

Контроль доступа к сети. Практика внедрения.

Максим Лукин

Руководитель направления Информационная
Безопасность

Cisco Expo 2011



Программа

Область применения

Практика внедрения. Подход СТИ

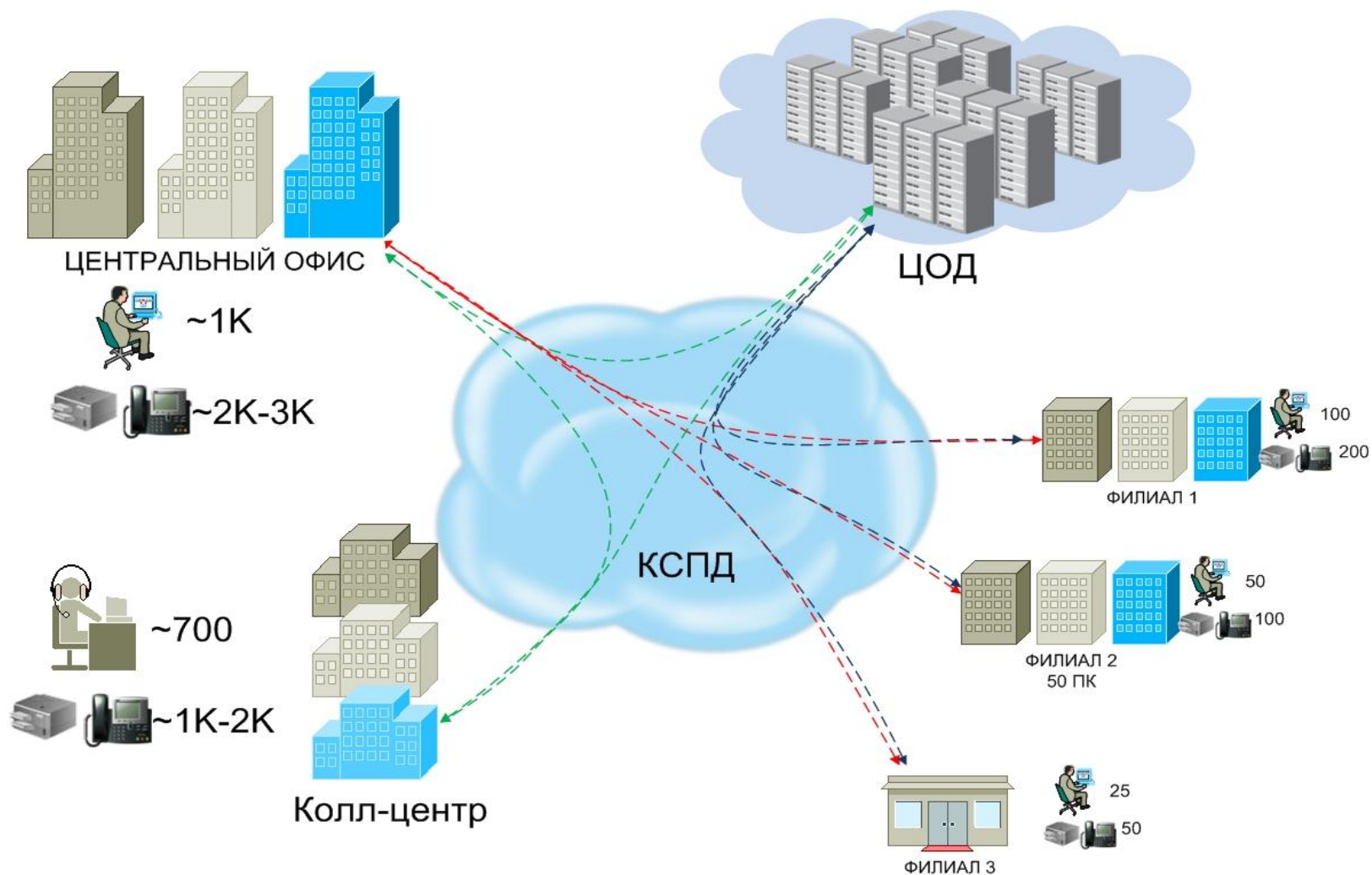
Область применения

В качестве примера рассмотрим организацию в сегменте крупного бизнеса:

Финансово-кредитная организация:

- Современная динамично развивающаяся компания
- Большая клиентская база
- Широкий портфель услуг для корпоративных заказчиков и частных клиентов
- Рыночная капитализация может достигать млрд долларов
- Высокая стоимость информационных активов
- Организация сильно зависит от ИТ структуры

Инфраструктура организации



Задачи по обеспечению ИБ

- Снижение рисков ИБ
 - Предотвращение утечки конфиденциальной информации
 - Защита от вредоносного ПО
- Контроль сетевого доступа
- Соответствие нормативным требованиям
- Возможность реализации политик ИБ



Средства реализации поставленных задач

- ПО контроля съемных устройств
- Системы предотвращения утечки конфиденциальной информации (DLP)
- Антивирус с обновленной базой сигнатур
- Контроль доступа к сети
- Контроль соответствия
- Организационные меры

Практика внедрения. Подход СТИ

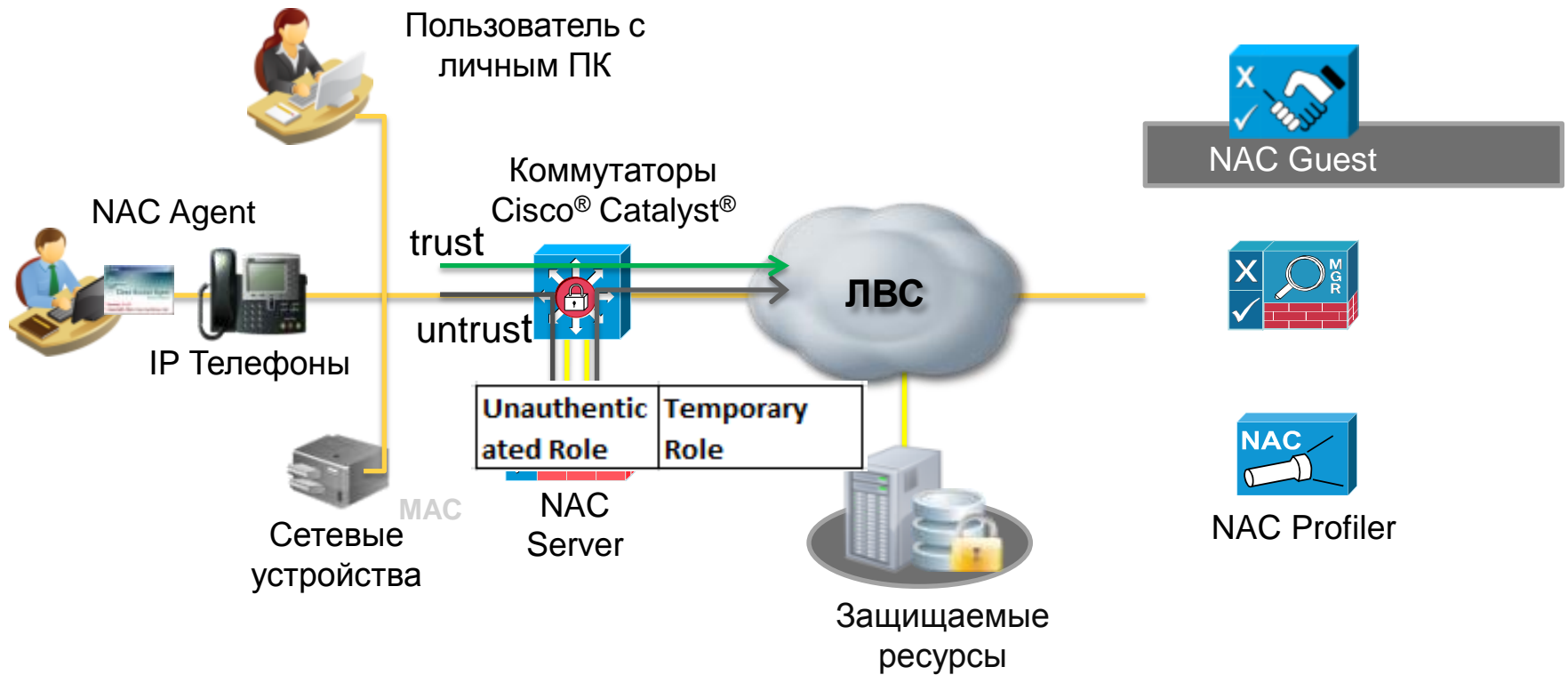
Предпроектное обследование

**Подбор оптимального решения для
вашего бизнеса**

Пилотное внедрение

Проект

Реализация требования «Обеспечения контроля доступа» средствами Cisco NAC

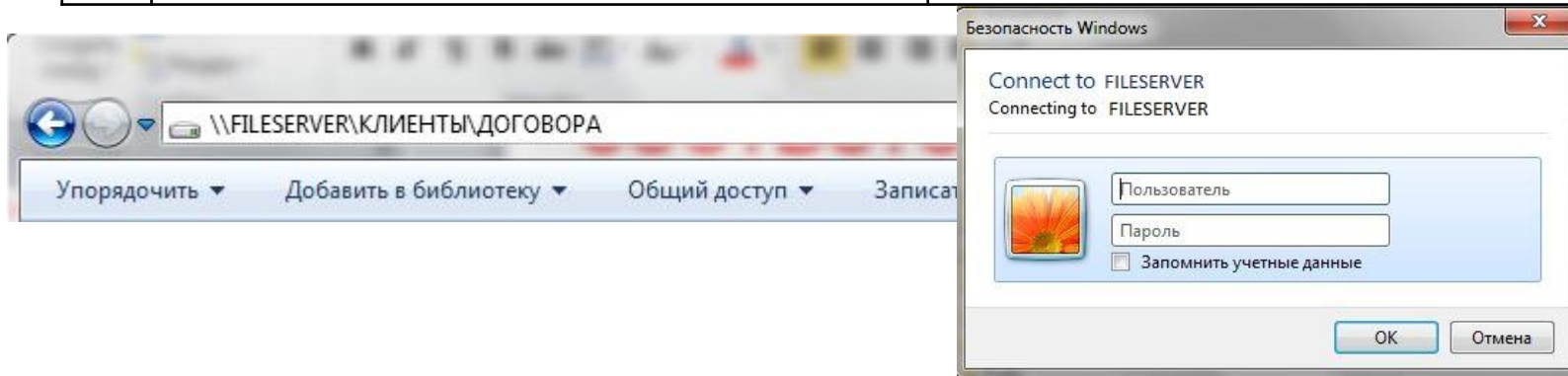


Сценарии доступа к ЛВС

	Характеристика ПК	Риски
1	Корпоративный ПК с установленными средствами защиты	Каналы утечки перекрыты, риски минимальны
2	Корпоративный ПК без установленных средств защиты	Каналы утечки не перекрыты. Защита от вредоносного ПО не обеспечивается
3	Личный ПК без средств защиты	

Решения Cisco NAC и Cisco ISE

**Контроль доступа
Проверка соответствия**



Сценарии контроля доступа с помощью Cisco NAC

Весь трафик от устройств доступа проходит через две роли

1 «Не прошедший аутентификацию»

2 «Временная роль»

Для роли 1 необходимо разрешать трафик к контроллерам домена и файловым серверам.

Доступ к файловым серверам разрешён?

- Любой пользователь, подключившейся к сети с личного ноутбука будет иметь доступ к файловым серверам и конфиденциальной информации.
- Корпоративные пользователи без Cisco NAC агента будут иметь доступ к конфиденциальной информации.

Если запретить доступ к файловым серверам?

- Обеспечена надежная защита конфиденциальной информации
- Возникновение проблемы с сетевыми дисками
- Возникновение проблемы с загружаемыми профилями
- Увеличение времени загрузки ОС

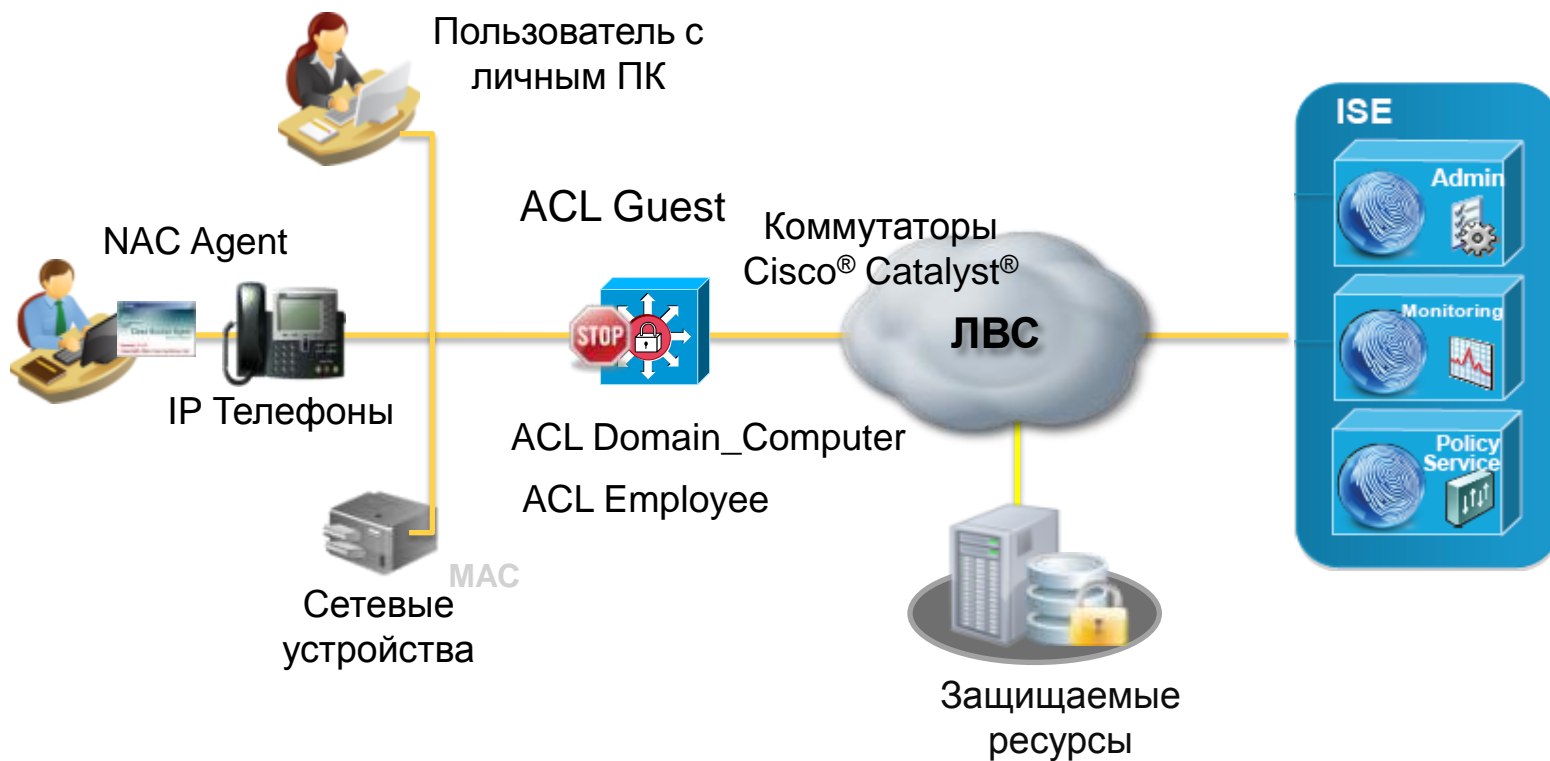
Unauthenticated Role		Temporary Role	
V Контроллеры домена	V Файловые серверы	V Контроллеры домена	X Файловые серверы
TCP 88,123,135,137,1 38,139,389,445,6 36,1025,1026,32 68,49152-65535	TCP 138,139,389, 445	TCP 88,123,135,137, ,138,139,389,4 45,636,1025,10 26,3268,49152- 65535	X
UDP 88,123,135,137,1 38,139,389,445,6 36,1025,1026,32 68	IP FRAG	UDP 88,123,135,137, ,138,139,389,4 45,636,1025,10 26,3268	X
IP FRAG		IP FRAG	

Unauthenticated Role		Temporary Role	
V Контроллеры домена	X Файловые серверы	V Контроллеры домена	X Файловые серверы
TCP 88,123,135,137,1 38,139,389,445,6 36,1025,1026,32 68,49152-65535	X	TCP 88,123,135,137, ,138,139,389,4 45,636,1025,10 26,3268,49152- 65535	X
UDP 88,123,135,137,1 38,139,389,445,6 36,1025,1026,32 68	X	UDP 88,123,135,137, ,138,139,389,4 45,636,1025,10 26,3268	X
IP FRAG		IP FRAG	

Ограничения Cisco NAC

- Отсутствие гибких механизмов контроля доступа к сети
- Проблемы с отчетностью
- Сложности при диагностировании неисправностей
- Ограничения при масштабировании
- Пользователи без Cisco NAC агента «скрытно» работают через роль «Не прошедший аутентификацию»
- Для аутентификации AD SSO должен быть установлен NAC Agent
- Модель «Переключение между vlan», «Смена IP адреса» приводит к проблемам в работе некоторых приложений

Реализация требования «Обеспечения контроля доступа» средствами Cisco ISE



Cisco ISE

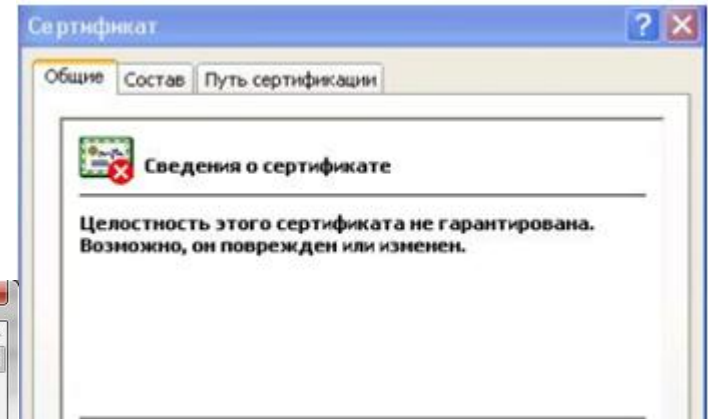
- Гибкие возможности контроля доступа
- Решается проблема с загрузкой профилей
- Решается проблема с подключением сетевых дисков
- Политика на основании контекста
- Аутентификация в сети происходит с помощью встроенного саппликанта 802.1x.
- Пользовательская аутентификация
- Проверка соответствия
- Профилирование

Что еще важно учесть при внедрении систем контроля доступа?

- Если взаимодействия между NAC Agent и сервером нет, то необходимо:
 1. Проверить, что корневые сертификаты установлены
 2. Проверить, что корневые сертификаты установлены корректно
 3. Проверить «время»
 4. Проверить доступ к серверу



```
Командная строка
G:\>
G:\>telnet 172.18.80.1 8905
```



- **Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4**
http://www.cisco.com/en/US/docs/security/ise/1.0/troubleshooting_guide/ise10_tsg.html

Пилотное внедрение

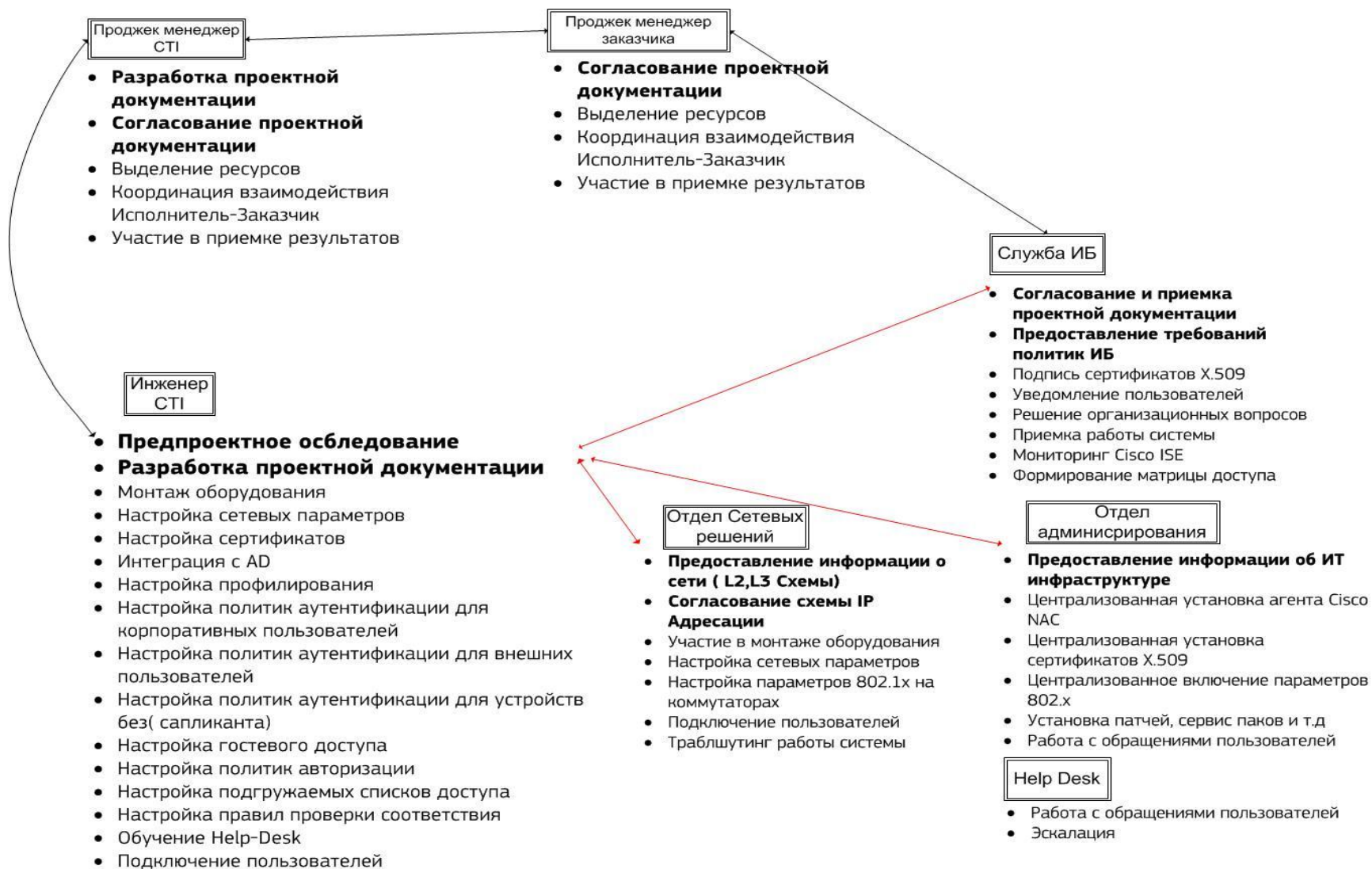
- Формализация целей проекта
- Формирование рабочей группы
- Четкое распределение ролей
- Сбор требований, включая:
 1. Политики безопасности
 2. Типы и количество устройств доступа к сети
 3. Обследование сетевой инфраструктуры
- Определение состава проектной документации
- Определение критериев успеха
 1. Желательно зафиксировать полученные договорённости в проектной документации (Устав Проекта)
- Обучение, подготовка регламентов и инструкций для службы технической поддержки
- Подготовка памятки пользователя по работе с системой

Практика внедрения. Размышления

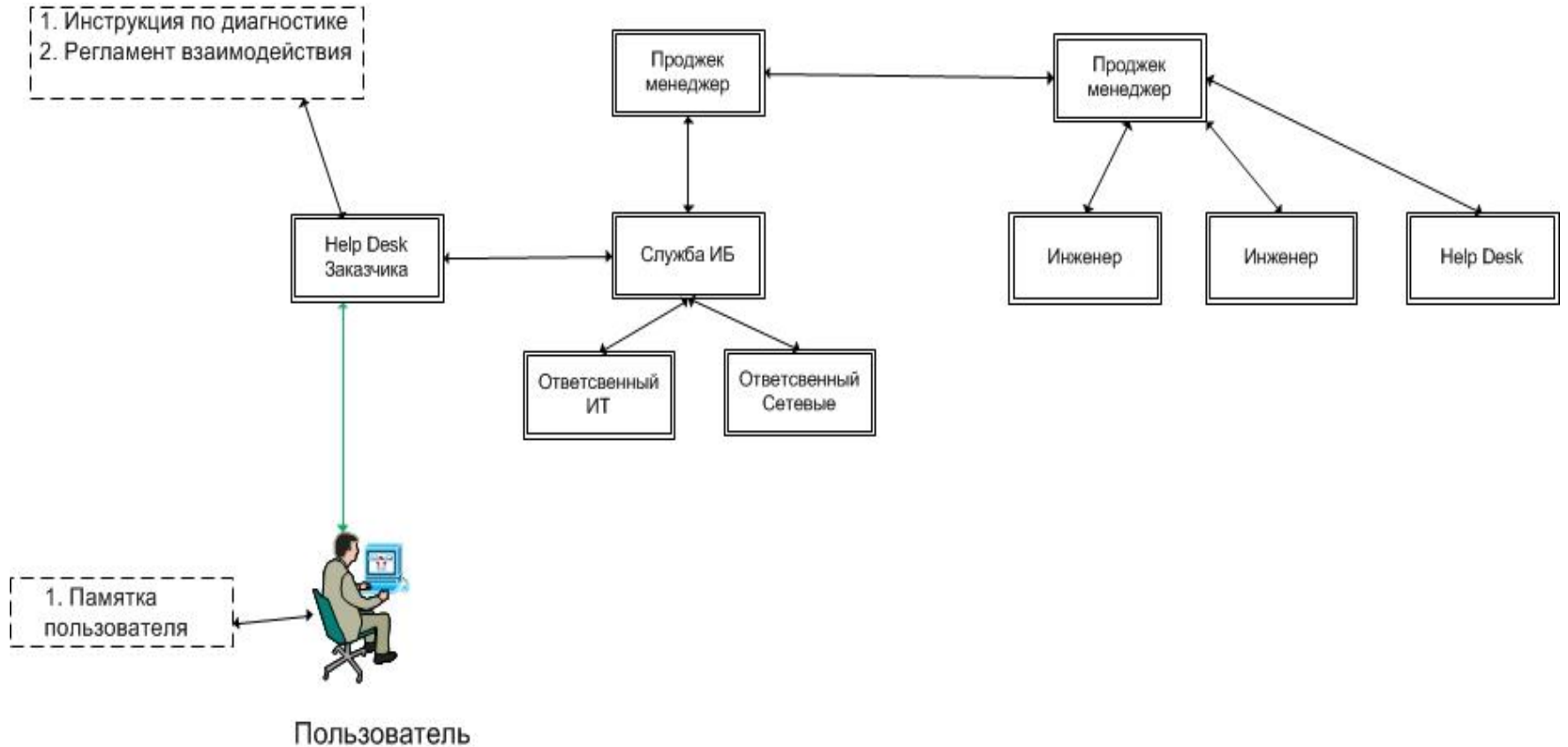
Важно для проекта:

1. Оценка трудозатрат всех участников проекта:
 - Департамент ИТ для централизованной установки Cisco NAC, корневых сертификатов, сервис паков, включение сапликантов 802.1x
 - Департамент сетевых технологий
 - а) подготовка сетевой инфраструктуры
 - б) совместное подключения пользователей (вечерние, ночные работы)
2. Разработка схемы взаимодействия Интегратор-Заказчик
3. Предоставление удаленного доступа Интегратор-Заказчик

Предпроектное обследование



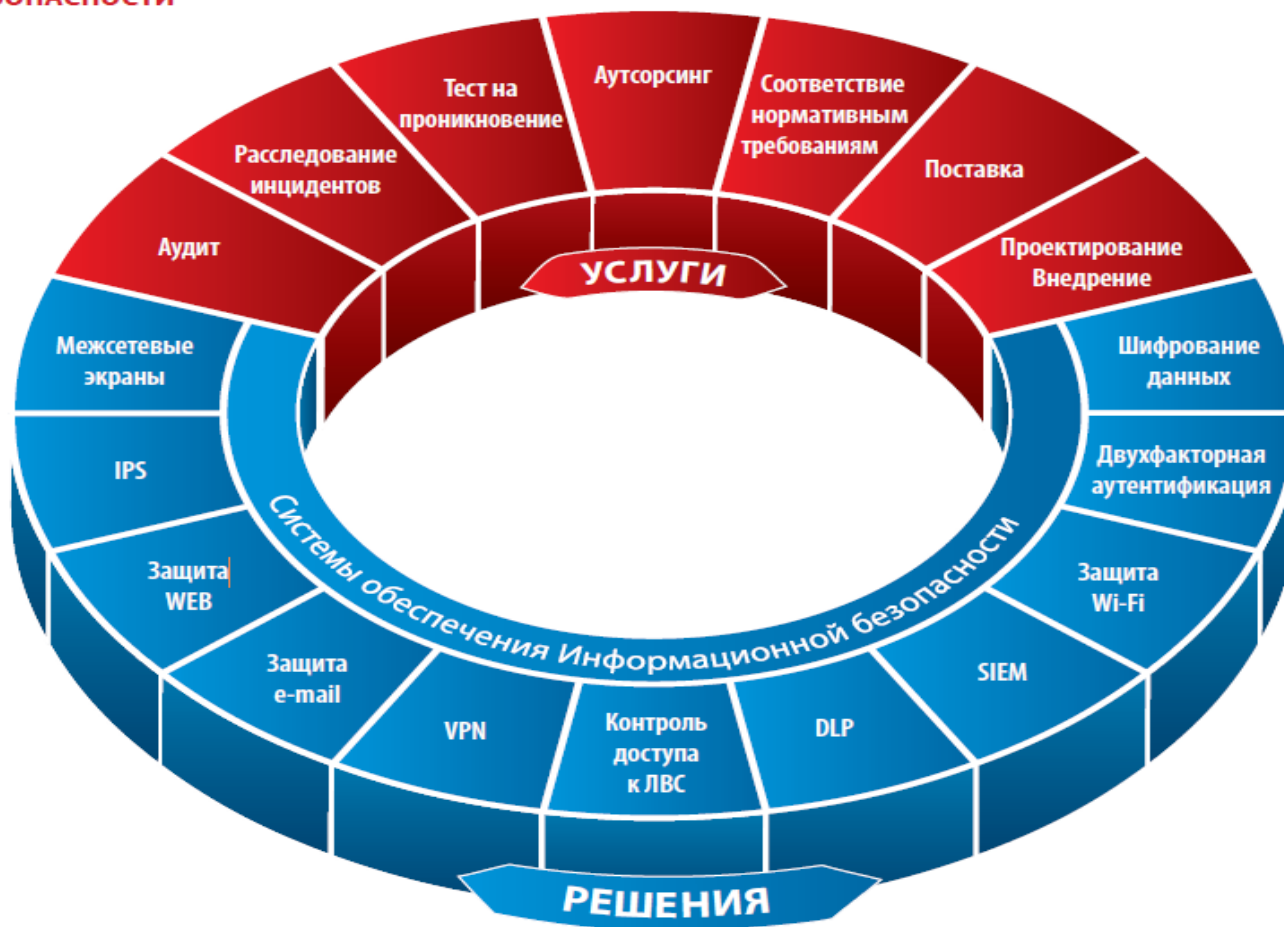
Работа с обращениями пользователей



ПРОЕКТ

Масштабирование результатов
достигнутых в ходе пилотного
проекта

**УСЛУГИ И РЕШЕНИЯ
СТІ В СФЕРЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**



Посетите стенд СТИ
для получения более подробной
информации о продуктах и
решениях

Максим Лукин

Руководитель направления Информационная
Безопасность

m.lukin@cti.ru

www.cti.ru / info@cti.ru
+7.495.784.73.13

СТИ Communications
Technology
Innovations