Ярославский государственный университет им. П.Г.Демидова
Университетский колледж

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.

Ярославль 2017

Актуальность темы

Перспективы использования услуг IP-телефонии. Чтобы оставаться конкурентоспособными, провайдеры IP-телефонии должный 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"

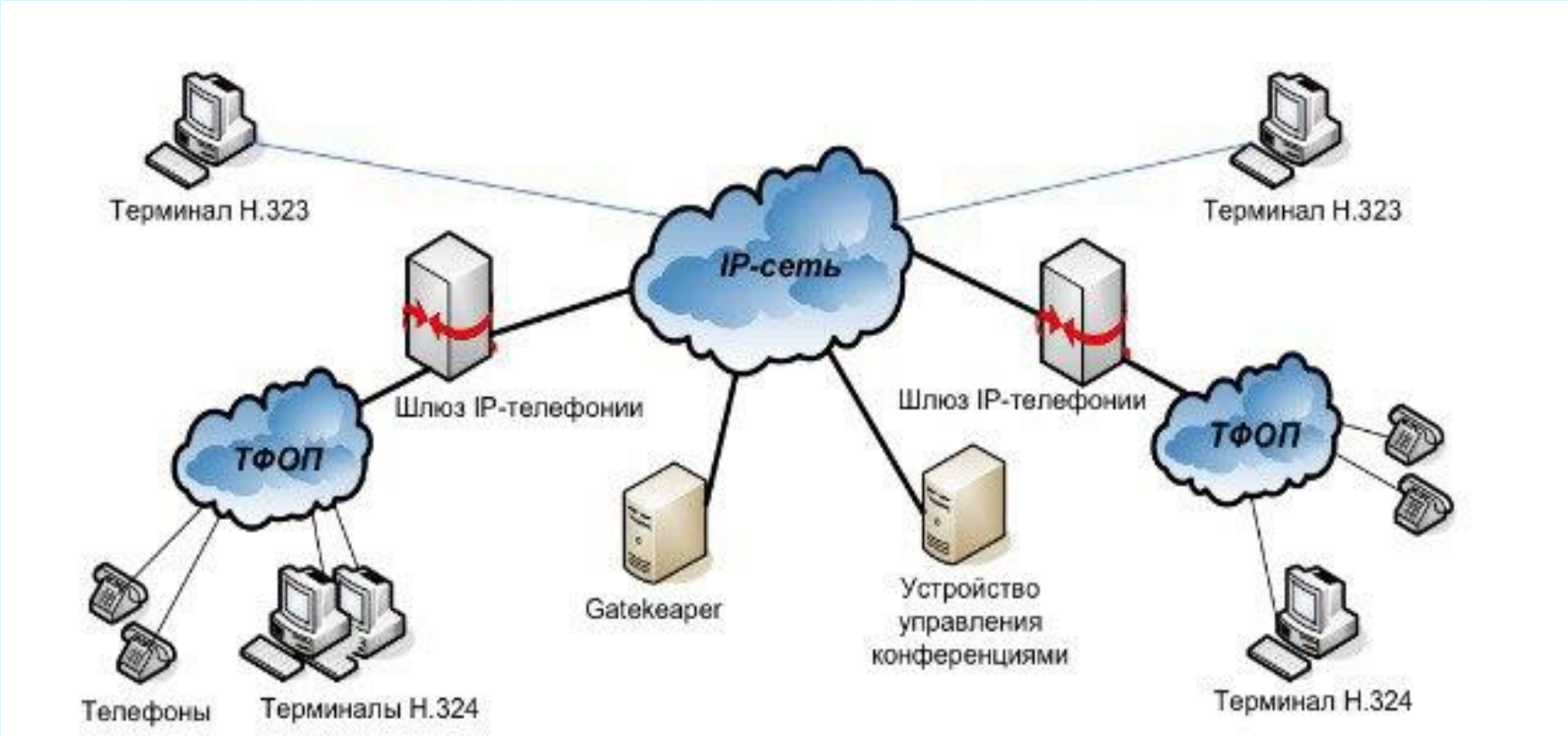
Новизна

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.

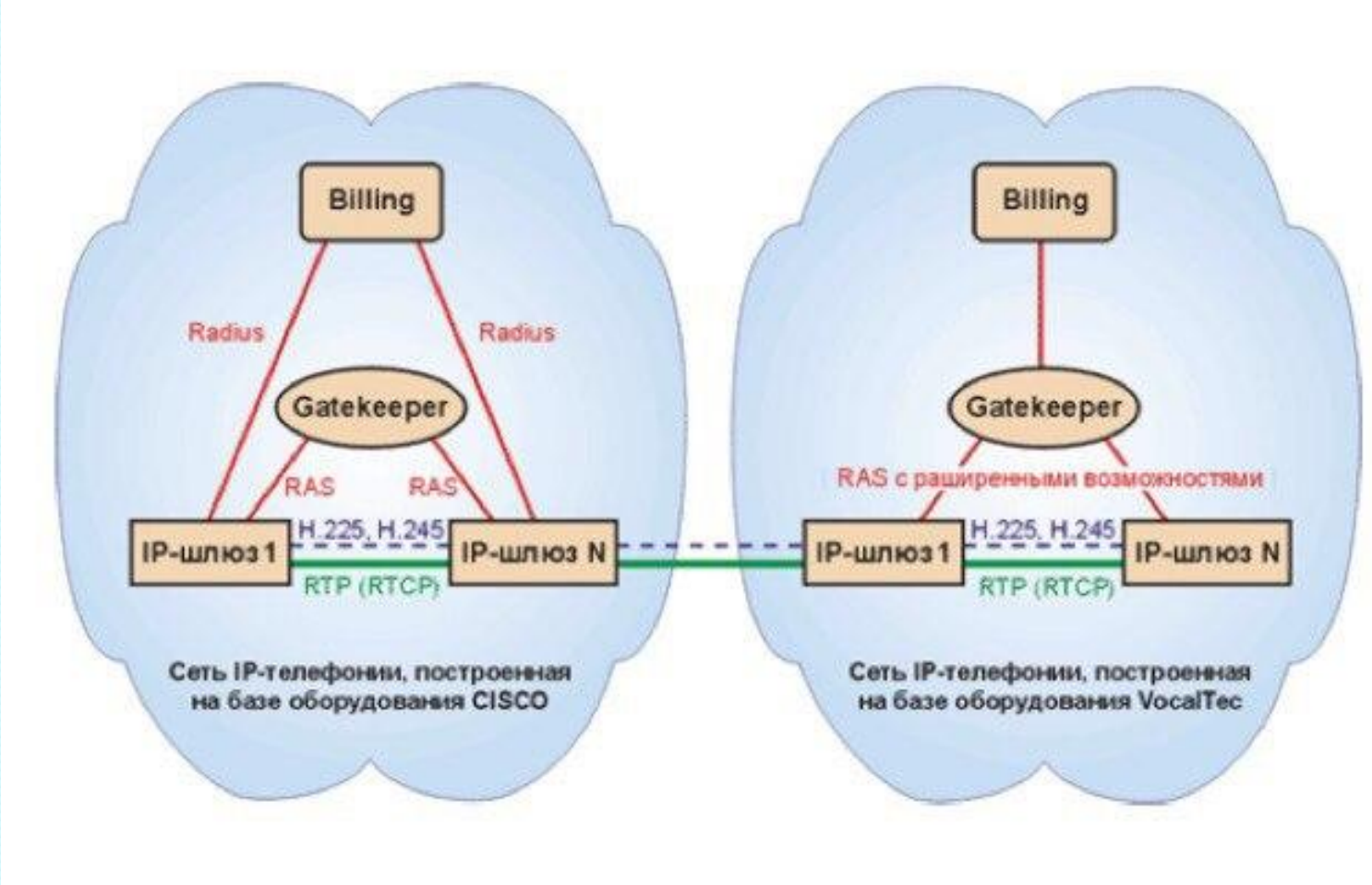
Архитектура сети, базирующейся на протоколе H.323



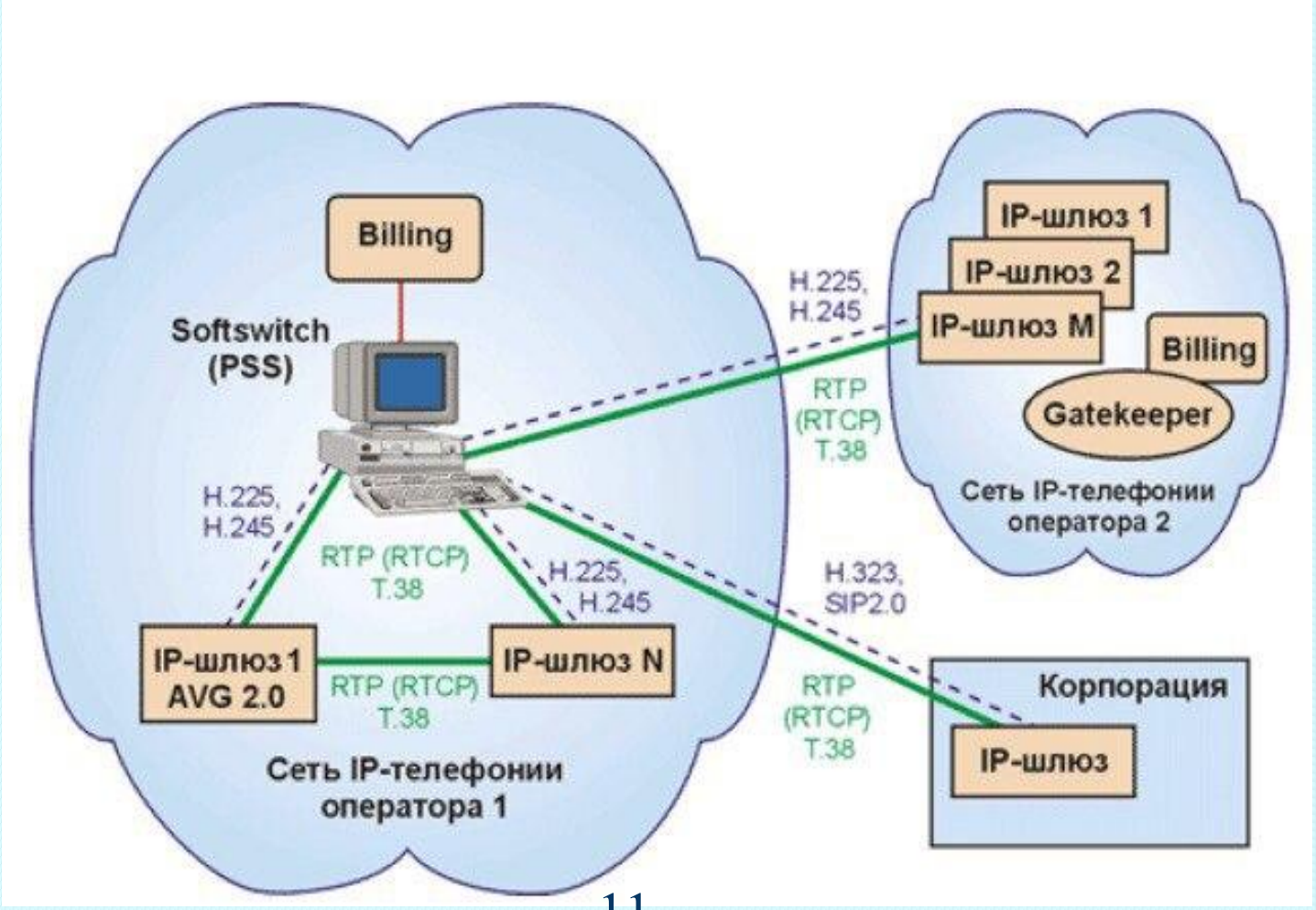
Атаки на сеть IP-телефонии и механизмы борьбы с ними

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»

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

TT (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:

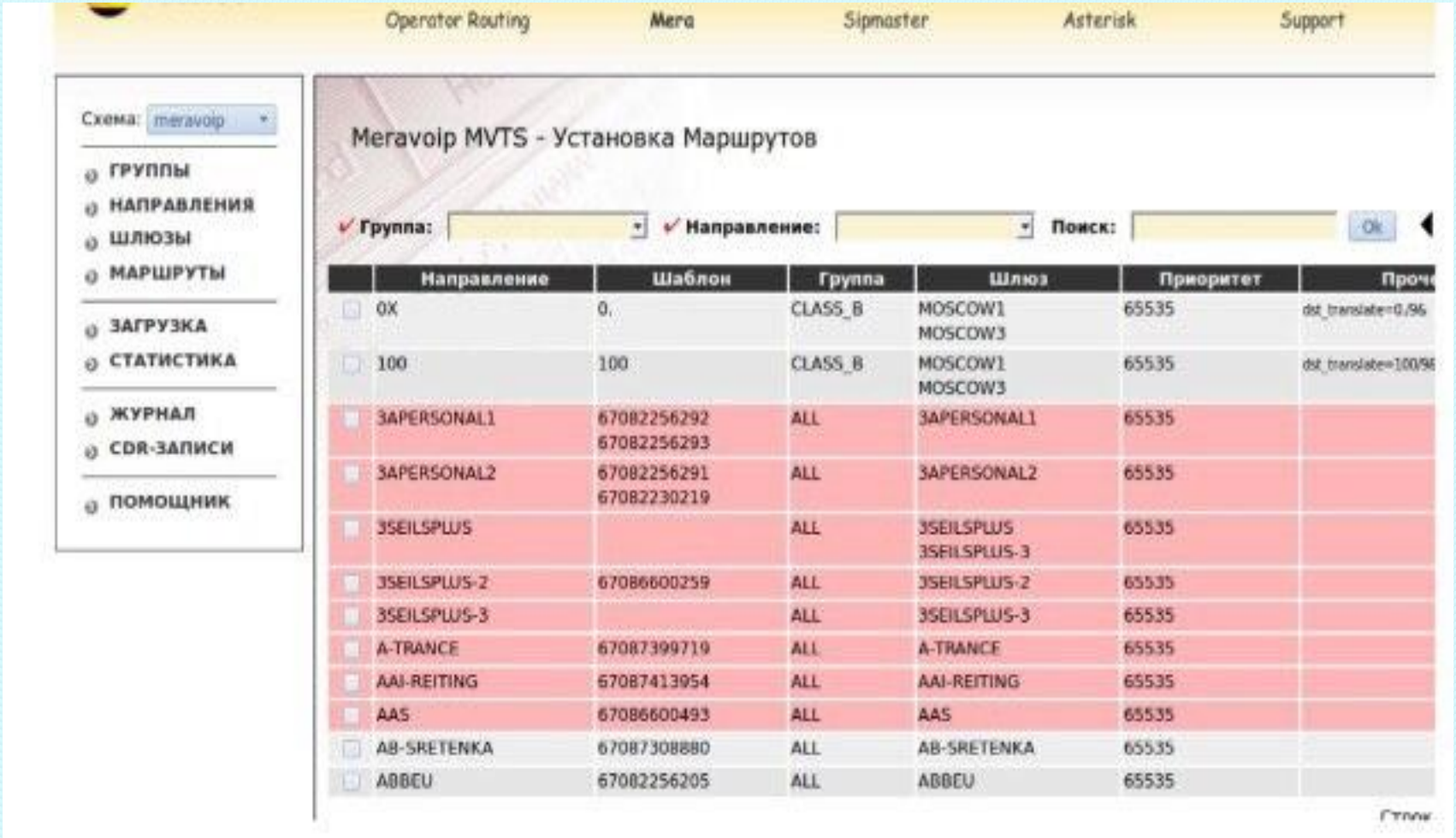
- принять от клиента или зафиксировать всплеск трафика на международные направления;
- проанализировать, является ли этот трафик фродовым;
- в случае подозрения передать заявку в работу дежурному смены опорных коммутаторов;
- выполнить блокировку международной связи клиенту.

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

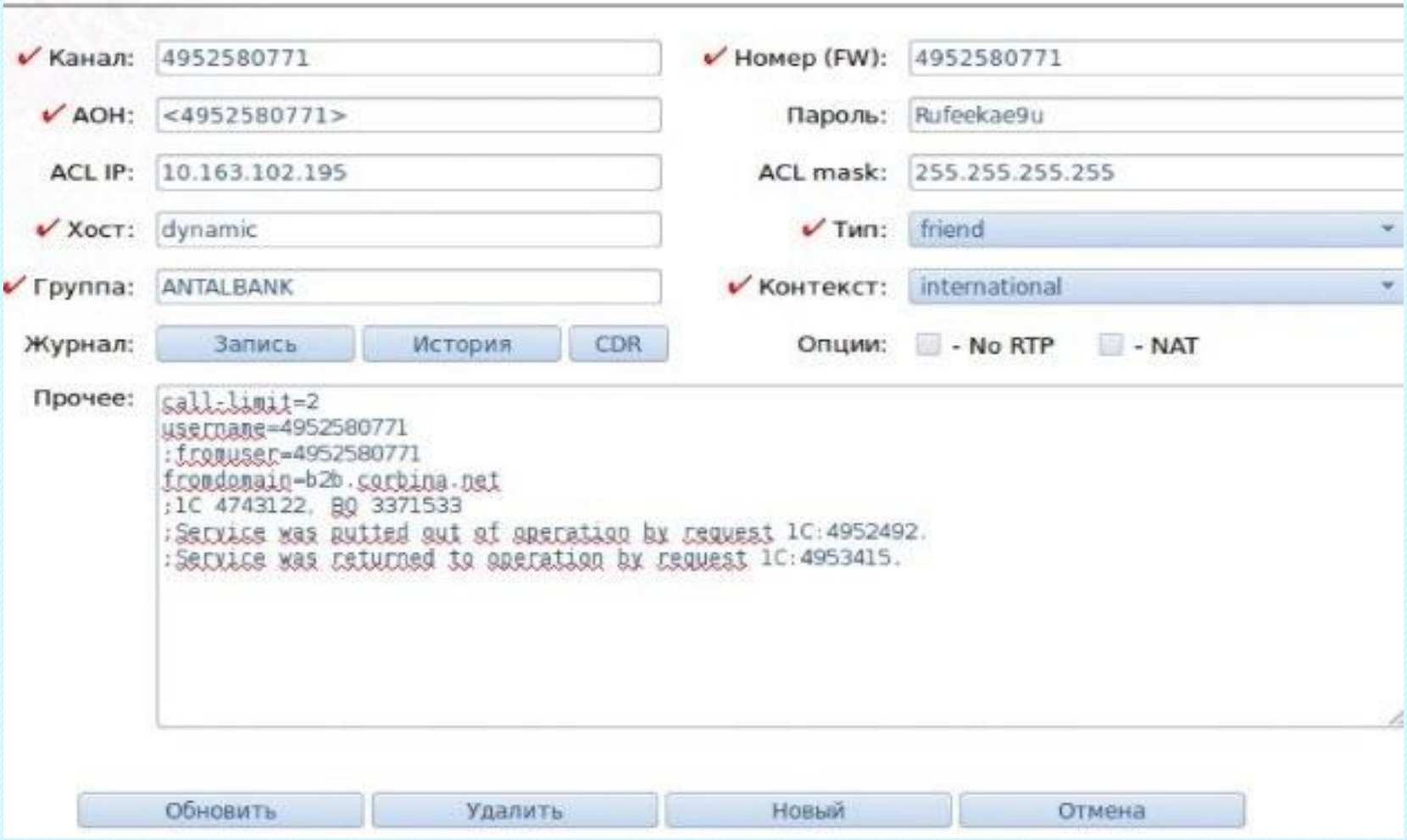
Алгоритм блокировки мн-связи VoIP-клиентам компании ПАО «Вымпелком»

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



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

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



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!