

## Анализ проблем обеспечения безопасности соединений в сетях IP-телефонии

Выполнила: Рыжкова А.А.

Студентка группы ССК-41КО

Специальность 11.02.11 Сети связи и  
системы коммутации

Руководитель: Сулейманян Е.А.

# Актуальность темы

Перспективы использования услуг IP-телефонии. Чтобы оставаться конкурентоспособными, провайдеры IP-телефонии должны учитывать потребности пользователей, а именно качество связи и безопасность соединений.

**Объектом исследования** анализ проблемы обеспечения безопасности соединений в сетях IP-телефонии.

**Предметом исследования:** особенности проблем обеспечения безопасности в сетях IP-телефонии.

**Цель исследования:** анализ рисков сети IP-телефонии с точки зрения проблем обеспечения безопасности соединений и поиск возможных способов их устранить.

# Задачи:

- возможности протоколов IP-телефонии, направленных на обеспечение безопасности соединений;
- выбор оптимального протокола аутентификации, авторизации и учета;
- слабые места процессов аутентификации, авторизации и учета в рамках обеспечения безопасного доступа к ресурсам сети.
- смоделировать ситуацию, попадающую под категорию атак на сеть IP-телефонии, предложить механизмы ее разрешения;
- технология защиты от фродовых атак в IP-телефонии на примере алгоритма, принятого в ПАО "Вымпелком"

# Новизна

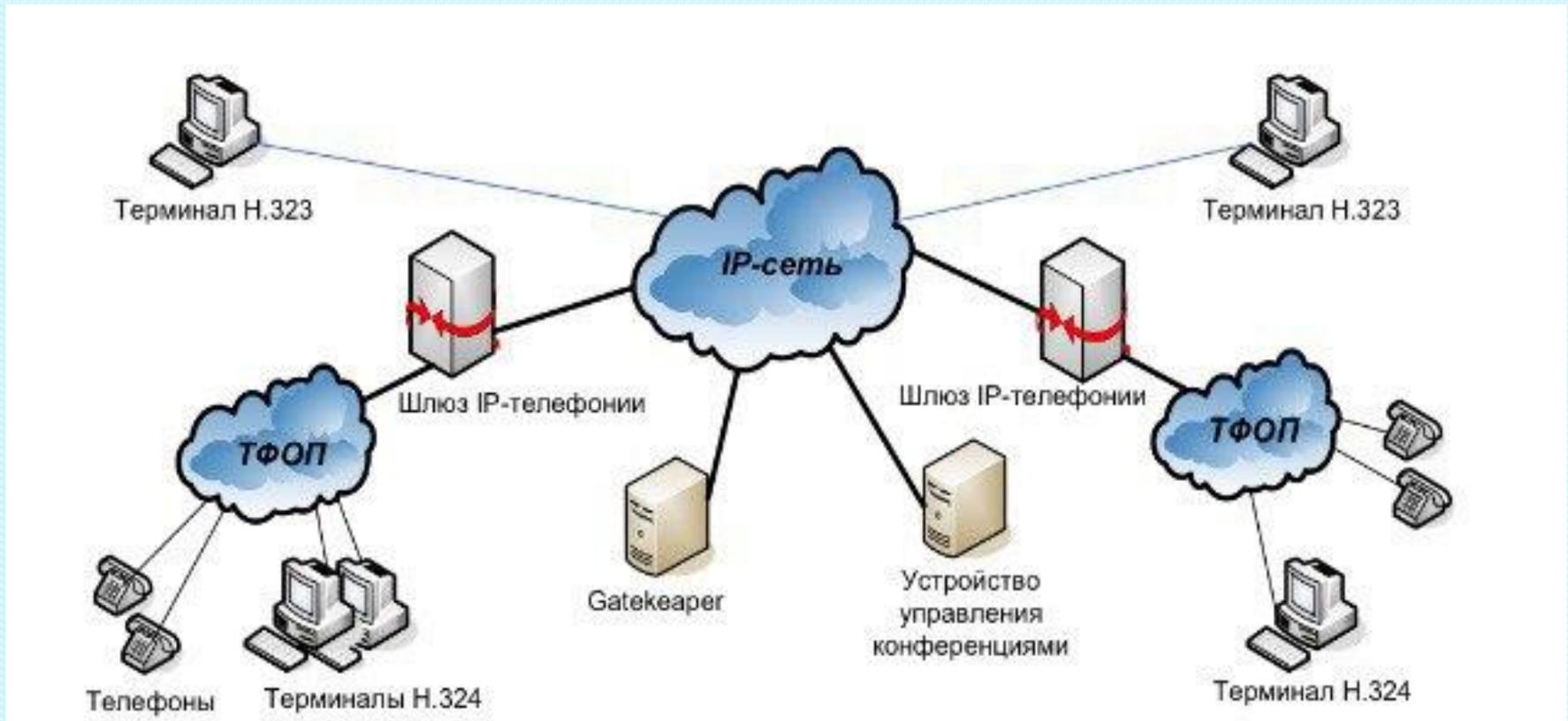
теоретическое обобщение, статей и учебных пособий по цифровой связи в целом и цифровой обработке сигналов в частности, технологии их реализации в мультисервисных сетях

# IP-телефония-

технология передачи голоса по компьютерной сети.



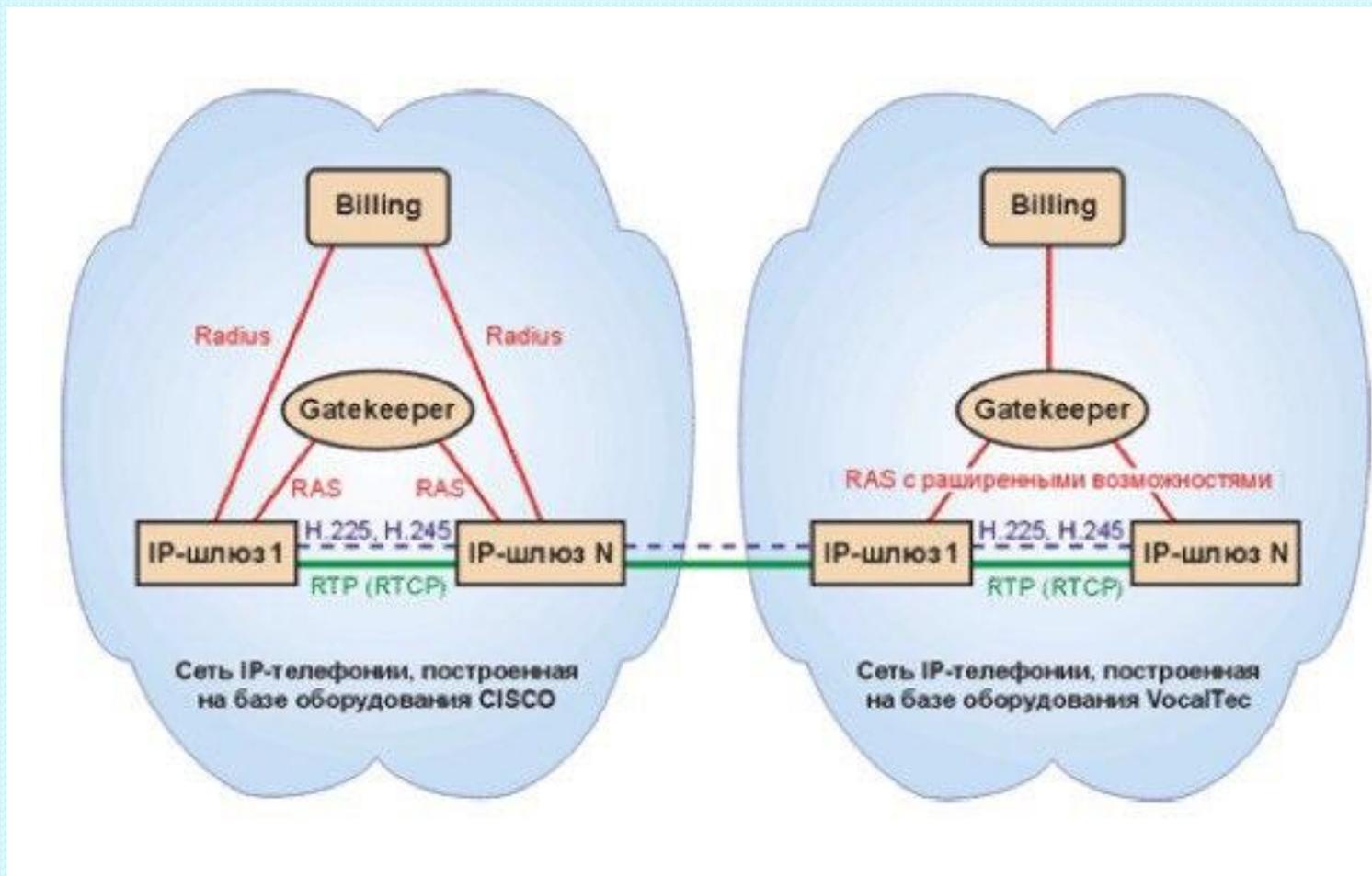
# Архитектура сети, базирующейся на протоколе H.323



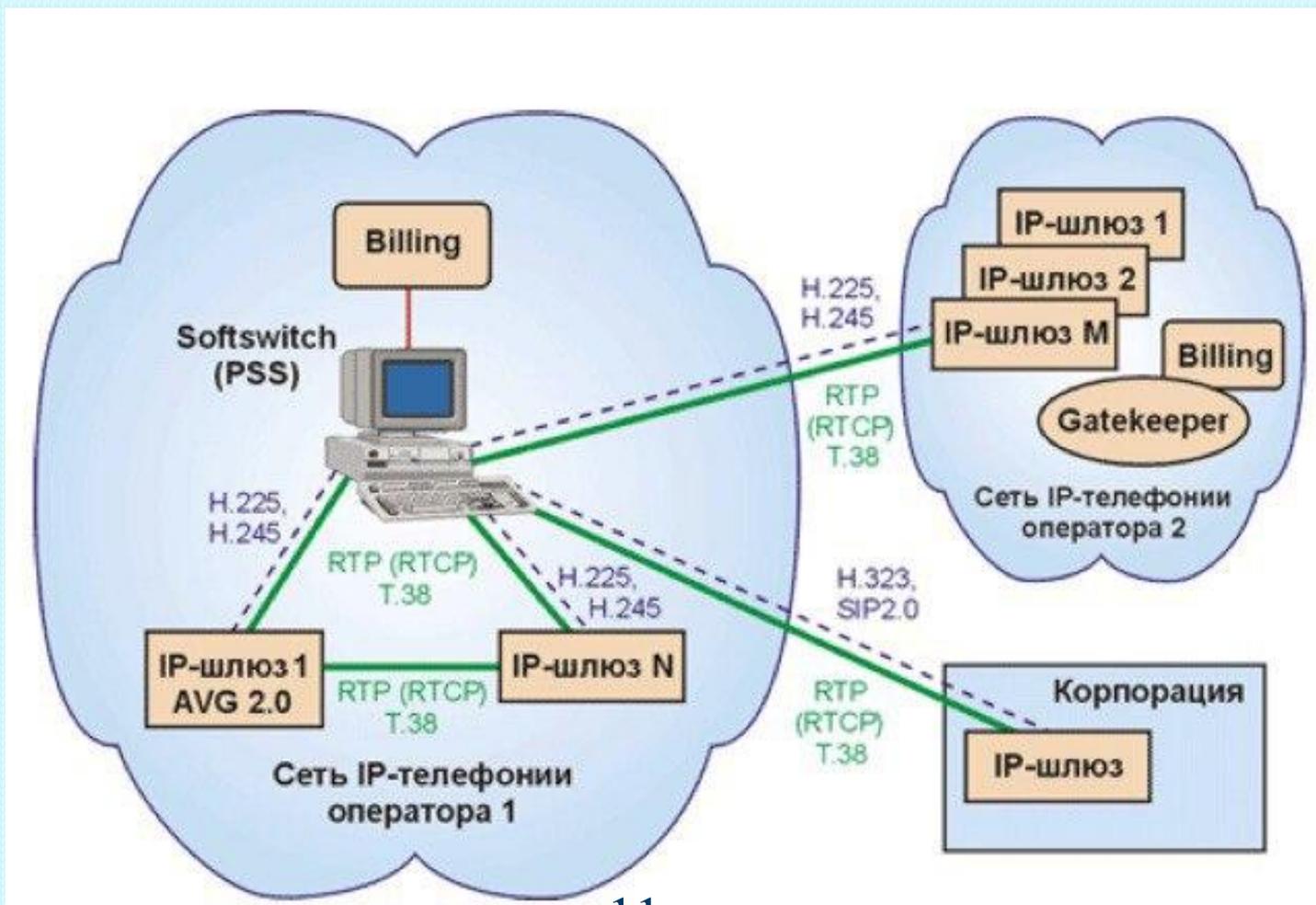
# Атаки на сеть IP-телефонии и механизмы борьбы с ними

1. Отказ в обслуживании
2. Подмена номера
3. Перехват данных

# Модель возведения и взаимодействия сети IP-телефонии без использования программного коммутатора



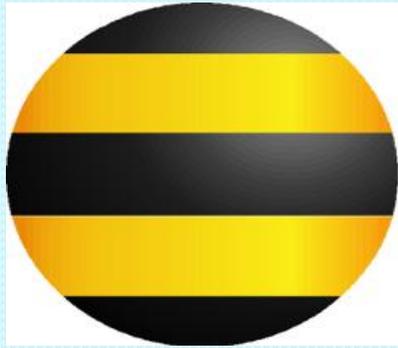
# Модель возведения и взаимодействия сети IP-телефонии с использованием программного коммутатора



# Ключевые функции безопасности IP-телефонии:

- аутентификация
- целостных данных
- секретность
- проверка отсутствия долгов

# Технология блокировки фрода на примере компании ПАО «Вымпелком»



# VimpelCom

*Фрод* - вид атак, в частном случае предполагающий многократное совершение международных дорогостоящих вызовов с использованием адресной информации пострадавшего лица.

*ТТ (Trouble Ticket)* - абонентская (или партнёрская) заявка на обнаружение проблемы в сети, зарегистрированная в специальной системе по работе внутри технических отделов компании.

# Краткий алгоритм анализа фродовых Trouble Ticket:

- принять от клиента или зафиксировать всплеск трафика на международные направления;
- проанализировать, является ли этот трафик фродовым;
- в случае подозрения передать заявку в работу дежурному смены опорных коммутаторов;
- выполнить блокировку международной связи клиенту.

# Алгоритм блокировки мн-связи VoIP-клиентам компании ПАО «Вымпелком»

- Для блокировки фрода у всех сотрудников имеется доступ к специальному программному обеспечению
- Алгоритм блокировки идентичен независимо от имеющегося оборудования
- Ручная блокировка имеет важное преимущество перед автоматической: сотрудник анализирует трафик на предмет его легитимности. Таким образом, исключена возможность ошибки

# Алгоритм блокировки мн-связи VoIP-клиентам компании ПАО «Вымпелком»

**Билайн**

Operator Routing | Mera | Sipmaster | Asterisk | Support

ВИЛАЙН  
ВЫМПЕЛКОМ  
СОВИНТЕЛ

Support - Вопросы и ответы

Стр. 1 2 3 4 5 6 7 8 9

65. login: **majorov** e-mail: mayorov\_aa@gldn.net date: 28.09.2010 13:04:33

Возвращаюсь к теме TRANSFER, пробовал разные варианты (отсылал айпи где не слушает sip сервер, подставлял даже опят сервера с которого делался TRANSFER) в любом случае cisco никогда не закидывала вызов. После сообщения SIP/2.0 302 Moved cisco присылает ACK и все, больше вызов на изначальный айпи, указанный в дайл-пире не шлется.

66. login: **bazil** e-mail: vnsuvorov@beeline.ru date: 07.10.2010 16:07:17

Добавления и исправления в Asterisk:

По долгожданному указанию руководства снят запрет на управление переадресацией номеров (клиентским звонком \*72, \*каналов с косыми АДН-ами (В-номер не равен А-номер).

67. login: **bazil** e-mail: vnsuvorov@beeline.ru date: 10.07.2011 11:46:46

# Алгоритм блокировки МН-связи VoIP-клиентам компании ПАО «Вымпелком»

Operator Routing    Мера    Sipmaster    Asterisk    Support

Схема: **meravoip**

- ГРУППЫ
- НАПРАВЛЕНИЯ
- ШЛЮЗЫ
- МАРШРУТЫ
- ЗАГРУЗКА
- СТАТИСТИКА
- ЖУРНАЛ
- CDR-ЗАПИСИ
- ПОМОЩНИК

### Meravoip MVTS - Установка Маршрутов

✓ Группа:     ✓ Направление:     Поиск:     Ok

	Направление	Шаблон	Группа	Шлюз	Приоритет	Проч
<input type="checkbox"/>	0X	0.	CLASS_B	MOSCOW1 MOSCOW3	65535	dst_translate=0/96
<input type="checkbox"/>	100	100	CLASS_B	MOSCOW1 MOSCOW3	65535	dst_translate=100/96
<input checked="" type="checkbox"/>	3APERSONAL1	67082256292 67082256293	ALL	3APERSONAL1	65535	
<input checked="" type="checkbox"/>	3APERSONAL2	67082256291 67082230219	ALL	3APERSONAL2	65535	
<input checked="" type="checkbox"/>	3SEILSPUS		ALL	3SEILSPUS 3SEILSPUS-3	65535	
<input checked="" type="checkbox"/>	3SEILSPUS-2	67086600259	ALL	3SEILSPUS-2	65535	
<input checked="" type="checkbox"/>	3SEILSPUS-3		ALL	3SEILSPUS-3	65535	
<input checked="" type="checkbox"/>	A-TRANCE	67087399719	ALL	A-TRANCE	65535	
<input checked="" type="checkbox"/>	AAI-REITING	67087413954	ALL	AAI-REITING	65535	
<input checked="" type="checkbox"/>	AAS	67086600493	ALL	AAS	65535	
<input type="checkbox"/>	AB-SRETENKA	67087308880	ALL	AB-SRETENKA	65535	
<input checked="" type="checkbox"/>	ABBEU	67082256205	ALL	ABBEU	65535	

Готово

# Алгоритм блокировки мн-связи VoIP-клиентам компании ПАО «Вымпелком»

✓ Канал:	<input type="text" value="4952580771"/>	✓ Номер (FW):	<input type="text" value="4952580771"/>
✓ АОН:	<input type="text" value="&lt;4952580771&gt;"/>	Пароль:	<input type="text" value="Rufeekae9u"/>
ACL IP:	<input type="text" value="10.163.102.195"/>	ACL mask:	<input type="text" value="255.255.255.255"/>
✓ Хост:	<input type="text" value="dynamic"/>	✓ Тип:	<input type="text" value="friend"/>
✓ Группа:	<input type="text" value="ANTALBANK"/>	✓ Контекст:	<input type="text" value="international"/>
Журнал:	<input type="button" value="Запись"/>	<input type="button" value="История"/>	<input type="button" value="CDR"/>
Опции:	<input type="checkbox"/> - No RTP <input type="checkbox"/> - NAT		
Прочее:	<pre>call-limit=2 username=4952580771 :fromuser=4952580771 fromdomain=b2b.corbina.net :IC 4743122, BQ 3371533 :Service was pulled out of operation by request IC:4952492. :Service was returned to operation by request IC:4953415.</pre>		
<input type="button" value="Обновить"/> <input type="button" value="Удалить"/> <input type="button" value="Новый"/> <input type="button" value="Отмена"/>			

## Выводы:

- Перехват данных, отказ в обслуживании, подмена номера – атаки, представляющие угрозу для обеспечения безопасности передачи данных. Их предотвращение является основной задачей для защиты функционирования сети.
- В настоящее время выработана рекомендация по обеспечению безопасности соединения в сетях IP-телефонии и представлен сценарий установления безопасного VoIP-соединения.
- Необходимо внедрение эффективных механизмов защиты соединений в сетях IP-телефонии для того, чтобы провайдер оставался конкурентоспособным на растущем рынке телекоммуникационных услуг.

## Выводы:

- Рассмотрен алгоритм выявления и предотвращения фрода с использованием АОН жертвы на примере работы соответствующих технических служб компании ПАО «Вымпелком», а именно, изучили способы ручной блокировки международной связи, если клиент подключен к оборудованию Mera.

**СПАСИБО ЗА ВНИМАНИЕ!**