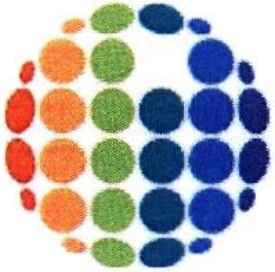


IPMATIKA

«Безопасность VoIP-коммуникаций»

Дмитрий Балашов

- VoIP
- Проблемы безопасности в VoIP
- Yealink и Yeastar – решение проблем безопасностиVoIP

Voice Over Internet Protocol

- Быстрота установки и настройки
- Удобство использования (удержание, трансфер, конференция, интерком)
- Дополнительные сервисы (голосовая почта, запись разговоров, автосекретарь)
- Низкая стоимость коммуникаций

Voice Over Internet Protocol

По данным J’son & Partners, 2013 год

Существующие угрозы и проблемы безопасности VoIP-коммуникаций

Коммуникационные топологии

IP-телефоны - такие же сетевые устройства как и персональные компьютеры, поэтому обеспечение их безопасности является важным аспектом комплексной безопасности сети , особенно при использовании «облачных» решений.

Основные угрозы

Конфиденциальность личных данных

Прослушивание

Internet

Телефонное мошенничество

Преднамеренные атаки

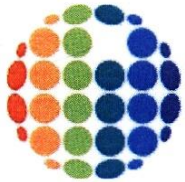
- Yealink и Yeastar – решение проблем безопасностиVoIP

Yealink

Yealink

EASY VoIP

- Компания основана в 2001 году
- 100% фокус на VoIP
- Профессиональная команда разработчиков
- Ведущие сотрудники имеют более 15 лет опыта в отрасли
- Продается в России с 2008 года (официальный дистрибьютор)



IPMATIKA

Yealink

EASY VoIP

Входит в 3-ку крупнейших производителей IP-телефонов в мире

По данным Frost & Sullivan 2013 год

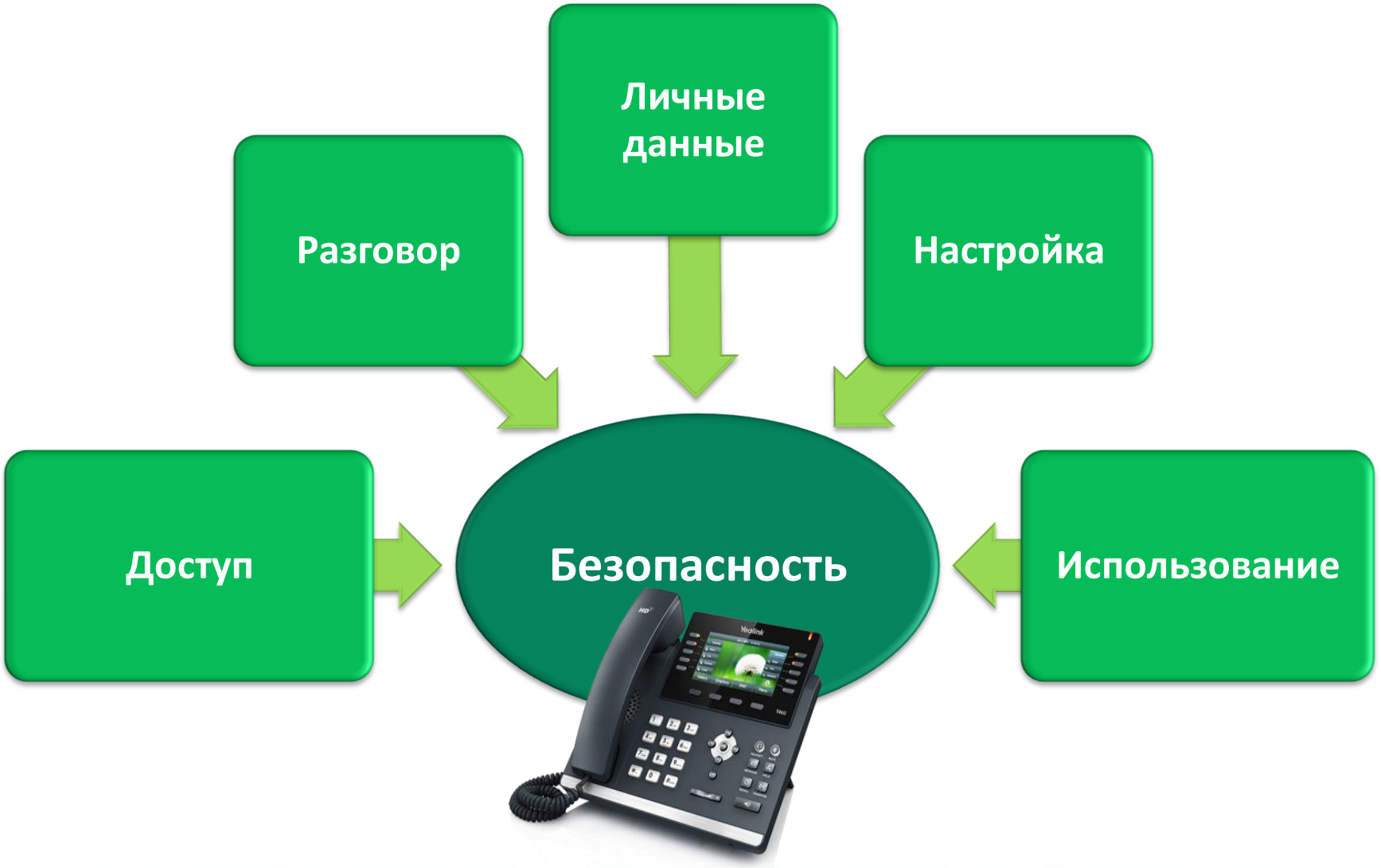
IPMATIKA

Yeastar

- Компания основана в 2006 году
- 100% фокус на VoIP
- Профессиональная команда разработчиков
- Более 50% сотрудников квалифицированные инженеры
- Продается в России с 2008 года (официальный дистрибьютор)

Сертифицировано лабораторией информационной безопасности IXI

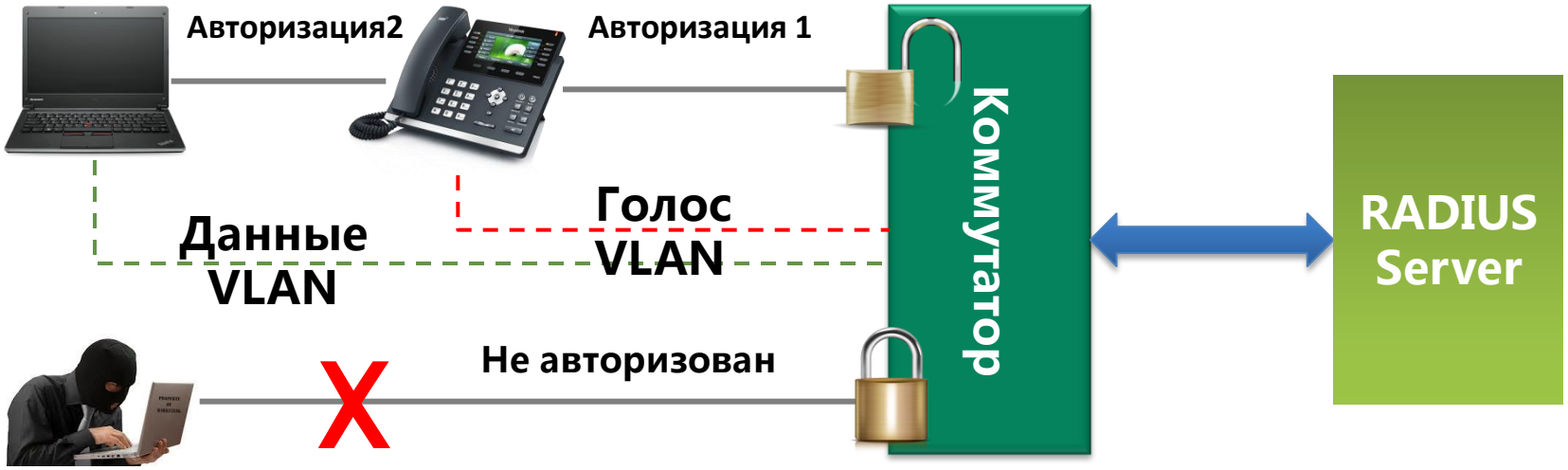
Обзор решений



- **Доступ к сети**

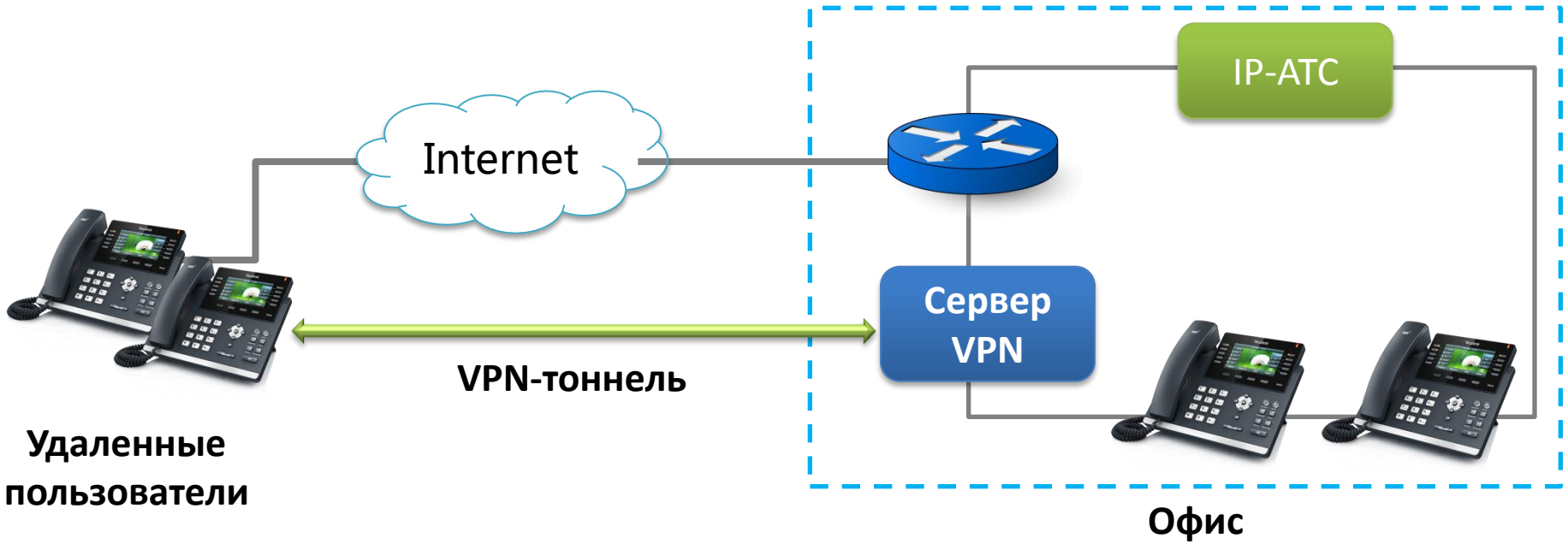
802.1X/EAP для защиты локальной сети

Проблема	• Неизвестный злоумышленник может подключиться к сети компании через PC-порт телефона, находящегося в приемной и скопировать конфиденциальные данные.
Решение	• Стандарт 802.1X ограничивает права неавторизованных компьютеров. • Методы EAP аутентификации: MD5, TLS. • Multi-Domain Authentication (MDA).



VPN для удаленных пользователей

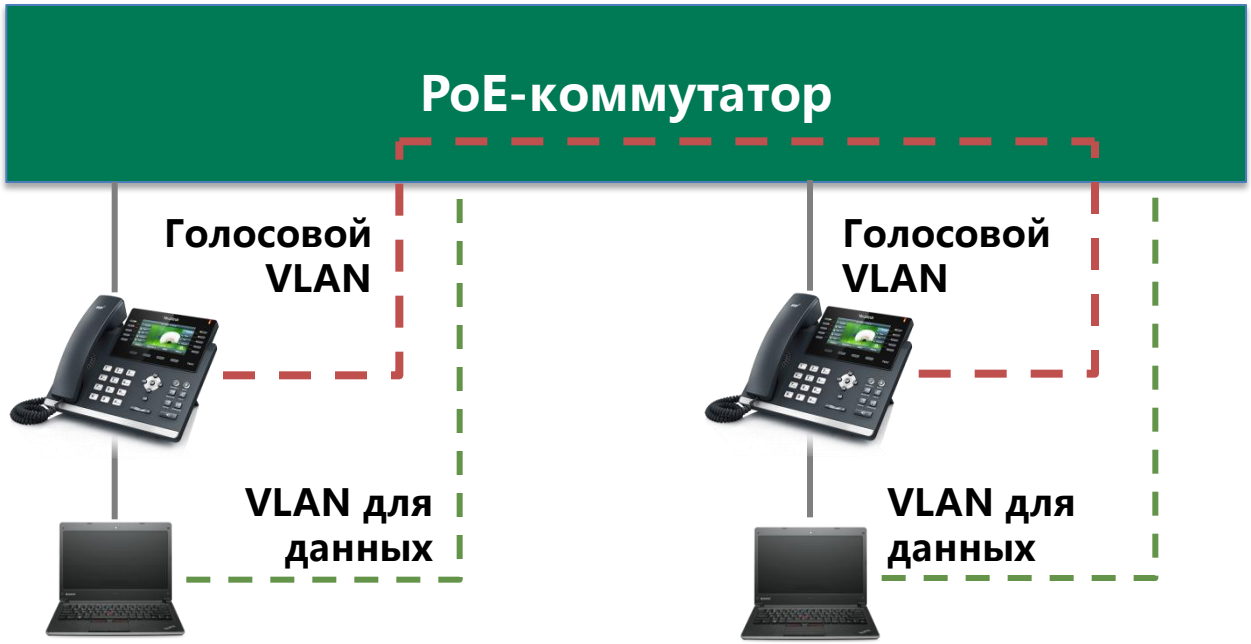
Проблема	• Проблемы безопасности при подключении удаленного пользователя к головному офису. • Приобретение роутеров с поддержкой VPN для удаленных пользователей.
Решение	• Встроенный в телефон OpenVPN-клиент. • Удаленные пользователи могут с высокой степенью защиты регистрировать IP-телефоны на офисной IP-АТС.



- **Разговор**

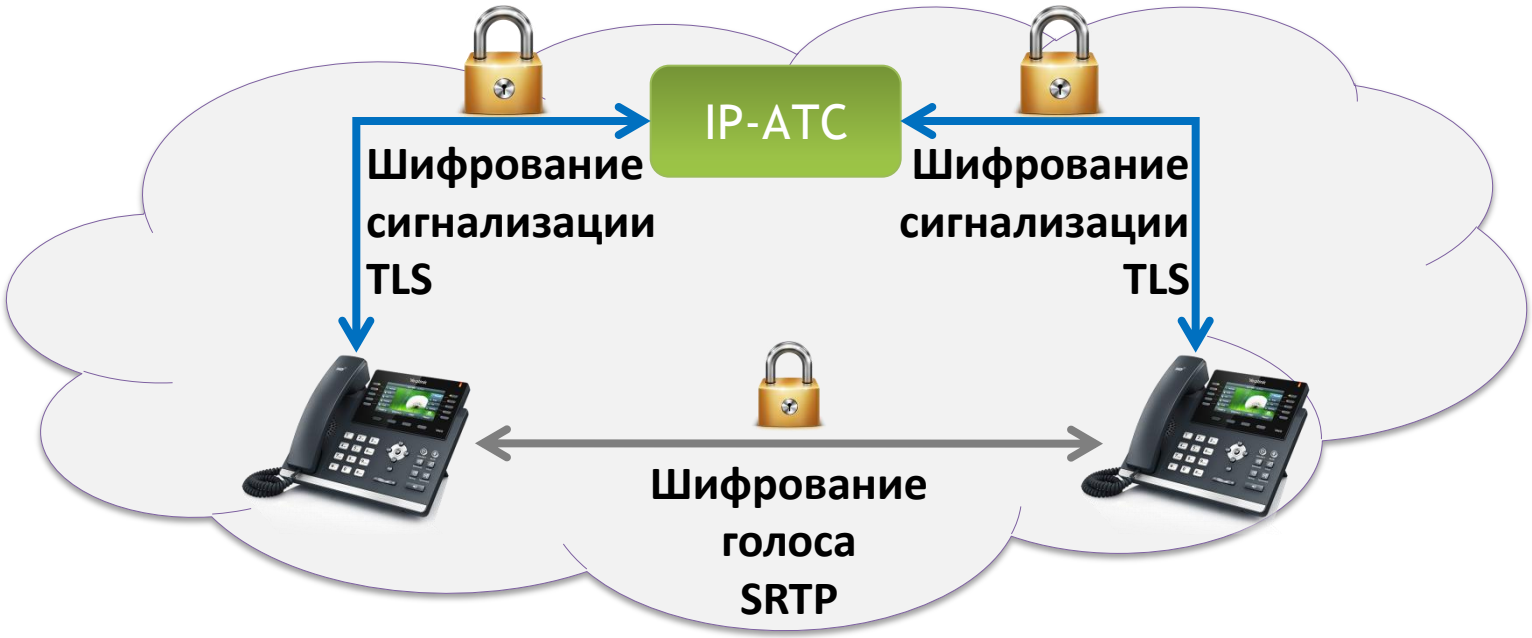
VLAN для качества связи

Проблема	• Качество передачи голоса – главное преимущество использования IP-телефона локальной сети компании.
Решение	• Ручная и автоматическая (с помощи LLDP или DHCP) настройка VLAN ID. • Использование VLAN гарантирует полосу пропускания для голоса. • Предотвращение сетевых коллизий. • Настройка защиты для IP-телефонов.



TLS и SRTP— шифрование сигнализации и голоса

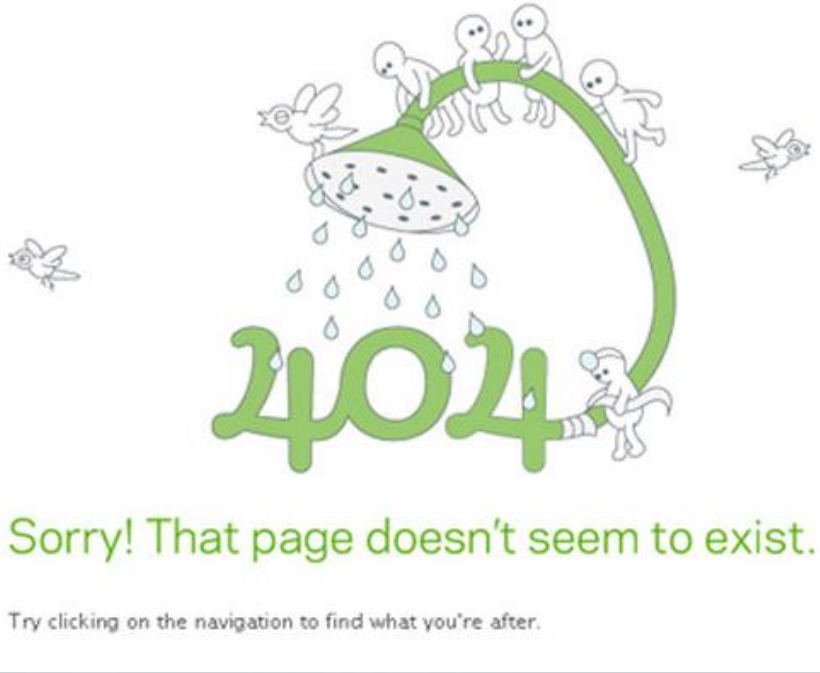
Проблема	• При звонке друг другу, SIP ID и телефонные номера обоих абонентов могут быть перехвачены злоумышленником. • Разговоры сотрудников прослушиваются злоумышленниками
Решение	• Авторизация вызывающего и вызываемого абонентов. • Использование криптографического протокола TLS для шифрования SIP-сообщений. • Использование 128-битного алгоритма AES для шифрования медиа-потока



- **Личные данные**

Блокировка телефона

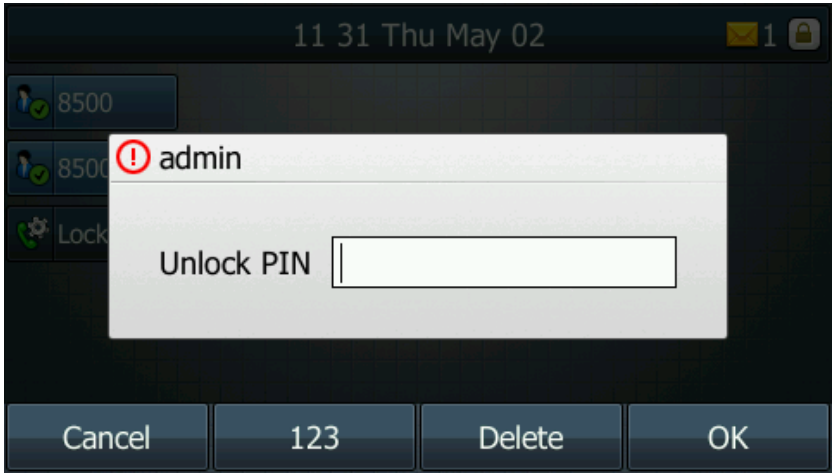
Проблема	• Необходимо защитить телефон, расположенный на публичном IP-адресе. Защитить пароли SIP-аккаунтов, хранимые телефоном.
Решение	• Использование механизма MD5 для шифрования паролей от SIP-аккаунтов пользователя, хранимых IP-телефоном Yealink. • Разграничение прав доступа к данным при подключении к SIP-телефону по Telnet. • Пользователь самостоятельно включает доступ по Telnet. • Возможность отключения доступа к SIP-телефону по WEB.



Блокировка телефона

Проблема	• Необходимо защитить персональные аккаунты, историю вызовов, контакты и настройки офисных пользователей.
Решение	• Пользователь может заблокировать свой IP-телефон и предотвратить доступ к личным данным. • Три режима блокировки: Все кнопки/Кнопки меню/Программируемые кнопки • Режимы срабатывания: Автоматическая или ручная блокировка • PIN может содержать до 15 символов • Экстренные номера всегда доступны для набора.

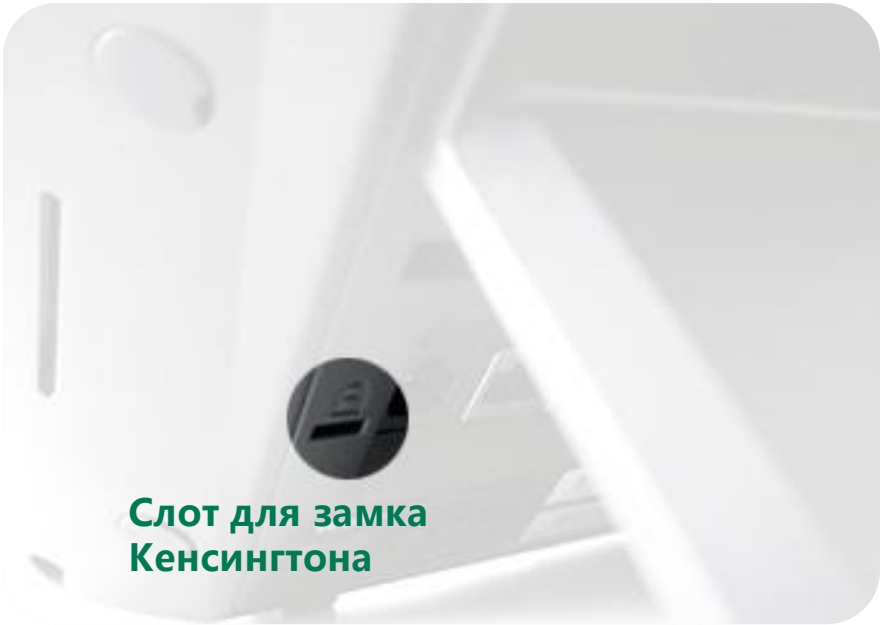
- **Блокировка**



- **PIN для разблокировки**

Замок Кенсингтона

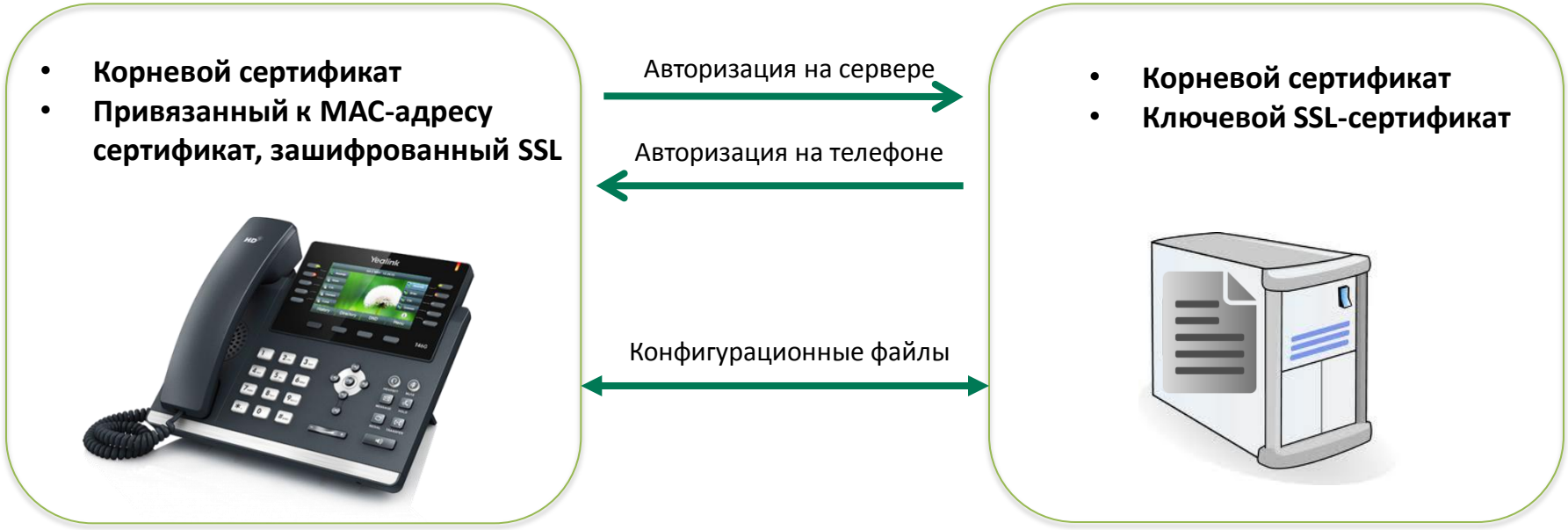
- **Физическое закрепление телефона для предотвращения кражи, например из холла с большим числом посетителей.**



- **Настройка**

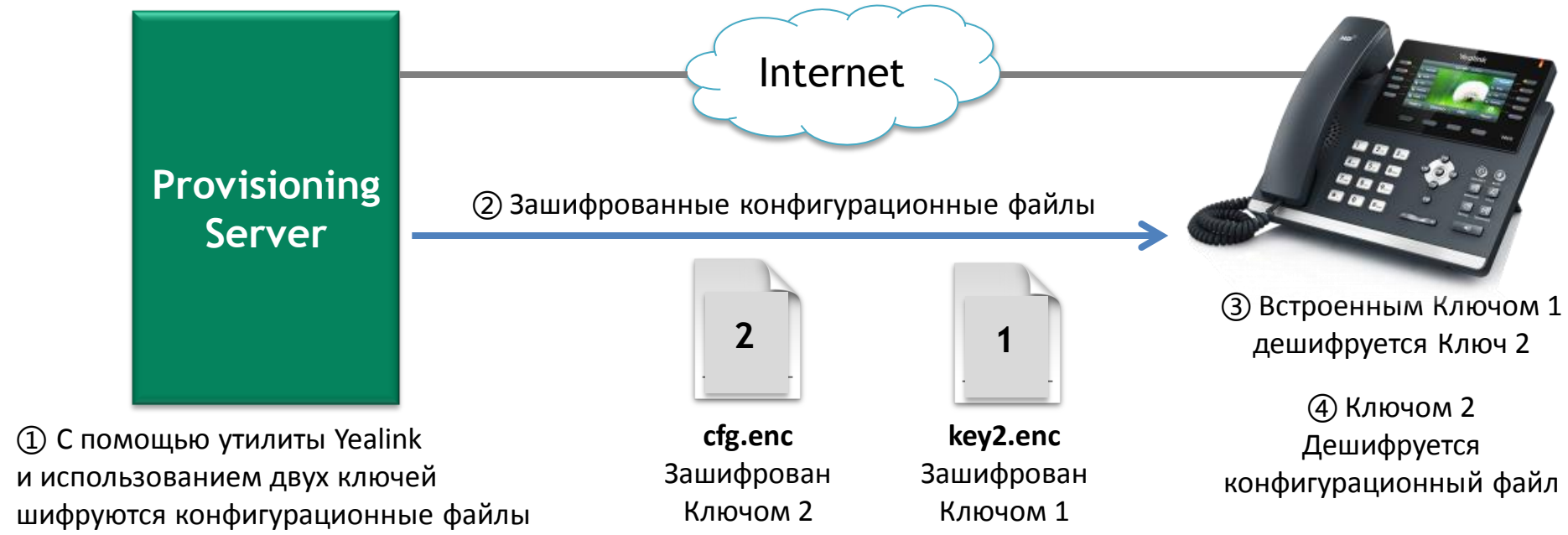
HTTPS Provisioning

Проблема	• Требуется защитить файлы конфигурации, которые IP-телефон получает при AutoProvision.
Решение	• Обоюдная авторизация устройств по TLS при обновлении конфигурации. • Заводской сертификат, привязанный к MAC-адресу. • Заводской список основных корневых сертификатов. • Загрузки персональных корневых сертификатов с SSL шифрованием



Шифрование конфигурационных файлов

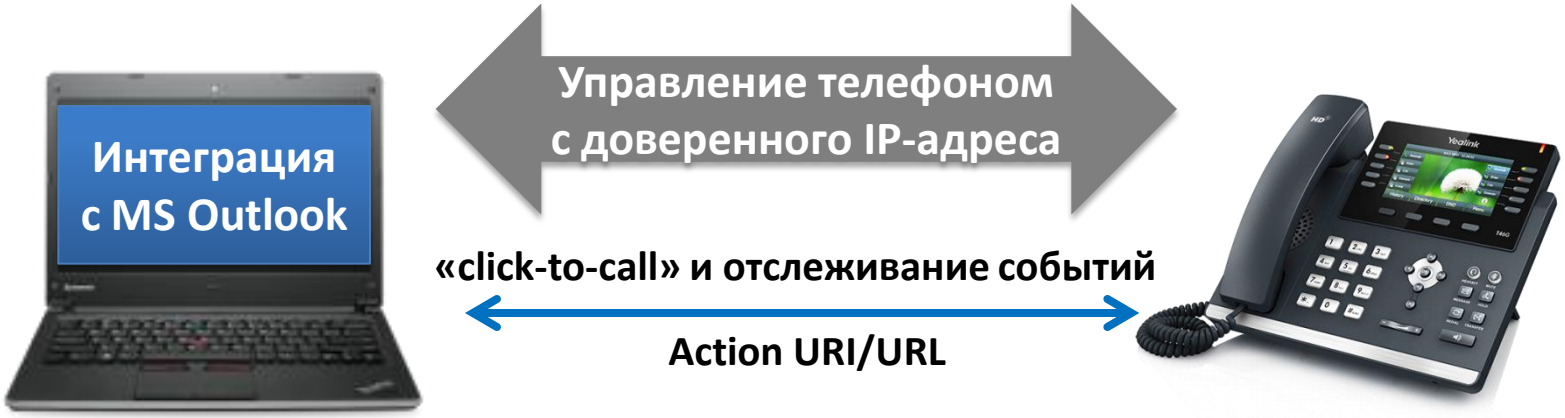
Проблема	• Администраторы небольших компаний не обладают знаниями о TLS/SSL. Требуется несложный механизм шифрования конфигурационных файлов.
Решение	• Шифрование конфигурационных файлов. • Утилита для шифрования со встроенным AES-ключом. • В телефоне встроен уникальный AES-ключ.



- **Использование**

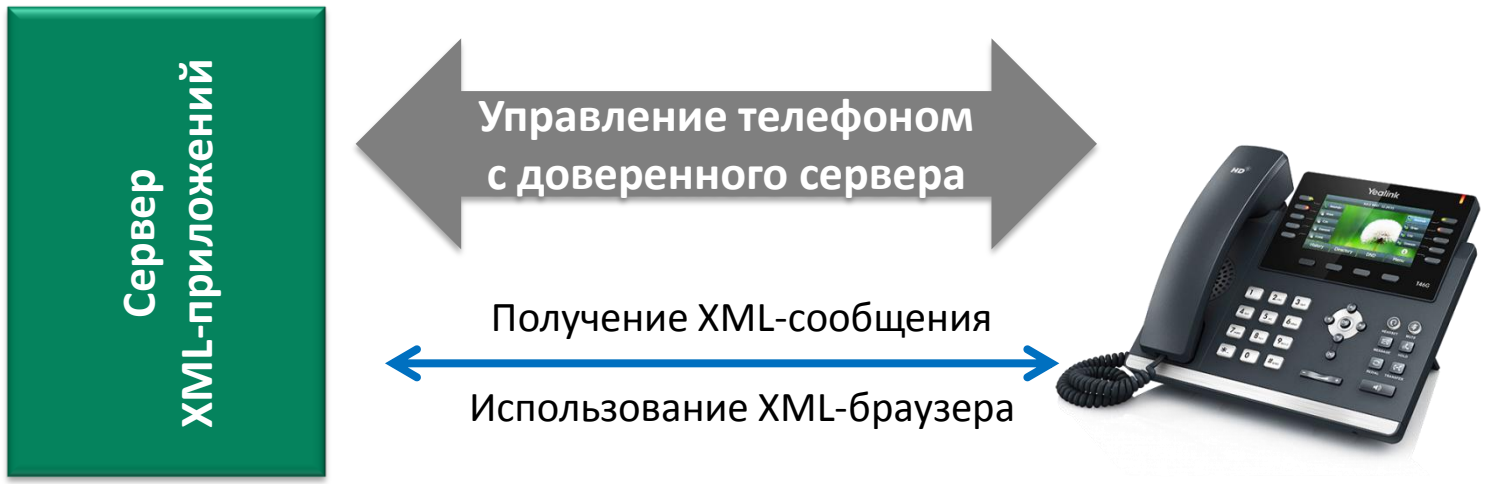
Доверенный IP для взаимодействия с ПК

Проблема	• Телефоны Yealink могут быть интегрированы с компьютерными приложениями, позволяющими выполнять управление телефоном с ПК. Злоумышленник может воспользоваться данной функцией.
Решение	• Только доверенные ПК могут взаимодействовать телефоном. • Список IP-адресов для использования функций Action URI/URL. • Пользователь сам предоставляет доступ к телефону.



Доверенный сервер XML-приложений

Проблема	• Телефоны Yealink имеют встроенный XML-браузер. Данную возможностью может воспользоваться злоумышленник.
Решение	• Только доверенный сервер может управлять телефоном через XML-браузер. • Список доверенных серверов для получения XML-сообщений. • Пользователь сам предоставляет доступ к телефону



Уровни безопасности

Уровень приложений	HTTPS web; CTI Trusted IP; HTTPS Provision; Config Files Encryption
Транспортный уровень	SRTP; TLS; Digest Authentication
Сетевой уровень	Disabling Ping
Уровень доступа к сети	802.1x; VLAN; VPN; Disabling PC Port

Спасибо за внимание! ☺

Дмитрий Балашов
ООО «АйПиМатика»
Москва, ул. Свободы д.1 корп.6
Тел: +7 (495) 921 36 70
Skype: ipmatika_dmitriy
Email: balashov@ipmatika.ru