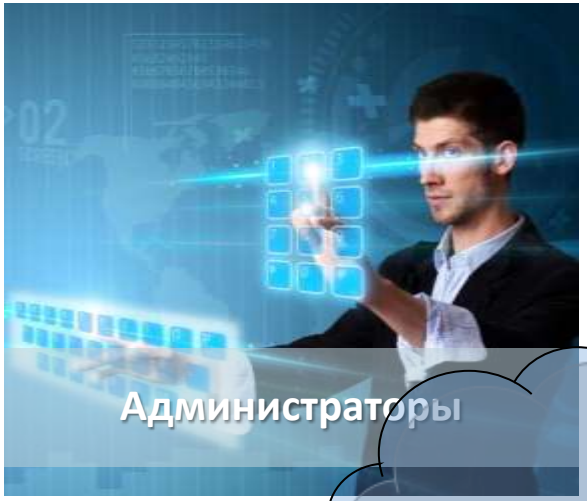
НАЦИОНАЛЬНЫЙ ИННОВАЦИОННЫЙ ЦЕНТР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

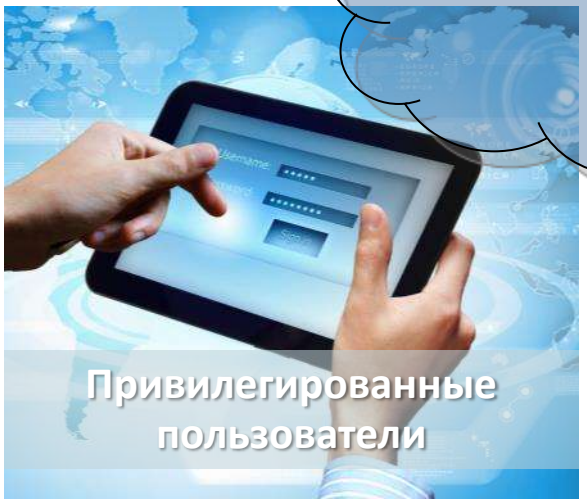
БЕЗОПАСНОЕ УПРАВЛЕНИЕ ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ НА БАЗЕ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА «ПТК-SR»

Суть проблемы

- Распространены случаи, когда сотрудники эксплуатируют ТКО, используя «обезличенные» учетные записи
- Сотрудники, имеющие права администраторов, имеют возможность скрыть следы своих действий
- Особенности эксплуатации ТКО затрудняют хранение в секрете паролей к ТКО (проблема enable для Cisco)
- Требуется допускать к ТКО представителей вендора или службы техподдержки для решения сложных проблем на оборудовании
- Уровень лояльности администраторов, как правило, никак не контролируется
- Проблемы доверия производителю ТКО

Чьи действия необходимо контролировать





Решение проблемы (Организационные меры)

Контроль и ограничение доступа субъектов к защищаемым ресурсам в соответствии с определенной моделью доступа

Регламент получения и изменения уровня привилегий для внутренних сотрудников

Регламент получения и изменения уровня привилегий для партнеров, сотрудников с удаленным доступом

Решение проблемы (Технические меры)

Внедрение надежной и эффективной автоматизированной системы контроля действий администраторов

Подсистема записи действий привилегированных учетных записей

Подсистема контроля выдачи прав

Подсистема блокировки команд и восстановления конфигурации

Основные функции ПАК «SafeRoute»

- Защита от несанкционированного подключения к локальным портам управления, включая консольные порты ТКО
- Обеспечение доверенной загрузки ТКО, контроль целостности образов операционной системы и конфигурационных файлов
- Реализация механизма внешней аутентификации администраторов ТКО (включая двухфакторную)
- Контроль действий администраторов ТКО (протоколирование всех команд в локальный файл, передача во внешний syslog-сервер)
- Возможность интеграции с внешними системами (продукты типа SIEM, внешней аутентификации, контроля конфигураций, системы управления)

Защита от несанкционированного подключения

Локальные порты управления, включая консольные порты ТКО

- Контроль доступности сетевого и консольного интерфейсов управления ТКО
- Мониторинг состояния сетевого и консольного кабелей (кабель подключен/отключен)
- Сигнализация об изменении состояния интерфейсов управления

Обеспечение доверенной загрузки ТКО

Контроль целостности образов операционной системы и конфигурационных файлов

- Доставка образа ОС и конфигурационного файла по контролируемому каналу (SR-ТКО)
- Подсчет контрольных сумм образов ОС и конфигурационного файла при помощи сертифицированного СЗИ, перед загрузкой и по расписанию
- Интеграция с ПК ЭФРОС в интересах контроля изменения конфигурационного файла

Контроль действий администраторов ТКО

Регистрация активности

- Перехват и тотальный контроль консоли администратора ТКО
- Протоколирование всех вводимых команд в локальный файл
- Контроль командных файлов включая их сохранение в архиве
- Передача всех команд во внешний syslog-сервер
- Черные и белые списки команд
- Анализ активности администратора

Черные/белые списки (пример магистрального ОС)

Команда	Всего команд за год	Команд в день
show	432 469	1 185
ping	26 397	72
terminal	18 058	49
exit	6 931	19
configure	5 778	16
interface	5 128	14
no	3 463	9
commit	2 952	8
write	2 877	8
switchport	1 600	4
description	1 201	3
delete	1 169	3
quit	1 136	3
traceroute	1 102	3
shutdown	1 027	3
ip	1 003	3
service-policy	818	2

Команда	Всего команд за год	Команд в день
default	695	2
edit	664	2
neighbor	428	1
router	423	1
encapsulation	400	1
xconnect	400	1
vrf	382	1
address-family	320	1
l2vpn	302	1

Всего не более 210 уникальных команд за год

Реализация механизма внешней аутентификации администраторов ТКО (включая двухфакторную)

Аутентификация

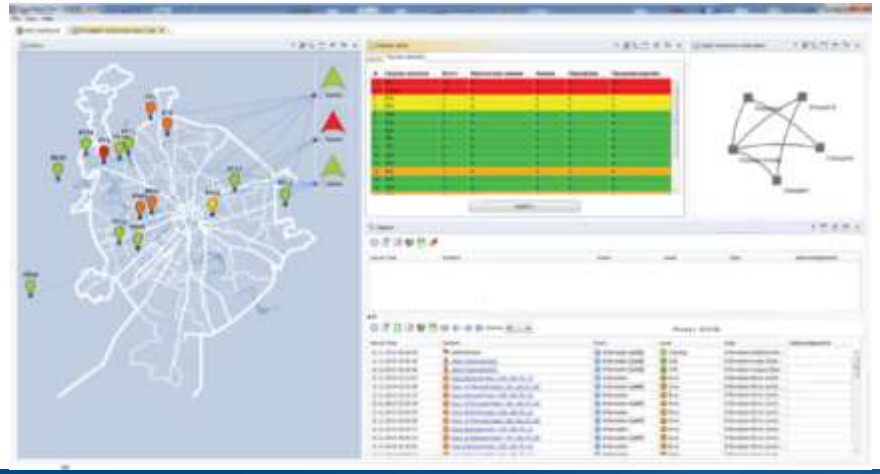
- Поддержка Radius-серверов как основного средства аутентификации (резервная локальная учетная запись)
- Поддержка SAS (сертифицированное решение двухфакторной аутентификации)
- Поддержка Open Source решений по двухфакторной аутентификации
- Настраиваемая ролевая модель доступа
- Сокрытие параметров доступа к ТКО

Возможность интеграции с внешними системами

Интеграция из коробки

- Используемые заказчиком клиенты таких протоколов удаленного доступа как Telnet, SSH
- Используемые заказчиком SIEM решения
- Используемые заказчиком Radius-сервера
- Используемый заказчиком программный комплекс ЭФРОС или другие системы контроля конфигураций
- Интеграция с зонтичными системами управления и мониторинга, например, платформа AggreGate от компании Tibbo.

Интеграция с внешними системами мониторинга

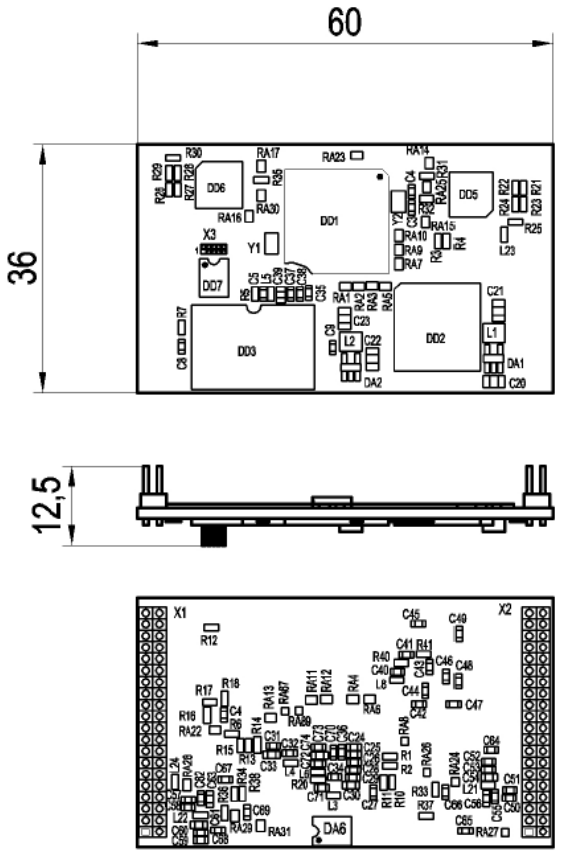


В рамках зонтичной системы управления и мониторинга имеется возможность обеспечить визуализацию процессов безопасного управления ТКО различных производителей, в которые установлены модули SR. (Географическое местоположение ТКО, состояние портов управления, кто и какие команды выполнял последний раз, откуда было управляющее воздействие).

Интеграция с зонтичными системами управления и мониторинга, например, платформа AggreGate от компании Tibbo.

Интеграция осуществляется на основании ТЗ согласованного с заказчиком и оплачивается отдельно от внедрения SR.

Программно-аппаратная платформа комплекса



Процессорный модуль

- Linux Debian\OpenVRT
- ATMEL ARM926 AT91SAM9x25
- 2x10/100BaseT
- 2xUSB 2.0, 1xUSB 1.1
- 3xRS 232

Варианты реализации ПАК SafeRoute с ТКО

Модульная реализация в слот WIC/HWIC

Модульная реализация в слот SPA

По запросу, реализация в виде модуля для любого ТКО (срок реализации 3 месяца)

Планы по развитию ПАК «SafeRoute»

Миграция на более производительную платформу.

2017 год

Сертификация ФСТЭК, ГАЗПРОМСЕРТ.

Конец 2016 года

Встраивание сертифицированного средства криптографической защиты канала управления.

По запросу

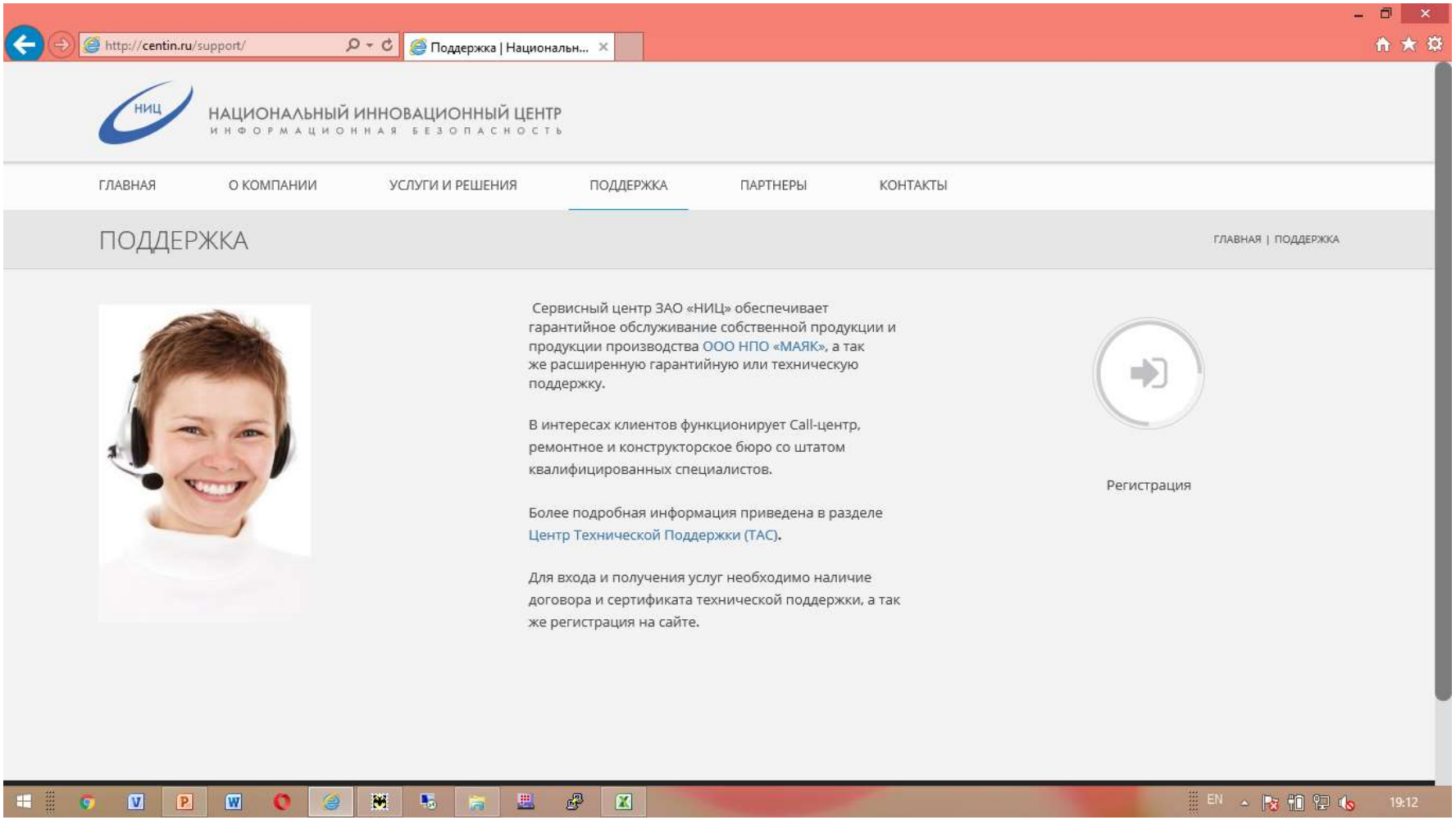
Обеспечение поддержки интерфейса Redfish для управления серверами.

конец 2017 года

Варианты применения

- Построение outbound системы управления с ее дальнейшей аттестацией
- Подготовка и проведение сертификации ТКО по требованиям безопасности
- Построение системы контроля действий администраторов в рамках оказания технической поддержки компаниями аутсорсерами и вендорами
- Разработка и внедрение механизмов контроля SLA в рамках оказания технической поддержки компаниями аутсорсерами и вендорами
- Повышение доверия к использованию ТКО иностранного производства
- Создание доверенных платформ для ТКО

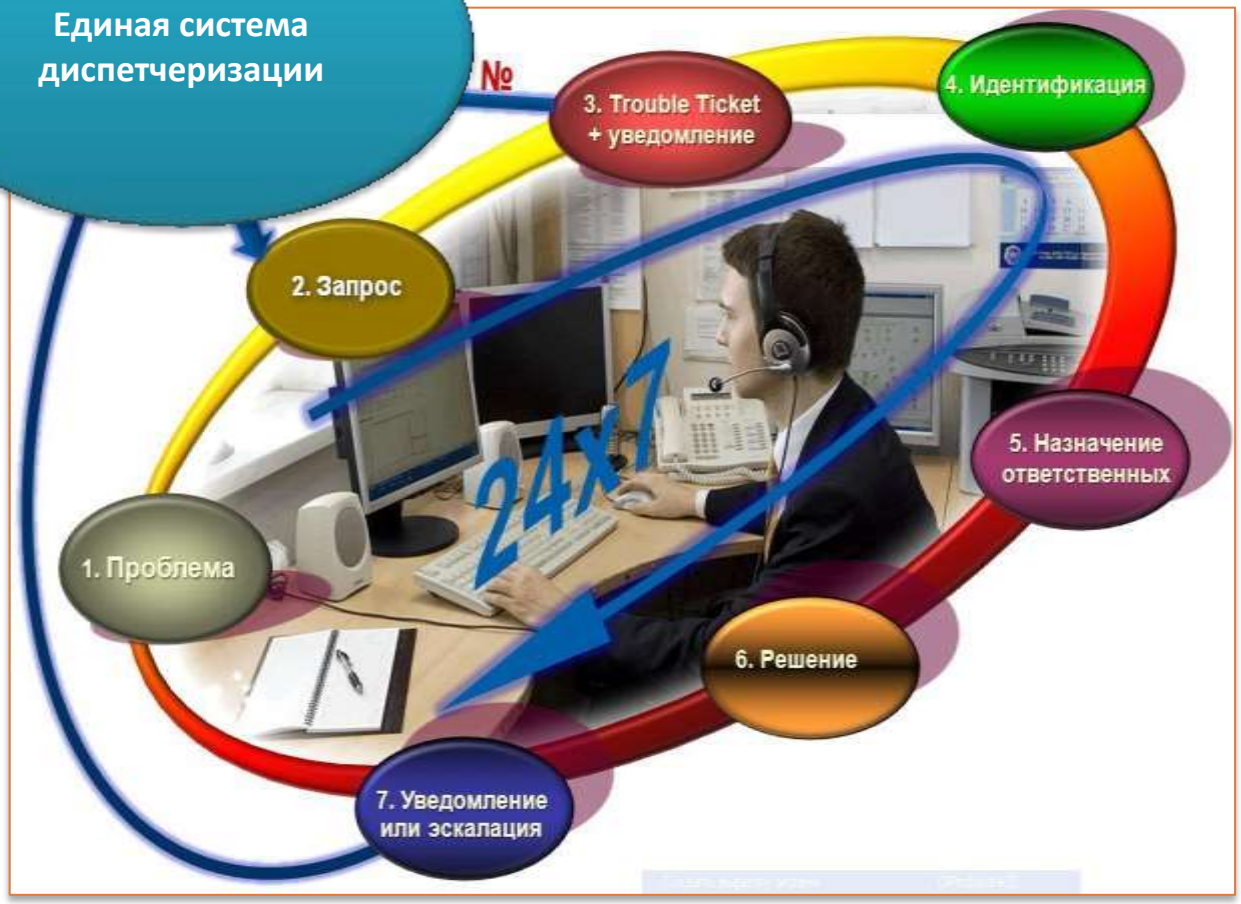
Центр технической поддержки



Базовые принципы обработки проблем и заявок

Заказчики

Единая система диспетчеризации



Функциональные единицы ЦТП

Первая линия поддержки (24x7)	Сменные инженеры (CCNA)	Прием заявок в работу, первичная обработка, решение простых вопросов, консультации
		Перевод заявок в обработку на вторую линию поддержки
Группа обеспечения деятельности (8x5)	Инженеры поддержки и администрирования инфраструктуры ЦТП	Системы: Call-центр, CRM, TTM, база знаний, система мониторинга
		LAN, WAN, АТС, рабочие места, пакет офисных программ
Координаторы (8x5)	Персонал сопровождения деятельности и поддержки договоров	Контроль качества обработки кейсов
		Контроль качества формирования базы знаний
		Контроль SLA и удовлетворенности клиентов
		Коммуникации с Заказчиками и партнерами
Вторая линия поддержки (8x5)	Инженеры узкой специализации (CCNP)	Инженеры по специализациям: телеком (IP MPLS), ВКС, UC, ИБ
	Региональные партнеры	Обеспечение регионального присутствия
		Монтажные и коммутационные работы в Заказчике
Третья линия поддержки	Вендорская техническая поддержка	

Функции Центра технической поддержки

- Прием и решение заявок заказчиков;
- Эскалация инцидентов производителям в формализованном (без привязки к объектам) виде в случае обнаружения ошибок функционирования ПО и оборудования;
- Организация и развитие экспертизы, с целью сокращения числа обращений к производителям ПО и оборудования;
- Формирование обширной отраслевой базы знаний по устранению проблем, решению инцидентов, ремонту оборудования на уровне типовых элементов замены по различным вендорам;

Функции Центра технической поддержки

- Накопление статистики работы оборудования и ПО на предприятиях отрасли с целью прогнозирования отказов по вероятностным характеристикам и принятия превентивных мер по замене конкретных моделей оборудования и ПО;

- Комплексное тестирование обновлений программного обеспечения, используемого на объектах информационно-телекоммуникационной инфраструктуры ОАО «Газпром», с целью определения корректности его функционирования после применения обновлений;

- Выработка рекомендаций на основании накопленных знаний и статистики по выбору наиболее надежных и приемлемых технических решений для автоматизации различного рода типовых задач;

- Выработка рекомендаций по формированию и планированию ЗИП в обслуживаемых сервисным центром организациях;

Спасибо за внимание!