



АПКШ «Континент»: Обеспечение безопасного сетевого взаимодействия и удаленного доступа при использовании сетей общего доступа

Группа компаний Информзащита

Александр Немошкалов
менеджер по продуктам



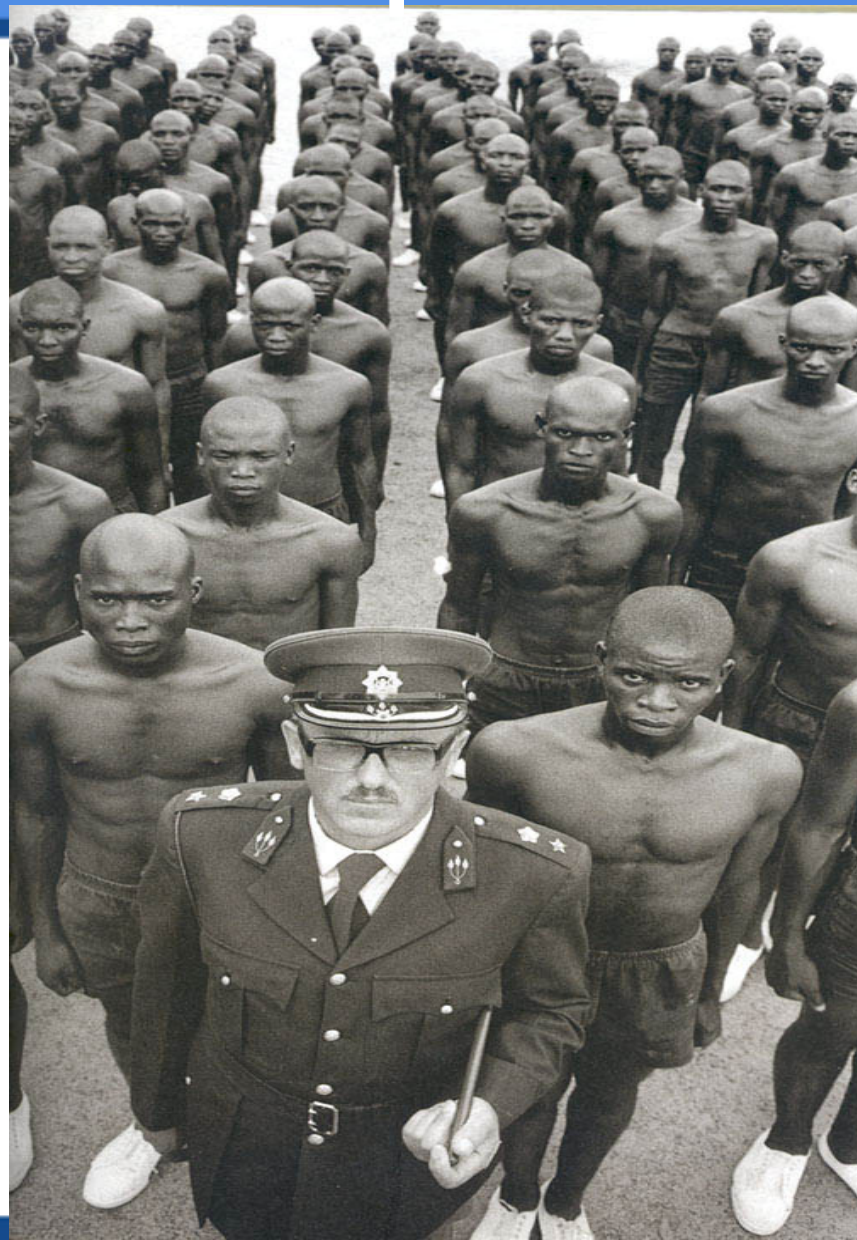
Требования к средствам VPN

Территориальная распределенность

<http://go.to/funpic>



Отсутствие квалифицированного персонала на местах



Отсутствие квалифицированного персонала на местах



Требования к VPN-решениям

- ✓ Простота внедрения
- ✓ Надежность
- ✓ Прозрачность
- ✓ Возможность организации различных схем связи
- ✓ Интеграция с PKI
- ✓ Сертификация (ФСБ, Гостехкомиссия)



Решение компании «Информзащита» - АПКШ «Континент»

Модельный ряд «Континент»



«Континент-mini»
для малых офисов



«Континент-Standard»

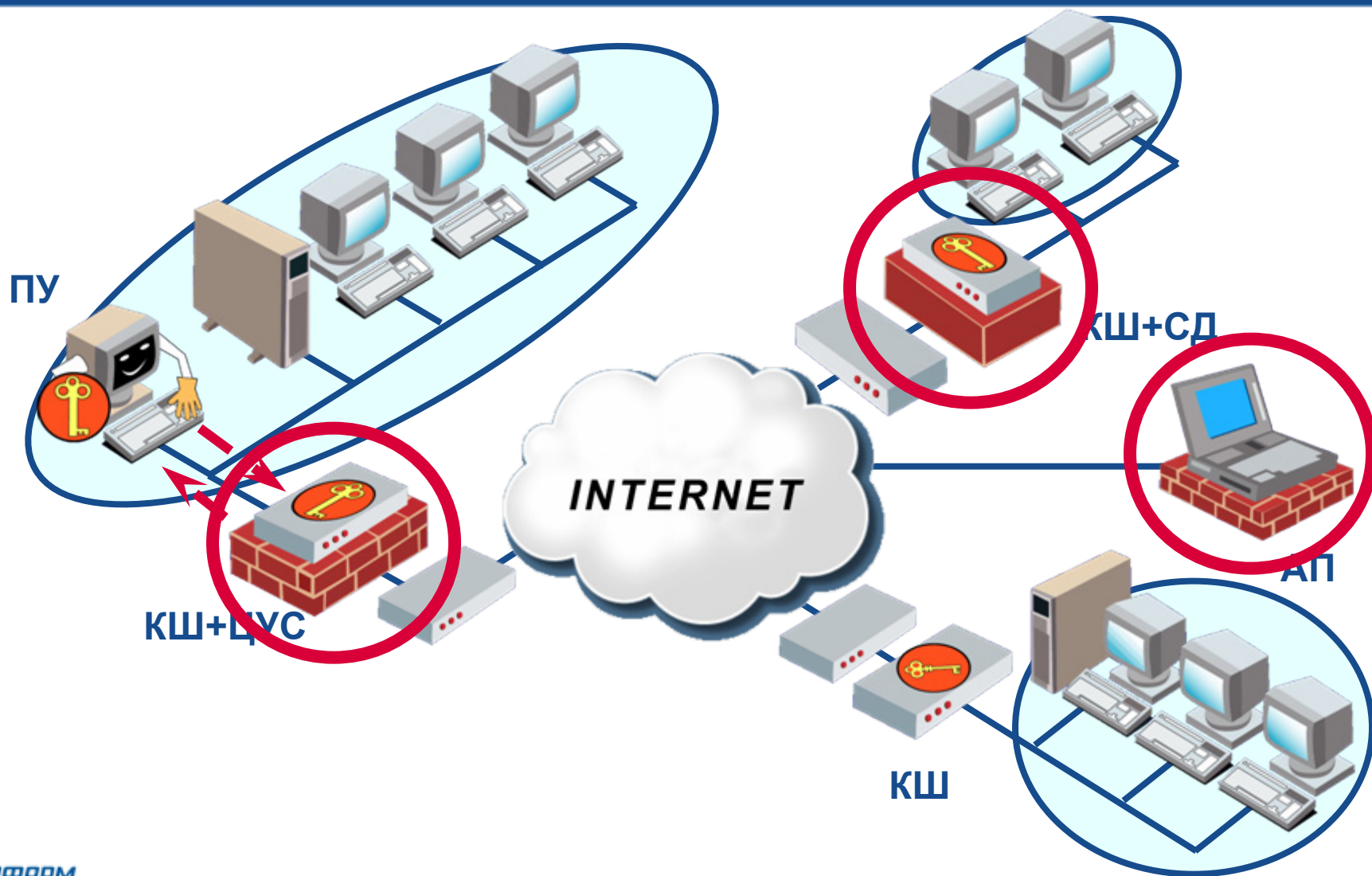


«Континент-1000»
высокопроизводительный

Структура АПКШ «Континент»



Схема построения VPN-сети на примере АПКШ «Континент»



Межсетевое экранирование

- ✓ Stateful inspection
- ✓ трансляция сетевых адресов (NAT)
- ✓ инкапсуляции пакетов
- ✓ Приоритизация



Сертификаты АПКШ «КОНТИНЕНТ»

Сертификат Гостехкомиссии России
года подтверждает соответствие
АПКШ "Континент" требованиям
руководящих документов
Гостехкомиссии России по 4-му
классу защищенности для
межсетевых экранов и по 3-му
уровню контроля на отсутствие
недекларированных возможностей.

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

 СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ
№ 808

Выдан 14 ноября 2003 г.
Действителен до 14 ноября 2006 г.

Настоящий сертификат удостоверяет, что аппаратно-программный комплекс шифрования «Континент», разработанный и производимый ЗАО Научно-инженерное предприятие «ИНФОРМЗАЩИТА» в соответствии с техническими условиями УВАЛ.00300-50 ТУ и предназначенный для построения виртуальных частных сетей (VPN) на основе глобальных сетей общего пользования, использующих протоколы семейства TCP/IP, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 3 уровню контроля и «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» по 4 классу защищенности.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ЦБИ-сервис» (аттестат аккредитации от 10.09.2001 № СИ RU.819.5026.059) - техническое заключение от 15.10.2003, и экспертного заключения Гостехкомиссии России от 12.11.2003.

Заявитель: ЗАО Научно-инженерное предприятие «ИНФОРМЗАЩИТА».
Адрес: 127018, Москва, а/я 55.
Телефон: (095) 289-42-32.

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям руководящих документов Гостехкомиссии России и технических условий осуществляется испытательной лабораторией ЗАО «ЦБИ-сервис».

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

 В.Г. Гадышчев

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 14 ноября 2003 г.

Сертификаты АПКШ «КОНТИНЕНТ»

Сертификаты соответствия ФСБ года
удостоверяют, что

- АПКШ "Континент"
- СКЗИ «Континент-АП»

могут быть использованы для
криптографической защиты конфиденциальной
информации.



Аппаратно-программное решение

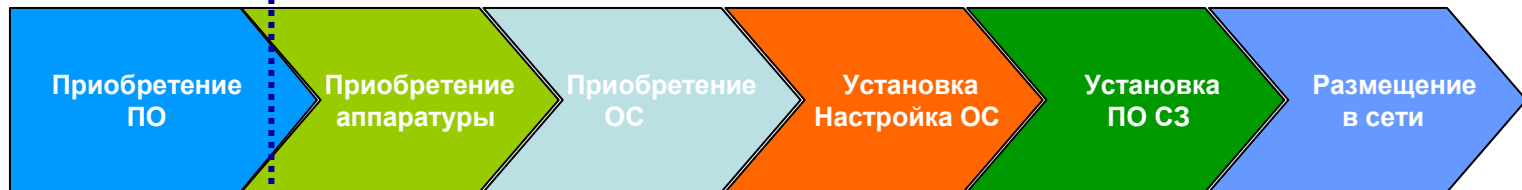
Специализированная аппаратная платформа



Внедрение за 15 минут? - ДА!

Вы
вскрываете
коробку...

Программное
решение



Аппаратное
решение



Устройство готово к работе
сразу после приобретения

Время внедрения



Достоинства Континент

✓ ЕДИНООБРАЗИЕ АППАРАТНОЙ ПЛАТФОРМЫ

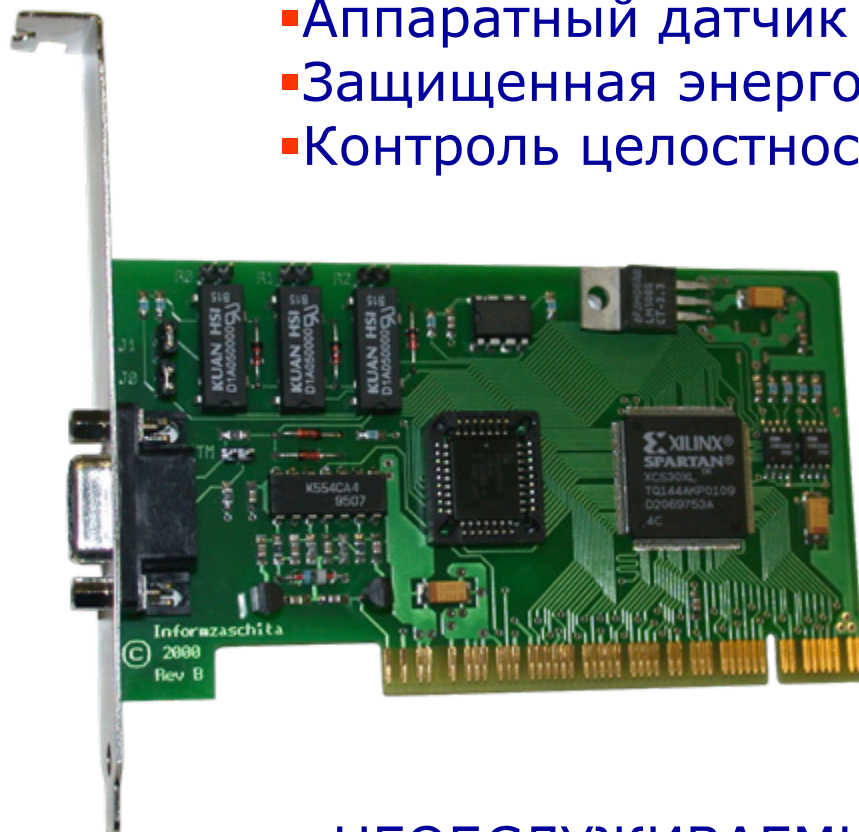


- Возможность построения кластерных решений
- Простое резервирование устройств
- Простота гарантийного обслуживания
- Быстрое восстановление работоспособности оборудования в случае его выхода из строя.

Достоинства Континент

✓ ИНТЕГРАЦИЯ С ЭЗ «Соболь»

- Блокировка внештатной загрузки ОС
- Аппаратный датчик случайных чисел
- Защищенная энергонезависимая память
- Контроль целостности файлов

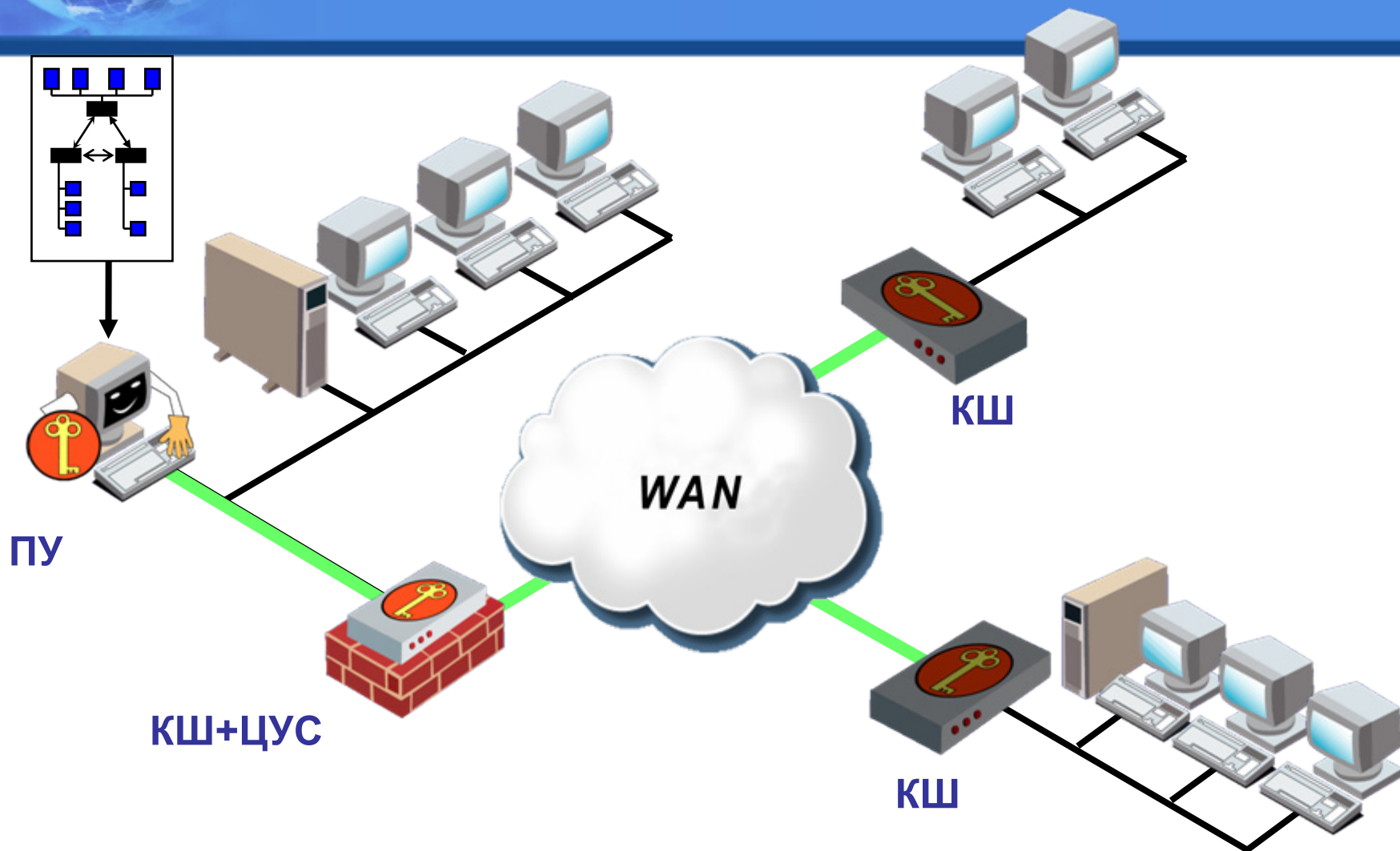


- НЕОБСЛУЖИВАЕМЫЙ КРУГЛОСУТОЧНЫЙ РЕЖИМ РАБОТЫ

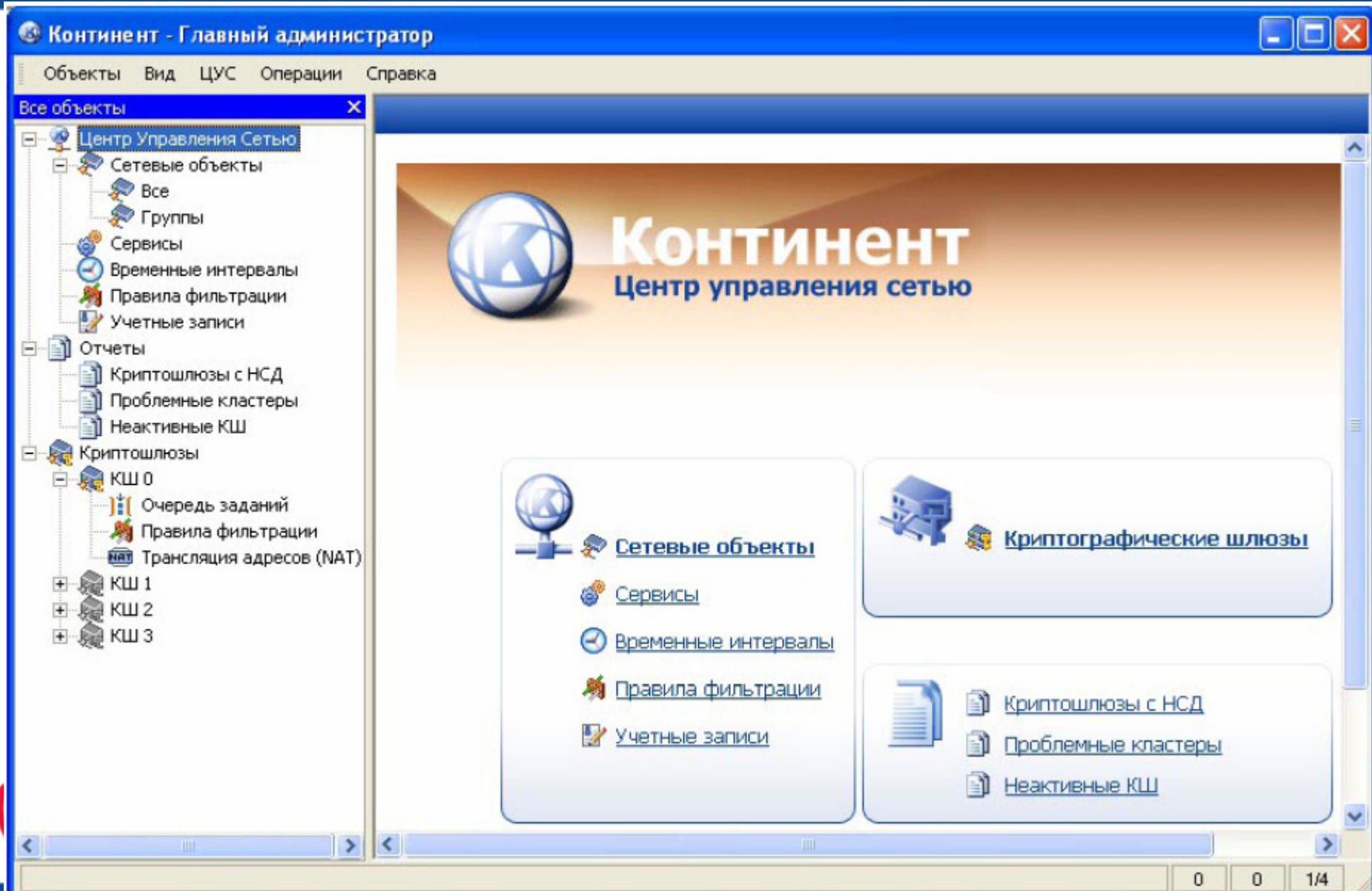


Возможности АПКШ «Континент»

Централизованное управление



Графический интерфейс управления



Все объекты

- Центр Управления Сетью
 - Сетевые объекты
 - Все
 - Группы
 - Сервисы
 - Временные интервалы
 - Правила фильтрации**
 - Учетные записи
 - Криптошлюзы
 - КШ с ЦУСом
 - Очередь заданий
 - Правила фильтрации
 - Трансляция адресов (NAT)
 - Криптошлюз 2
 - Очередь заданий
 - Правила фильтрации
 - Трансляция адресов (NAT)
 - Криптошлюз 3
 - Очередь заданий
 - Правила фильтрации
 - Трансляция адресов (NAT)
 - Отчеты
 - Криптошлюзы с НСД
 - Проблемные кластеры
 - Неактивные КШ

Правила фильтрации

Название	Отправитель	Получатель	Обработка па...	Временной и...	Регистрация	Сервисы
134.17.11.0/24 ->...	Защищаемая сеть КШ "КШ с ЦУС...	192.168.1.0/24	Пропустить	Постоянно	Не регистриров...	Любой TCP; Лю...
192.168.1.0/24->...	192.168.1.0/24	Защищаемая се...	Пропустить	Постоянно	Не регистриров...	Любой TCP; Лю...
FTP сервер	Защищаемая сеть КШ "КШ с ЦУС...	Сервер FTP	Пропустить	Постоянно	Не регистриров...	ftp;

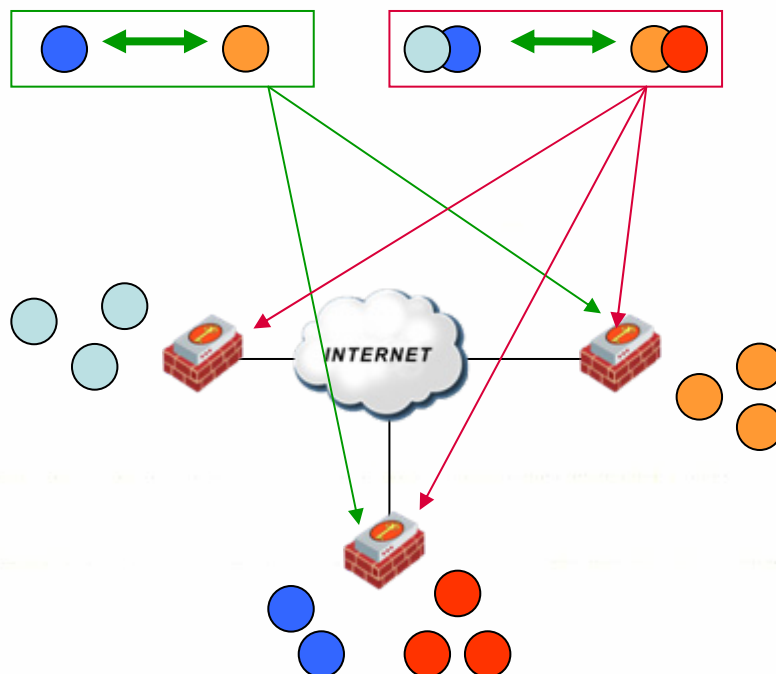
Континент - Главный администратор

Все объекты

- Центр Управления Сетью
 - Сетевые объекты
 - Все
 - Группы
 - Сервисы
 - Временные интервалы
 - Правила фильтрации
 - Учетные записи
 - Криптошлюзы
 - КШ с ЦУСом
 - Очередь заданий
 - Правила фильтрации
 - Трансляция адресов (NAT)
 - Криптошлюз 2
 - Очередь заданий
 - Правила фильтрации**
 - Трансляция адресов (NAT)
 - Криптошлюз 3
 - Очередь заданий
 - Правила фильтрации
 - Трансляция адресов (NAT)
 - Отчеты
 - Криптошлюзы с НСД
 - Проблемные кластеры
 - Неактивные КШ

Правила фильтрации (Криптошлюз 2)

Название	Отправитель	Получатель	Обработка па...	Временной и...	Регистрация	Сервисы
134.17.11.0/24 ->...	Защищаемая сеть КШ "КШ с ЦУС...	192.168.1.0/24	Пропустить	Постоянно	Не регистриров...	Любой TCP; Лю...
192.168.1.0/24->...	192.168.1.0/24	Защищаемая се...	Пропустить	Постоянно	Не регистриров...	Любой TCP; Лю...



Все объекты

- Центр Управления Сетью
 - Сетевые объекты
 - Все
 - Группы
 - Сервисы
 - Временные интервалы
 - Правила фильтрации
 - Учетные записи
 - Криптошлюзы
 - КШ с ЦУСом
 - Криптошлюз 2
 - Криптошлюз 3
 - Отчеты

Сетевые объекты

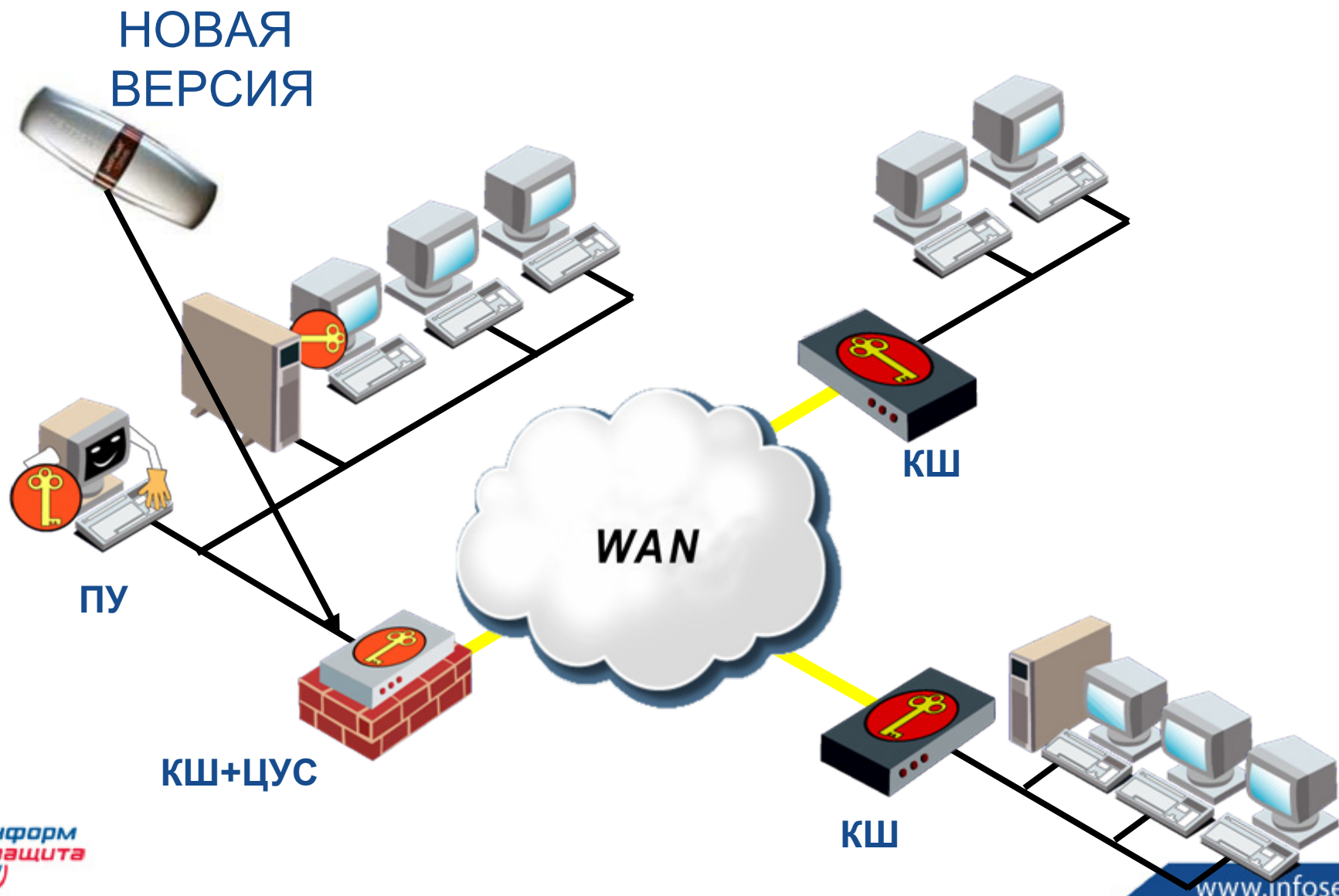


Наименование	Описание	IP-адрес	Маска	Криптошлюз	Тип привязки	Интерфейс
Любой	Любой	0.0.0.0	0.0.0.0		Нет	
Защищаемая сеть КШ "КШ ...	Защищаемая сеть КШ ...	134.17.11.0	255.255.255.0	КШ с ЦУСом	Защищаемый	fxp1
192.168.1.0/24	Защищаемая сеть Кри...	192.168.1.0	255.255.255.0	Криптошлюз 2	Защищаемый	fxp1
Сервер FTP		10.2.0.252	255.255.255.255		Нет	
192.168.2.0/24		192.168.2.0	255.255.255.0	Криптошлюз 3	Внутренний	fxp2

Возможность ролевого управления

Элемент управления	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Просмотр правил фильтрации	+	+	-	+
Изменение правил фильтрации	+	+	-	-
Управление настройками КШ	+	+	-	-
Управление журналами	+	-	-	+
Управление пользователями	+	-	-	-

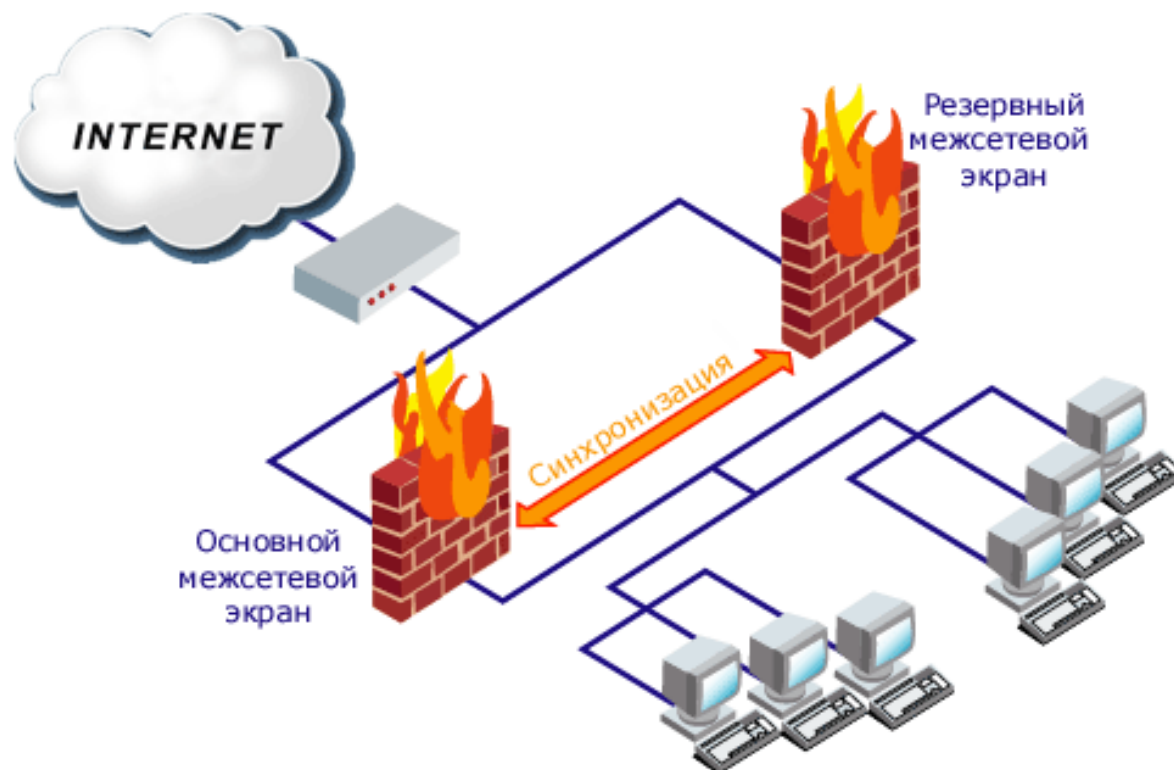
Удаленное обновление ПО



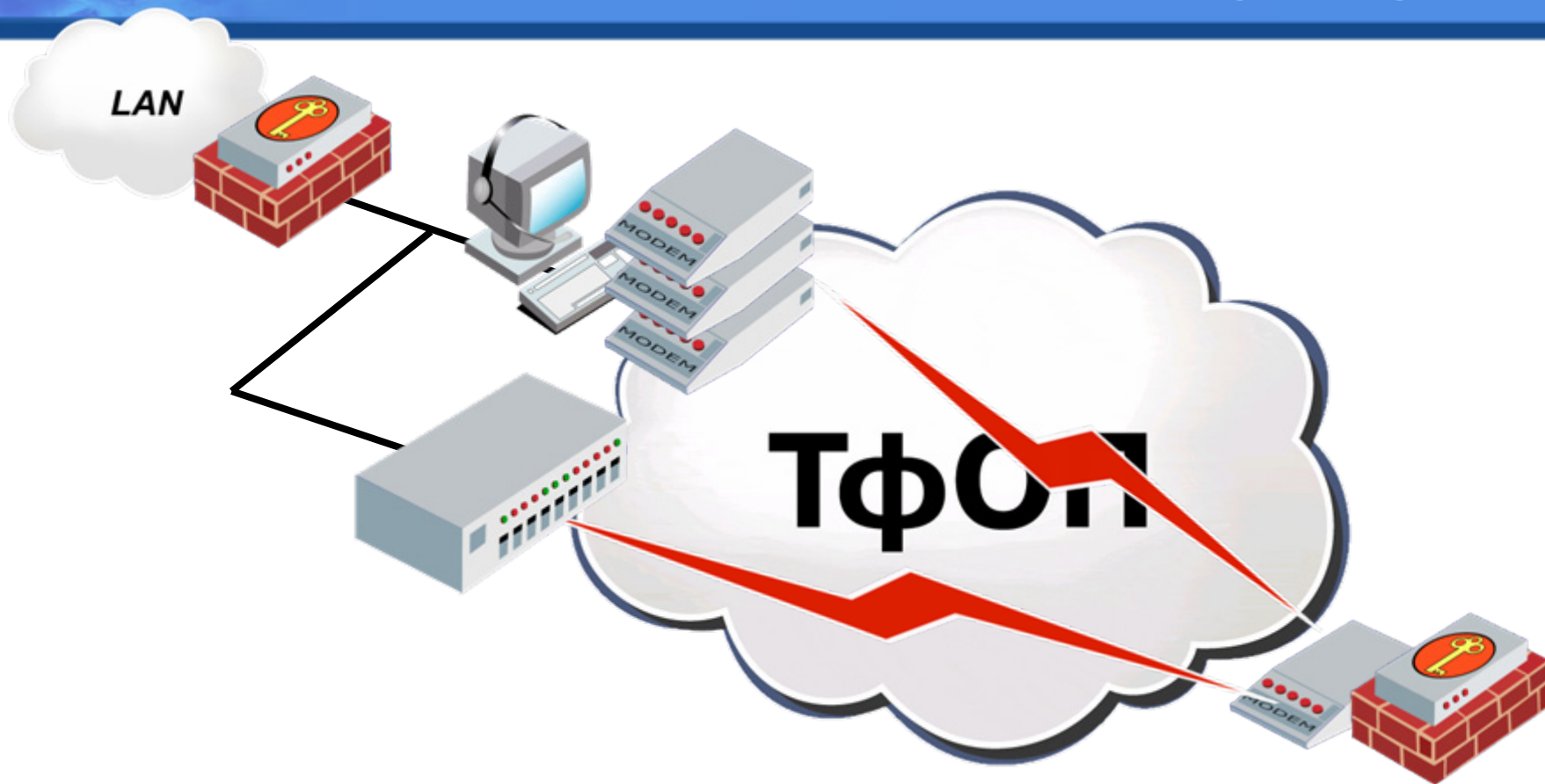
Высокая надежность

Реализованы механизмы

- ✓ «Холодного» резервирования
- ✓ «Горячего» резервирования

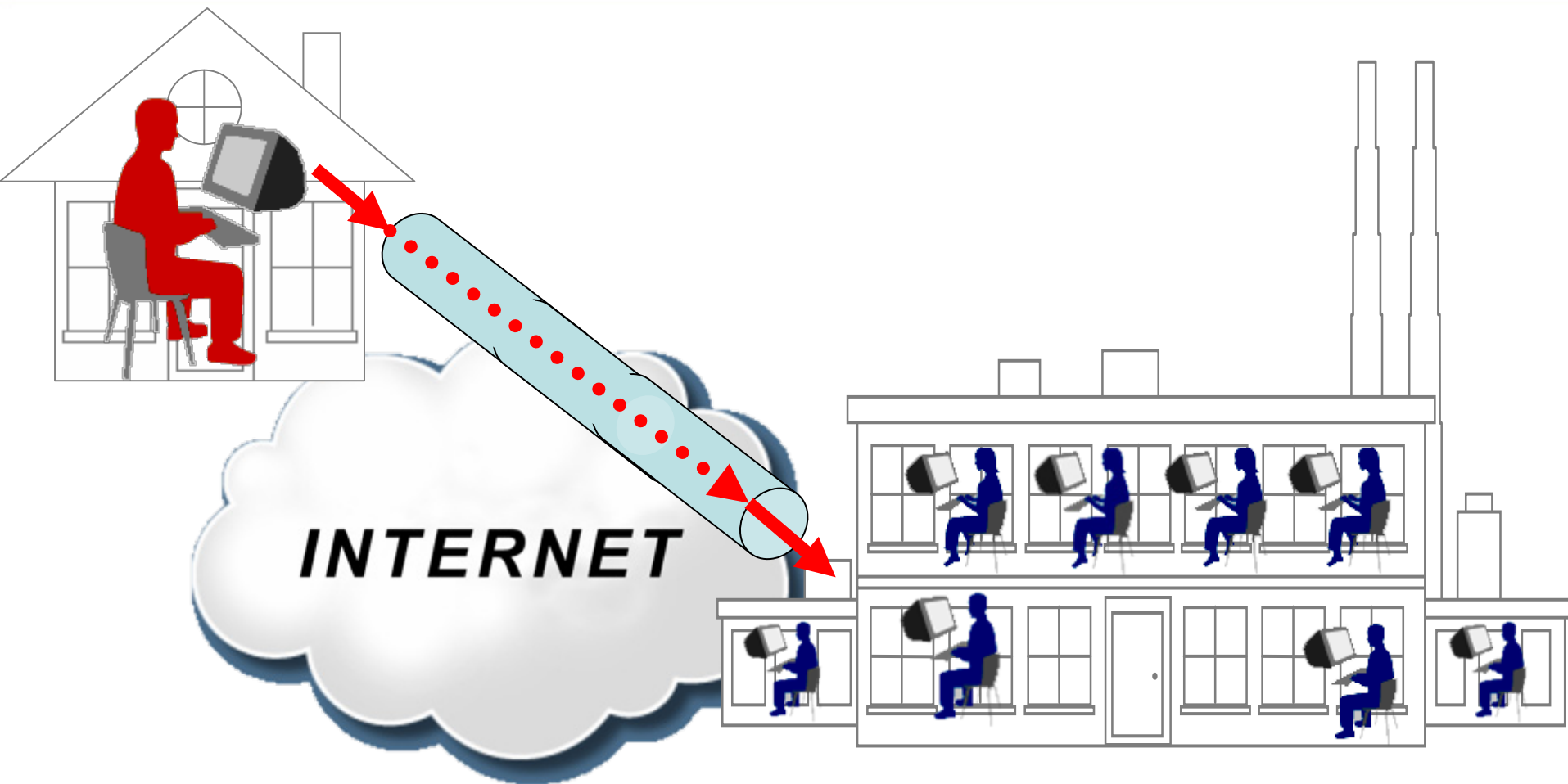


Работа по различным каналам связи

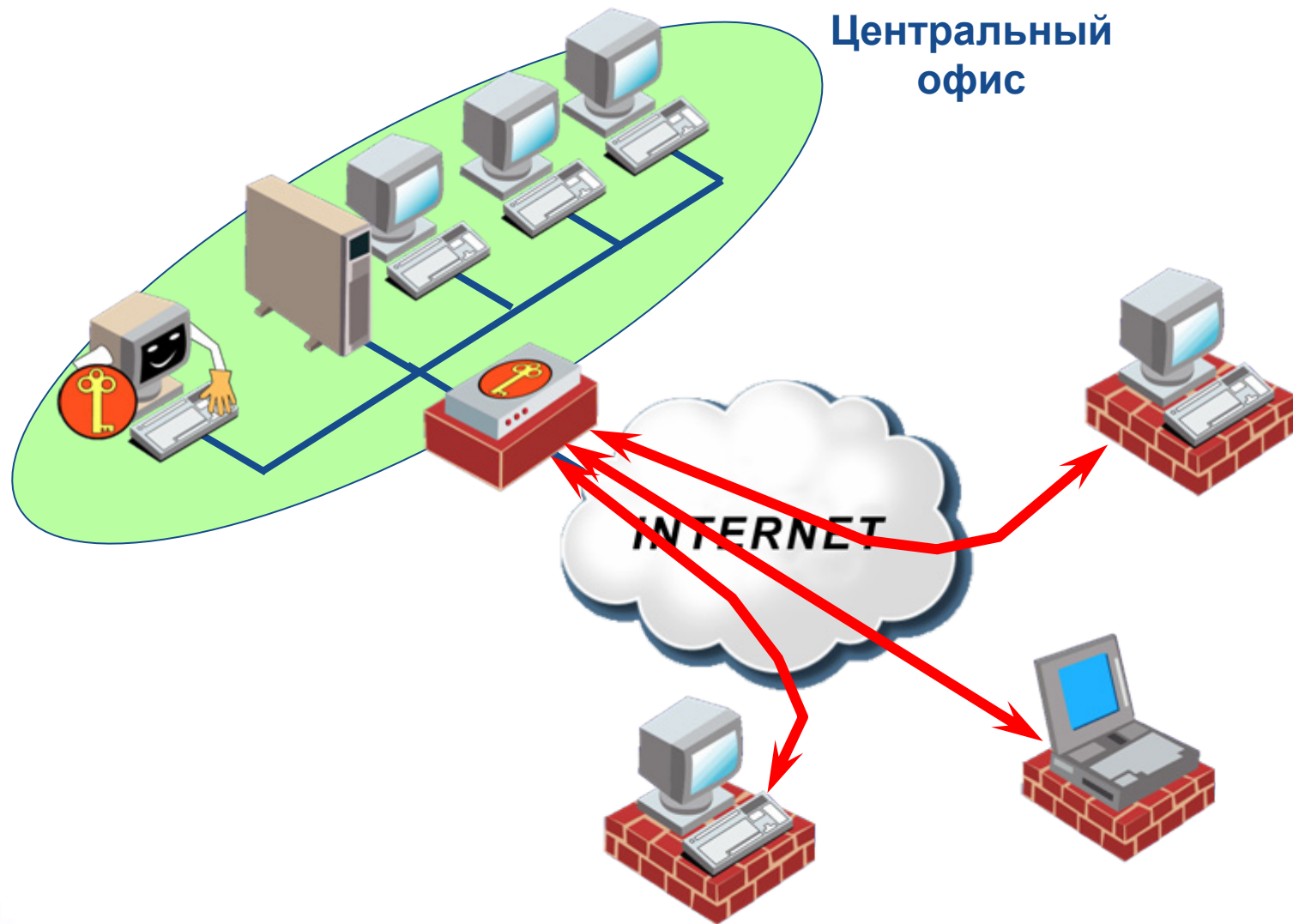


Реализован механизм удаленного доступа.

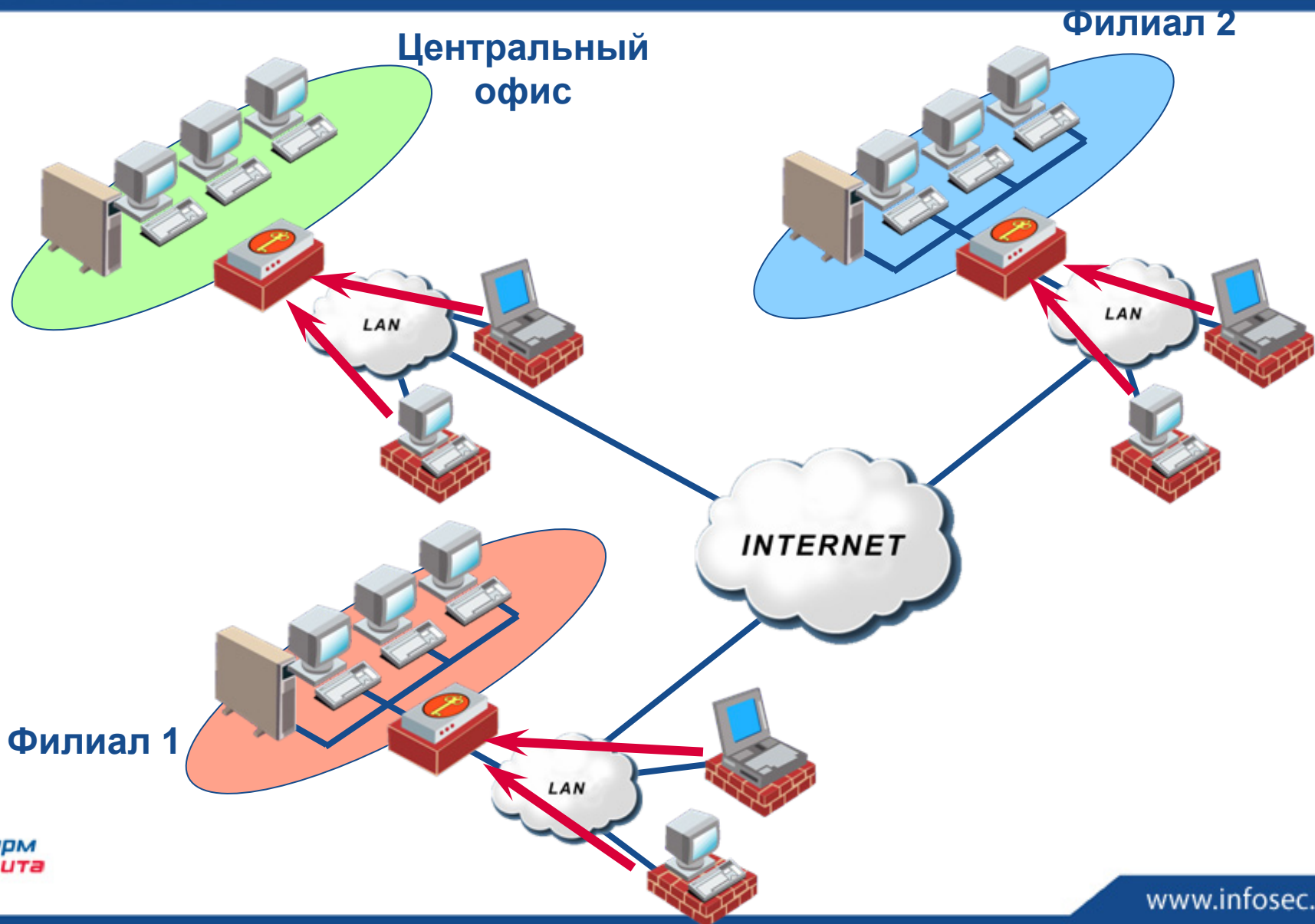
Возможности удаленного доступа



Централизованное подключение АП

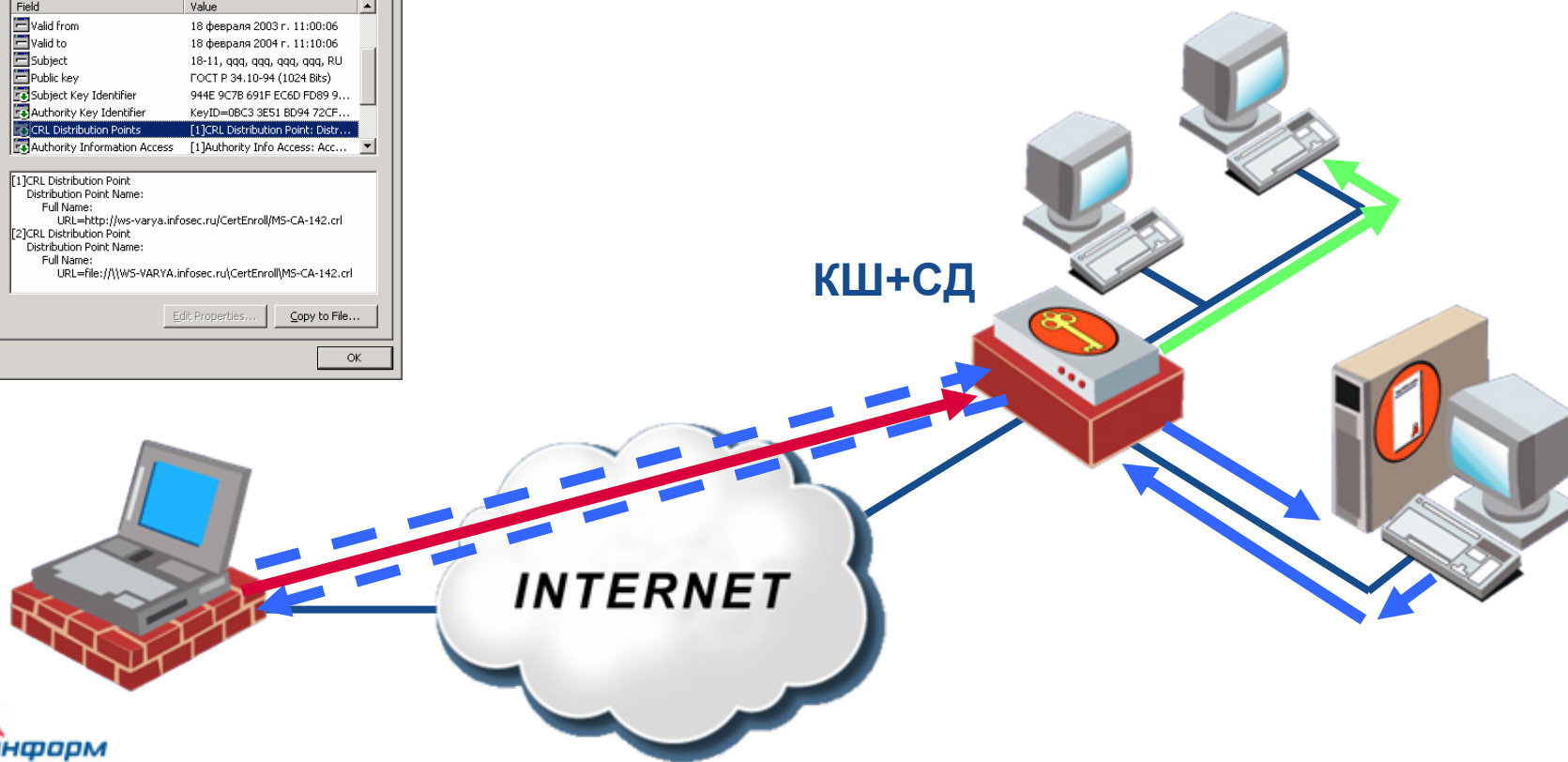
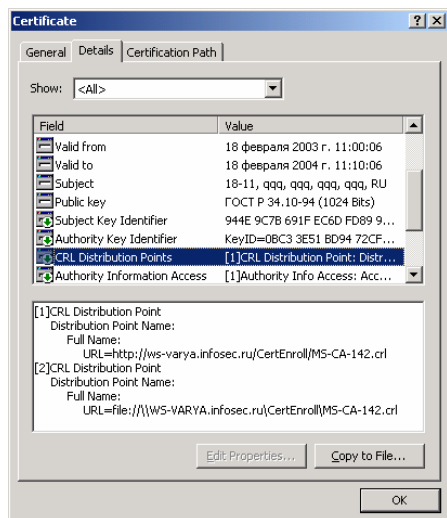


Подключение АП по схеме «дерево»



Возможности удаленного доступа

Интеграция с РКИ

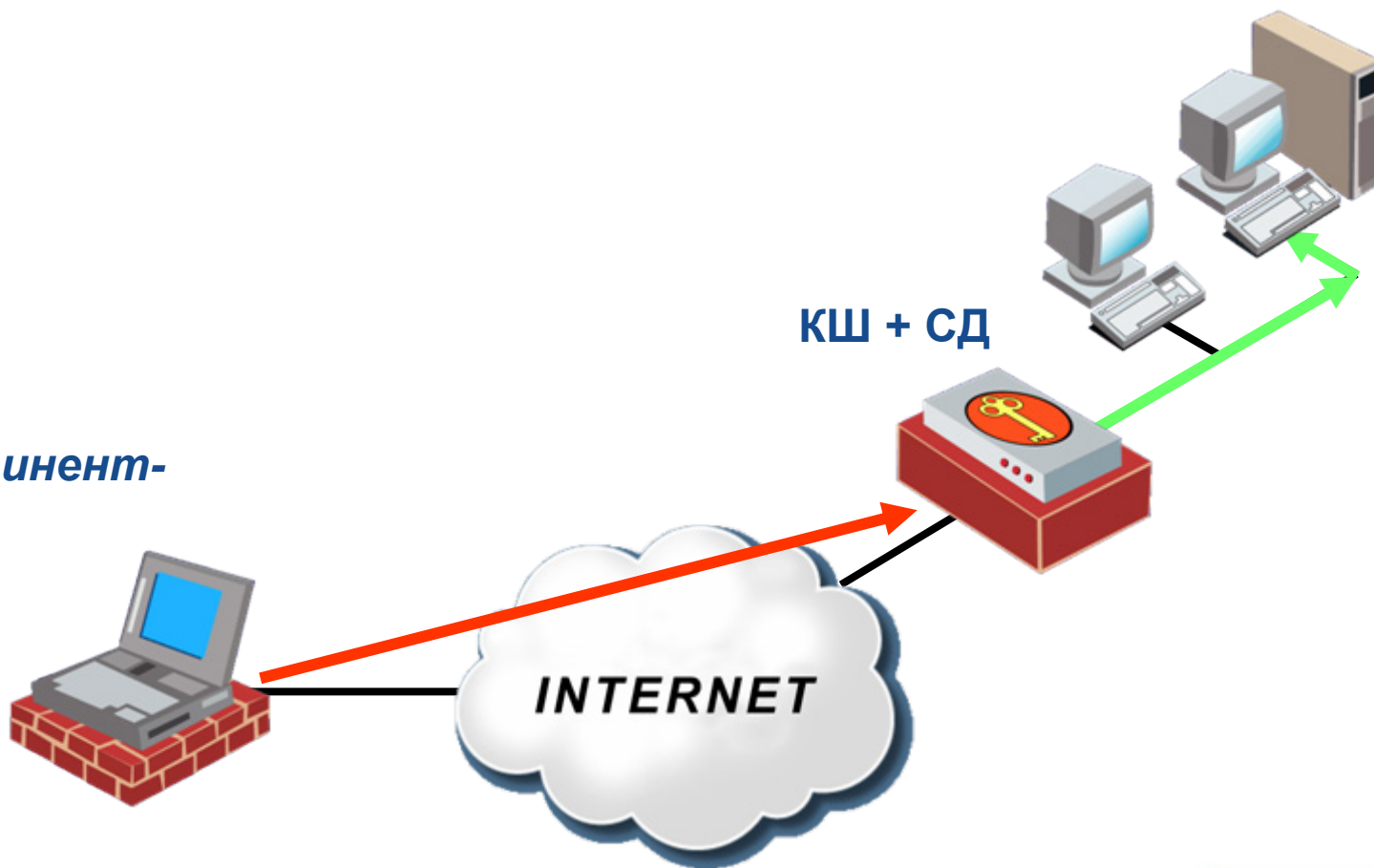


Абонентский пункт СКЗИ «Континент-АП»

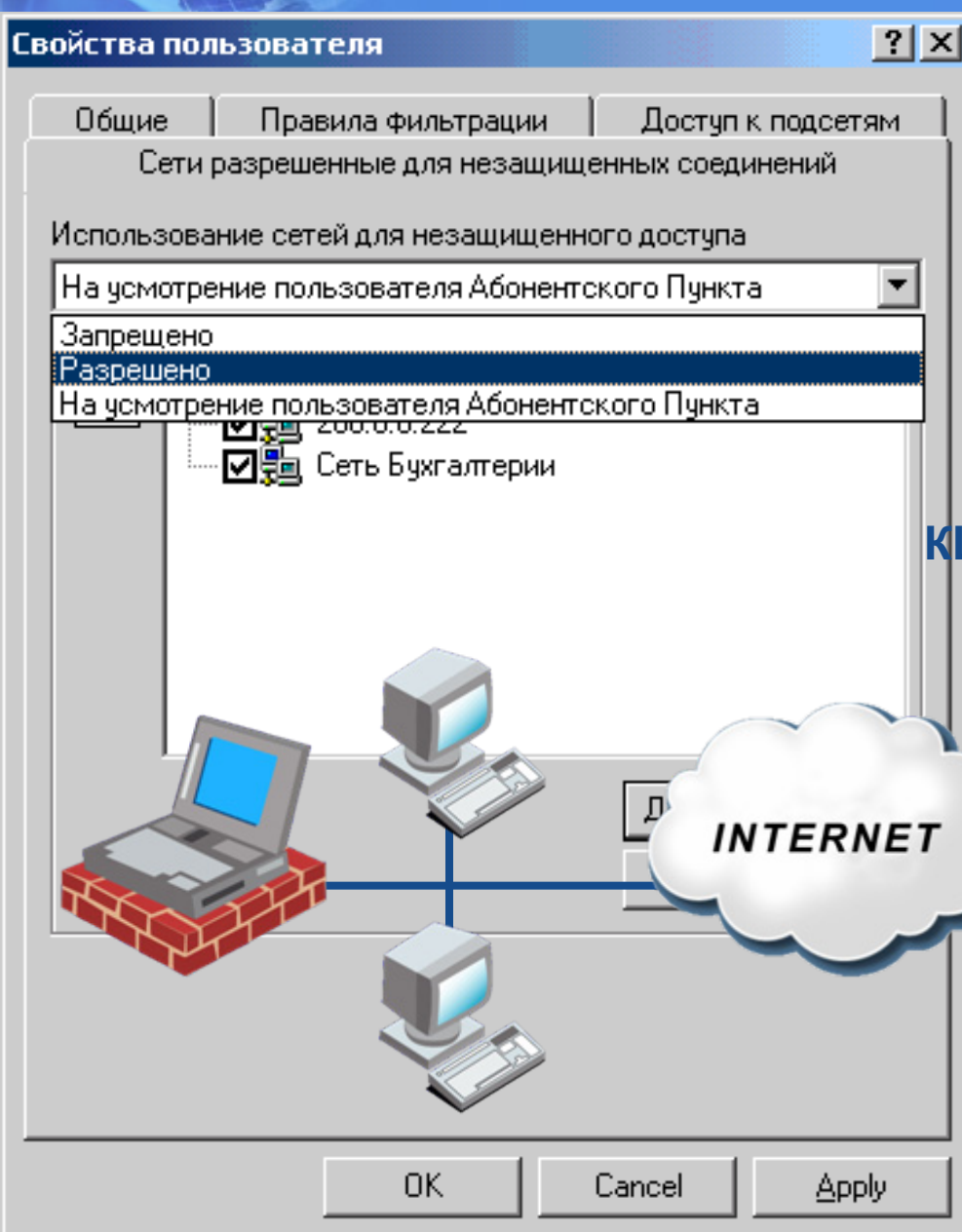


- Добавлена возможность назначения абонентскому пункту внутрисетевого адреса.

СКЗИ «Континент-АП»



Локальная безопасность АП



КШ+СД

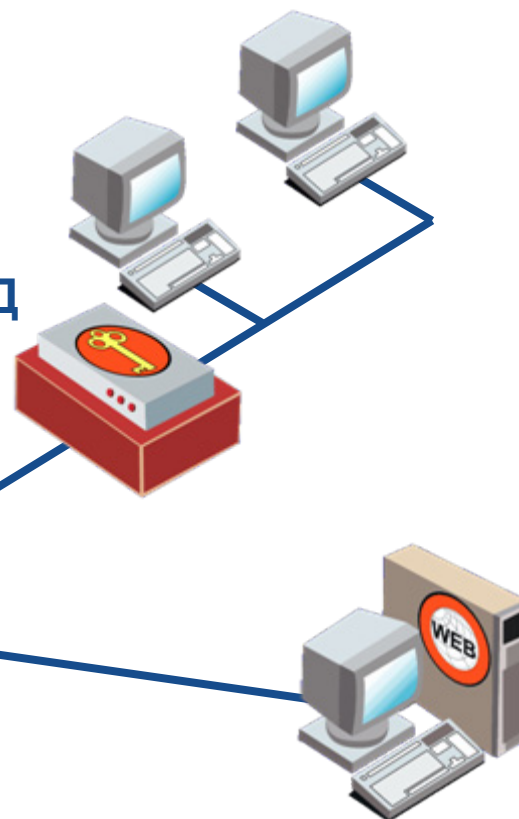
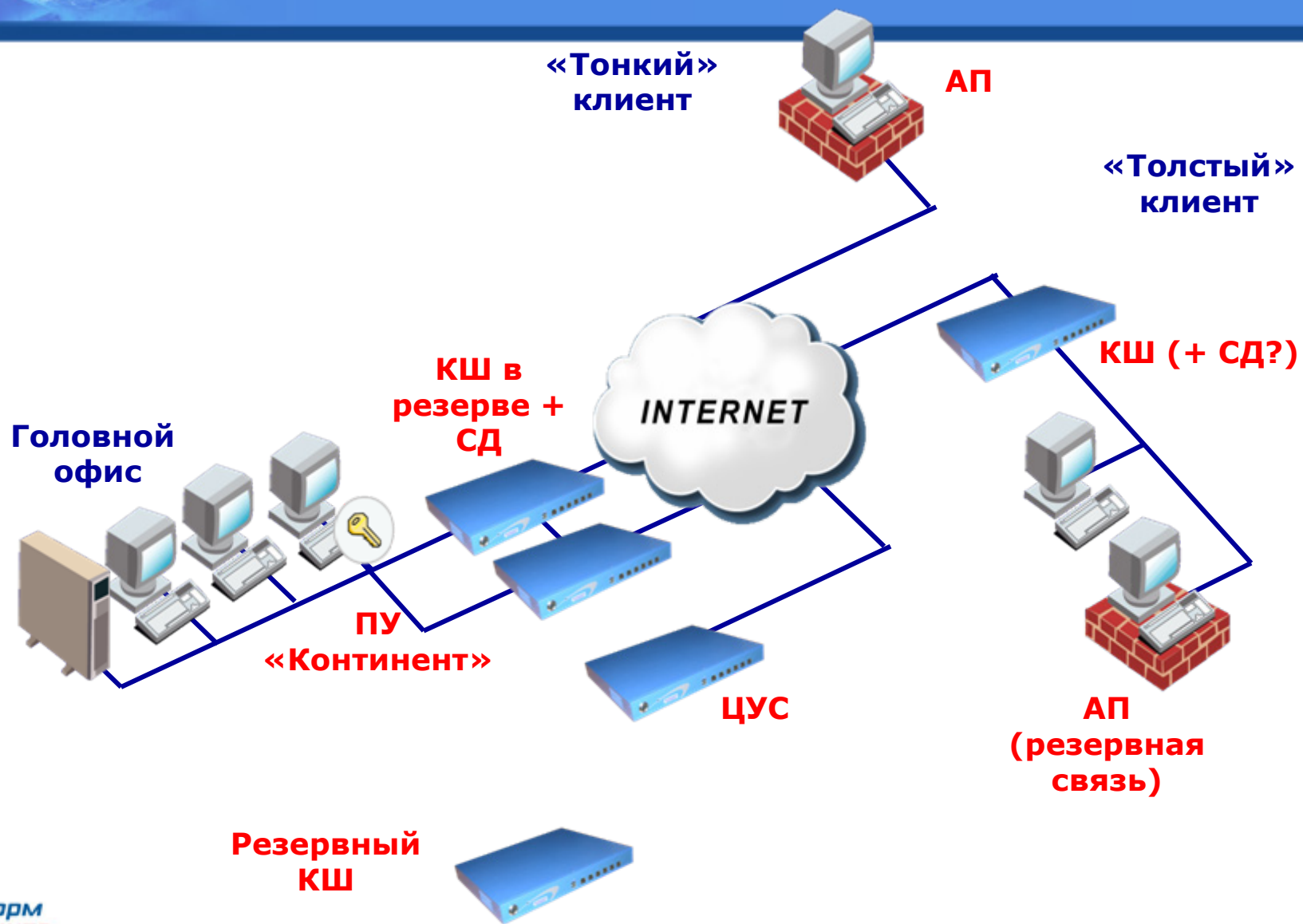


Схема типовой корпоративной сети



Зрелое решение

Более 15000 установок:

- Минфин России
- ГАС «Выборы»
- 27 регионов ЦБ России
- Нефтяные корпорации





ВОПРОСЫ?