ПЕРСПЕКТИВЫ ПОСТРОЕНИЯ ВЕДОМСТВЕННОГО ЦЕНТРА КОМПЛЕКСНОГО ПРОТИВОДЕЙСТВИЯ АТАКАМ НА КОМПЬЮТЕРНЫЕ СЕТИ В ОАО «АГАТ-СИСТЕМЫ УПРАВЛЕНИЯ»

Автор доклада
Спесивцев В.В.
ОАО «АГАТ-системы управления», г. Минск

Статистика киберпреступности

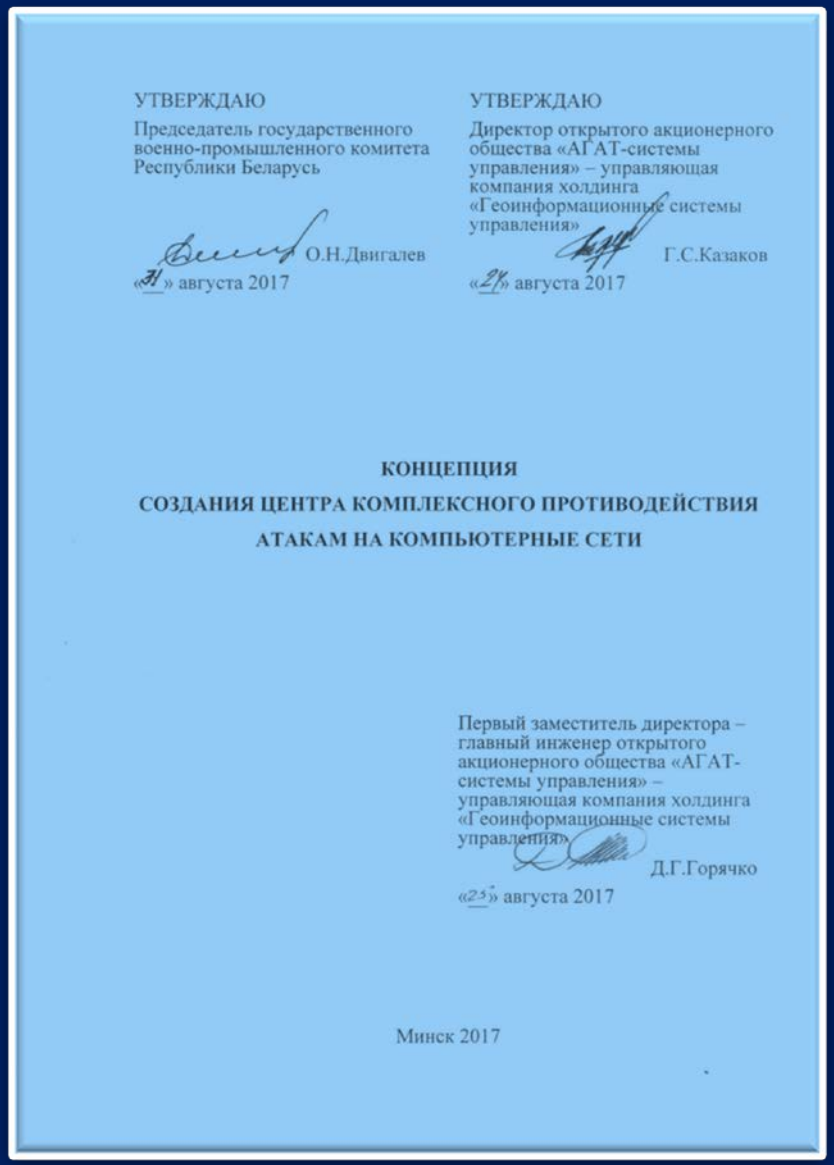
АГАТ
СИСТЕМЫ УПРАВЛЕНИЯ

Основные угрозы информационной безопасности

АГАТ
СИСТЕМЫ УПРАВЛЕНИЯ

1. Утечка конфиденциальной информации.
2. Потеря или недоступность информации.
3. Использование неполной или искаженной информации.
4. Несанкционированная скрытая эксплуатация информационно-вычислительных ресурсов.
5. Распространение во внешней среде информации, угрожающей репутации организации или предприятия.

Концепция создания Центра



УТВЕРЖДАЮ
Председатель государственного военно-промышленного комитета Республики Беларусь
О.Н.Двигалев
«31» августа 2017

УТВЕРЖДАЮ
Директор открытого акционерного общества «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»
Г.С.Казаков
«24» августа 2017

КОНЦЕПЦИЯ
СОЗДАНИЯ ЦЕНТРА КОМПЛЕКСНОГО ПРОТИВОДЕЙСТВИЯ АТАКАМ НА КОМПЬЮТЕРНЫЕ СЕТИ

Первый заместитель директора – главный инженер открытого акционерного общества «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»
Д.Г.Горячко
«25» августа 2017

Минск 2017

Центр – что это?

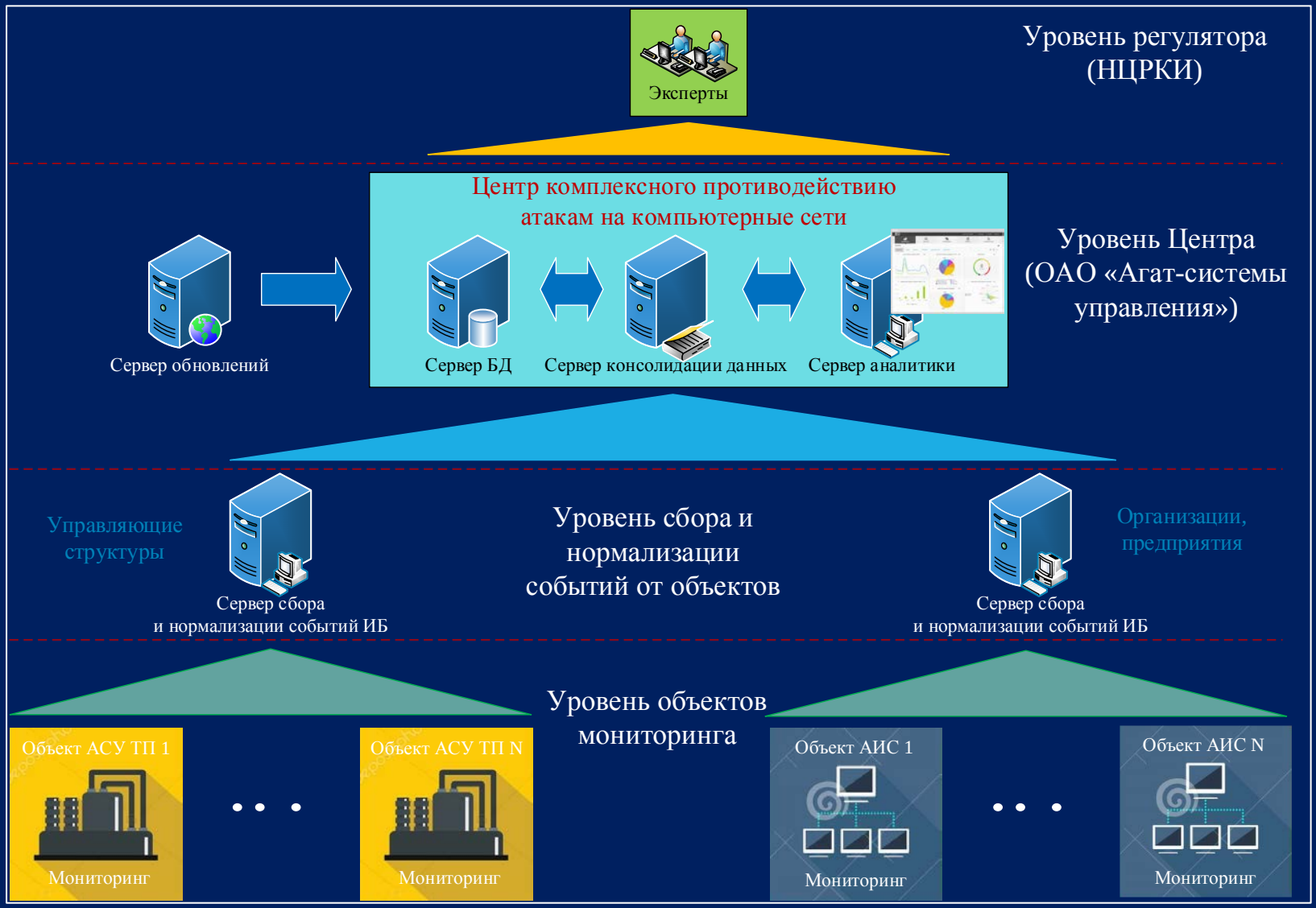
АГАТ СИСТЕМЫ УПРАВЛЕНИЯ

Совокупность технологий, процессов и человеческих ресурсов, направленных на предупреждение, своевременное выявление, реагирование и минимизацию последствий компьютерных атак на критичные информационные ресурсы.

Основные функции:

- **предупреждение компьютерных атак;**
- **обнаружение компьютерных атак;**
- **реагирование на компьютерные атаки;**
- **ликвидация последствий компьютерных атак;**
- **оценка эффективности принимаемых мер.**

Уровни сбора и обработки событий ИБ

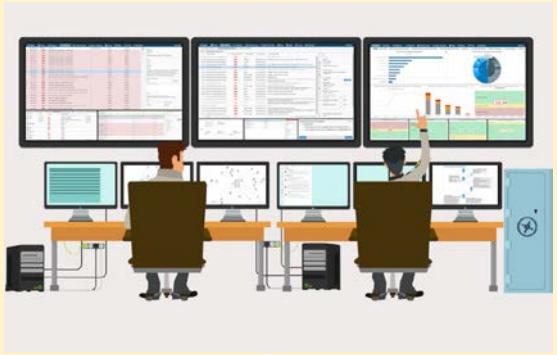


1 Этап формирования Центра

АГАТ СИСТЕМЫ УПРАВЛЕНИЯ

Локальная информационная система ОАО «АГАТ-системы управления»

Аналитики дежурной смены



НЦРКИ

Инциденты

SIEM-система

Сервер обновлений

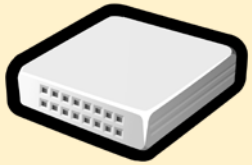
События ИБ

Межсетевые экраны

Антивирусные системы

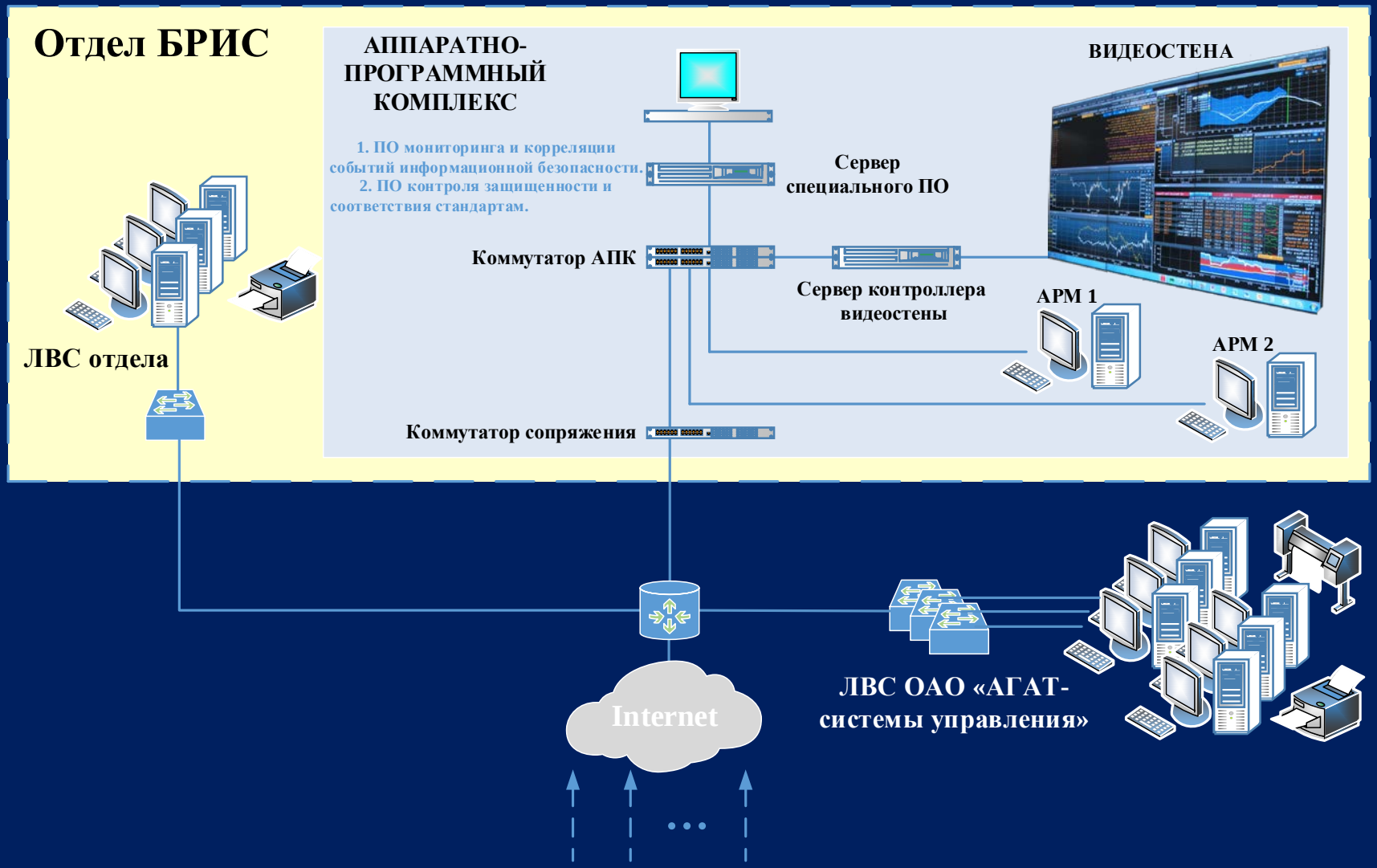
Системы предупреждения вторжений

Базы данных



Коммутаторы

Первичная структура аппаратно-программного ядра Центра



2 Этап формирования Центра

АГАТ-системы управления

Центр комплексного противодействия атакам на компьютерные сети

НЦРКИ

Сервер обновлений

VPN

INTERNET

VPN

VPN

VPN

VPN

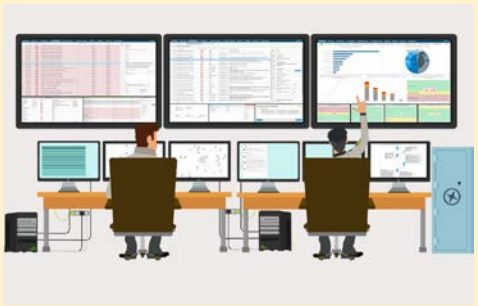
ОАО «Научно-исследовательский институт электронных вычислительных машин»

ОАО «АГАТ-СИСТЕМ»

ОАО «Агат – электромеханический завод»

ОАО «Техника связи»

3 Этап формирования Центра



АГАТ-системы управления

Центр комплексного противодействия атакам на компьютерные сети

НЦРКИ

Сервер обновлений

VPN

INTERNET

VPN

VPN

VPN

Предприятия холдинга

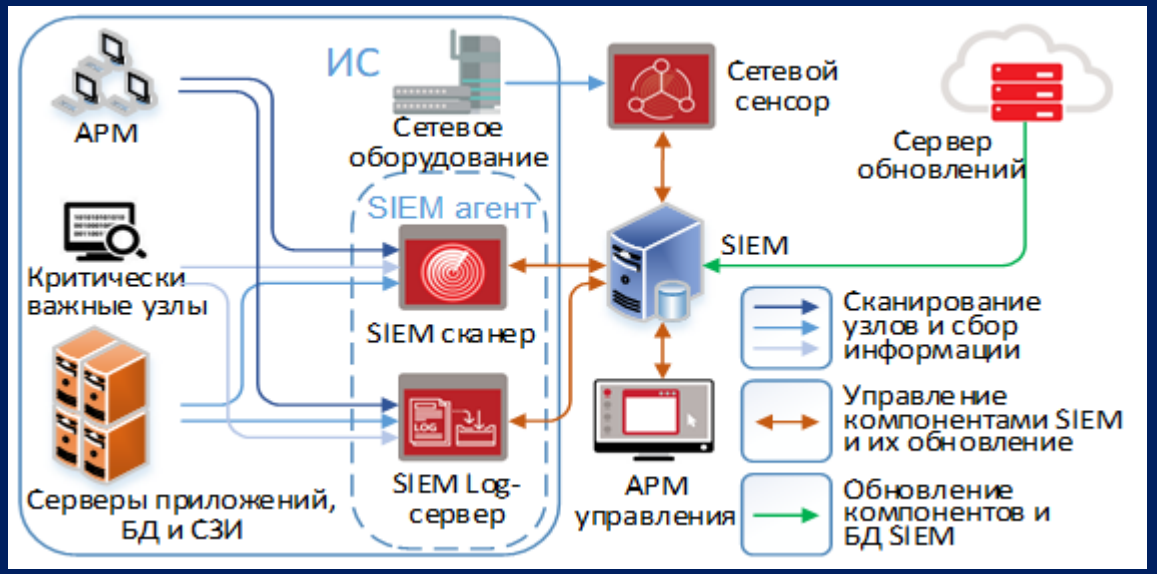
Предприятия ГВПК

Иные заинтересованные предприятия и ведомства

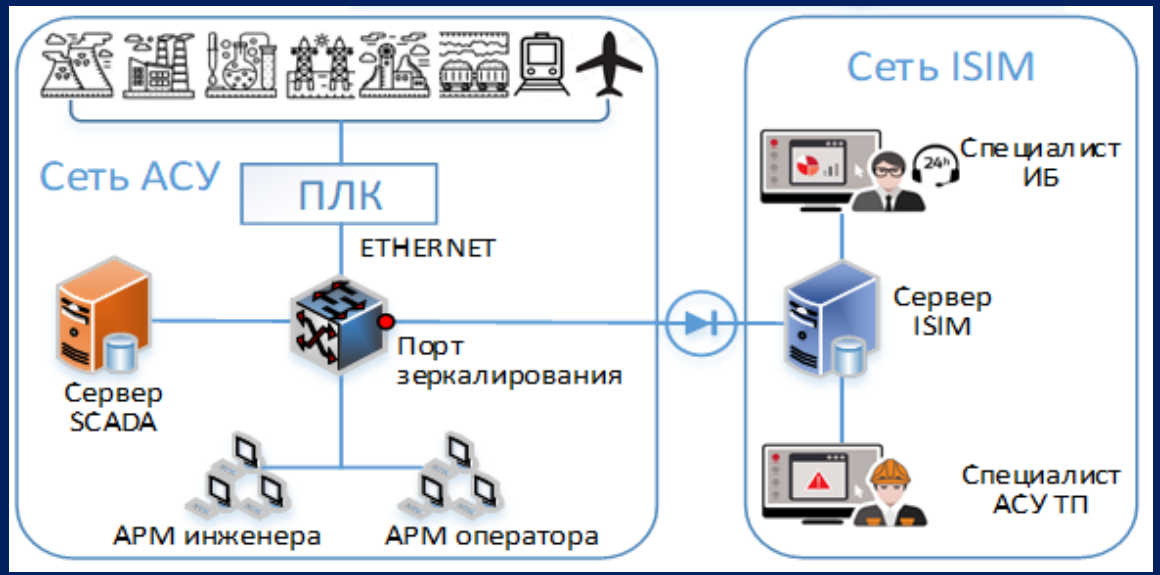
Потенциальные заказчики услуг Центра

АГАТ СИСТЕМЫ УПРАВЛЕНИЯ

1. Государственные автоматизированные информационные системы, отнесенные к КВОИ (АИС предприятий холдинга, ГВПК…)



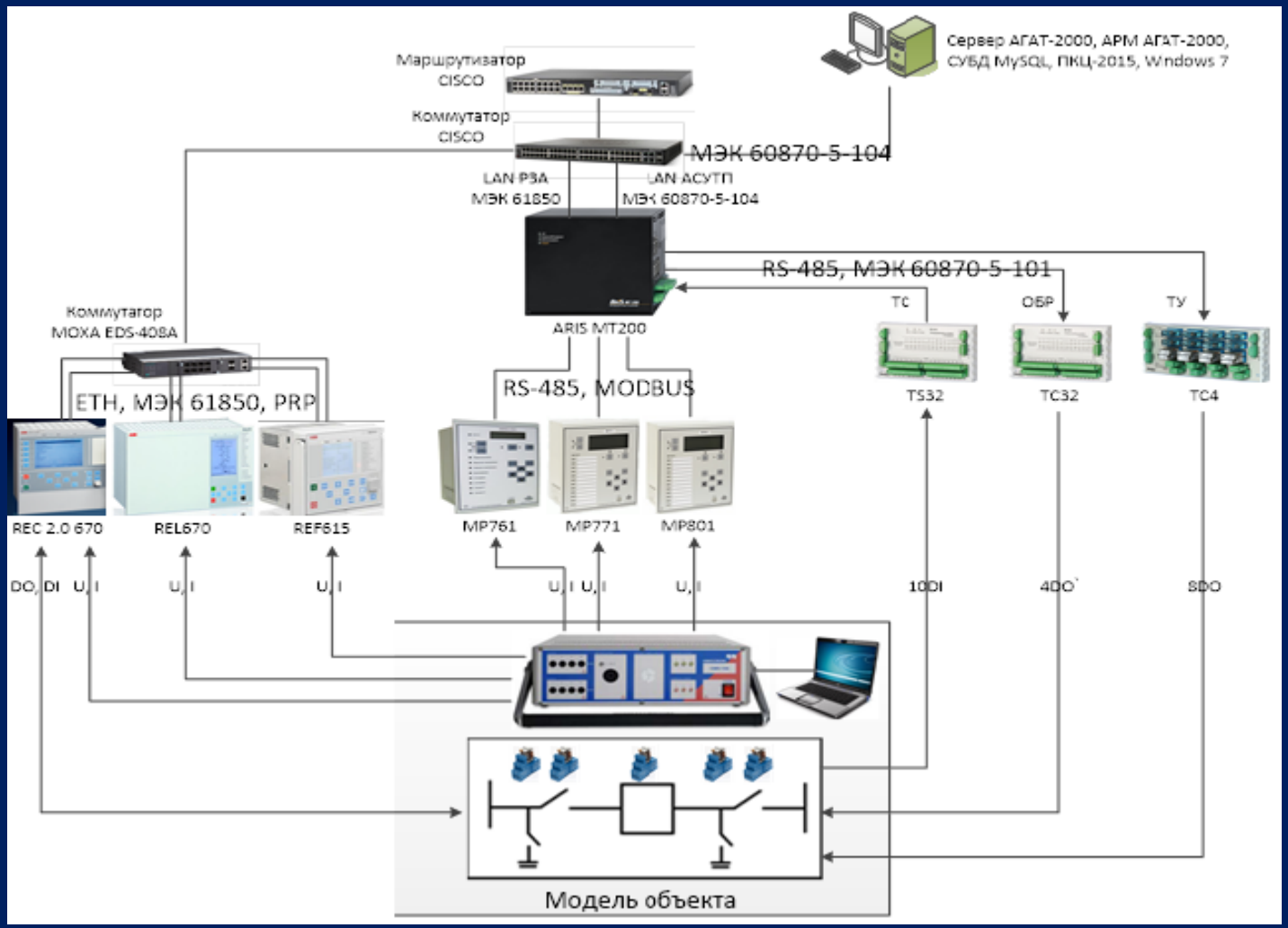
2. Государственные информационные системы в АСУ ТП, отнесенные к КВОИ (сети АСУ ТП Минэнерго, Минтранса…)



Анализ защищенности элементов КВОИ на базе стенда АСУ ТП

АГАТ СИСТЕМЫ УПРАВЛЕНИЯ

Структурная схема стенда для проведения анализа в области ИБ

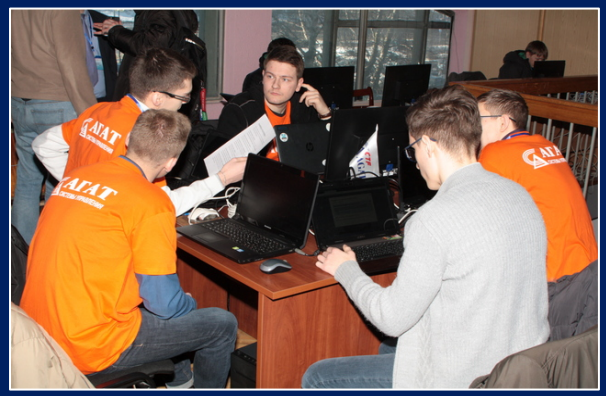


Штатная структура Центра на начальных этапах его формирования

Кадровый источник Центра

АГАТ
СИСТЕМЫ УПРАВЛЕНИЯ

Agat CTF - 2018



АГАТ
СИСТЕМЫ УПРАВЛЕНИЯ

Спасибо за внимание!