали) с внешними системами (общего или специального назначения) организуется отдельный ОА, включающий закрытый и открытый сегменты и оснащенный ПО платформы системной интеграции (ПСИ).
- Взаимодействие между узлами закрытого(ых) сегмента(ов) реализуется 2-мя независимыми физическими трактами : *информационно-технологическим* (для выполнения технологических процессов) и *специальным* (для объективного контроля состояния ИБ и управления СЗИ).

RTSoft

Перечень работ по созданию Системы Защиты Информации на объекте Заказчика

1	**Техническое задание (отдельный документ)**
1.1	Разработка и согласование Частного технического задания на систему защиты информации - СЗИ (90)
2	**Инженерное обследование и разработка Пояснительной записки Технического проекта (отдельные книги)**
2.1	Модель угроз и модель нарушителя
2.2	Обоснование и выбор модели защиты
2.3	Основные технические решения по созданию СЗИ
3	**Рабочее проектирование (эт. 1 -Разработка Программной Документации)**
3.1	Разработка интерфейсов АРМ ДЛ
3.2	Доработка интерфейсов АРМ ФК (по согласованию с Заказчиком)
3.3	Разработка адаптеров сопряжения и комплекта сценариев событий ИБ для АРМ ОБИ
4	**Рабочее проектирование (эт. 2 -Разработка Эксплуатационной Документации)**
4.1	Спецификация (20)
4.2	Описание программы (13)
4.3	Руководство оператора (34)
4.4	Руководство системного программиста (32)
4.5	Программа и методика испытаний (91)
5	**Рабочее проектирование (эт. 3 – объектовые Испытания СЗИ)**
5.1	Подготовка и проведение объектовых испытаний СЗИ
5.2	Доработка СЗИ по результатам объектовых испытаний
6	**Передача в опытную эксплуатацию (ОЭ)**
6.1	Комплексные проверки функционирования СЗИ на объекте заказчика
6.2	Корректировка ЭД по результатам комплексных проверок и передача изделия заказчику в ОЭ
6.3	Сопровождение опытной эксплуатации
7	**Аттестование объекта и обучение персонала**
7.1	Подготовка к аттестованию объекта, обучение персонала, разработка и выпуск комплекта инструкций по эксплуатации СЗИ на объекте Заказчика

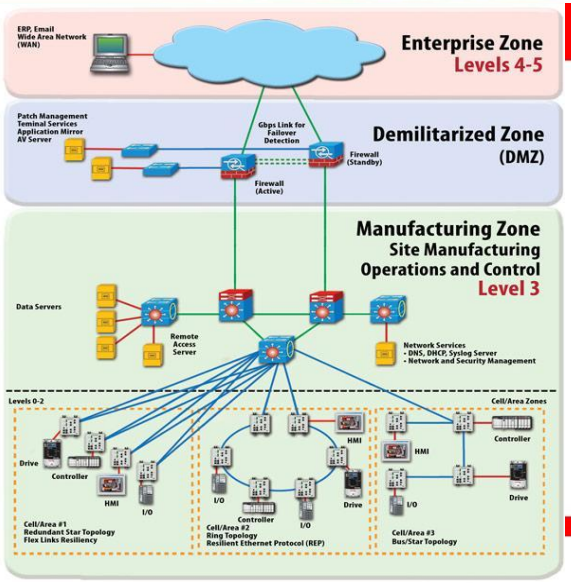
СООТВЕТСТВИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ “PLATO RT” (АО «РТСОФТ») БАЗОВЫМ НАБОРАМ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ АСУ ТП КВО (ПРИКАЗ №31 2014Г. ФСТЭК РФ)

НАИМЕНОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ	“PLATO RT” (компоненты)
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
III. Ограничение программной среды (ОПС)	
IV. Защита машинных носителей информации (ЗНИ)	
V. Регистрация событий безопасности (РСБ)	
VI. Антивирусная защита (АВЗ)	
VII. Обнаружение вторжений (СОВ)	
VIII. Контроль (анализ) защищенности информации (АНЗ)	
IX. Обеспечение целостности (ОЦЛ)	
X. Обеспечение доступности (ОДТ)	
XI. Защита среды виртуализации (ЗСВ)	
XII. Контроль целостности виртуальной инфраструктуры и ее конфигураций	
XII. Защита технических средств (ЗТС)	
XIII. Защита автоматизированной системы и ее компонентов (ЗИС)	
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)	
XV. Управление обновлениями программного обеспечения (ОПО)	
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)	
XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	
XVIII. Информирование и обучение персонала (ИПО)	
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)	
XX. Выявление инцидентов и реагирование на них (ИНЦ)	
XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	
ВСЕГО требований (мероприятий) : 167 PLATO_RT_СООТВЕТСТВИЕ ПРИКАЗУ_31_ФСТЭК_3.docx	Реализовано в “PLATO RT”– 106 (63%)

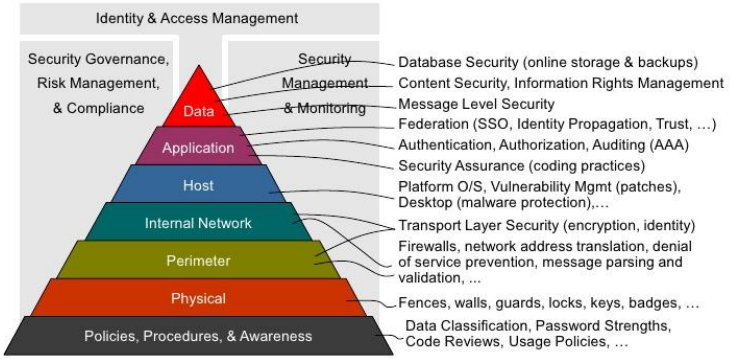
RTSoft
средства и системы автоматизации

Спасибо за внимание!

105037, Москва, ул. В. Первомайская, д. 51
Тел.: +7 (495) 967-15-05
E-mail: rtsoft@rtsoft.ru
www.rtsoft.ru



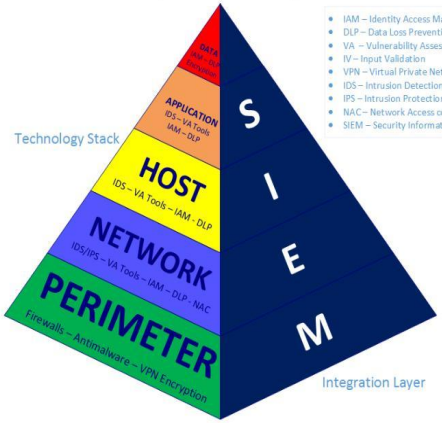
Defense in Depth: Layers



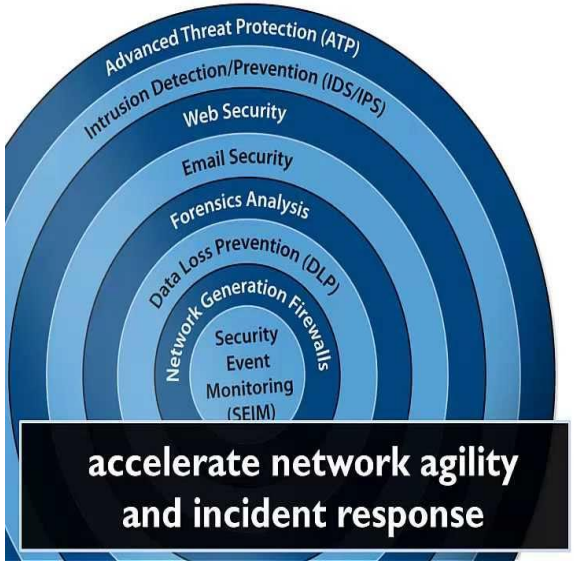
ORACLE George Moraetes, CCISO, CISM, CGEIT

OTN Architect Day 2011

The Layered Security Model



Network Defense-in-Depth



Network Security in Layers

1. **Advanced Threat Protection (ATP)**
   e.g. FireEye, Cisco/Ironport
2. **Intrusion Detection/Prevention (IDS/IPS)**
   e.g. Sourcefire, McAfee
3. **Web Security**
   e.g. Imperva, Fortinet,
4. **Email Security**
   e.g. Bluecoat, Trustwave
5. **Forensics Analysis**
   e.g. RSA/NetWitness, Solera
6. **Data Loss Prevention (DLP)**
   e.g. Websense, TrendMicro
7. **Network Generation Firewalls**
   e.g. Palo Alto Networks, Checkpoint
8. **Security Event Monitoring (SEIM)**
   e.g. HP/Arcsight, IBM/Q1Labs