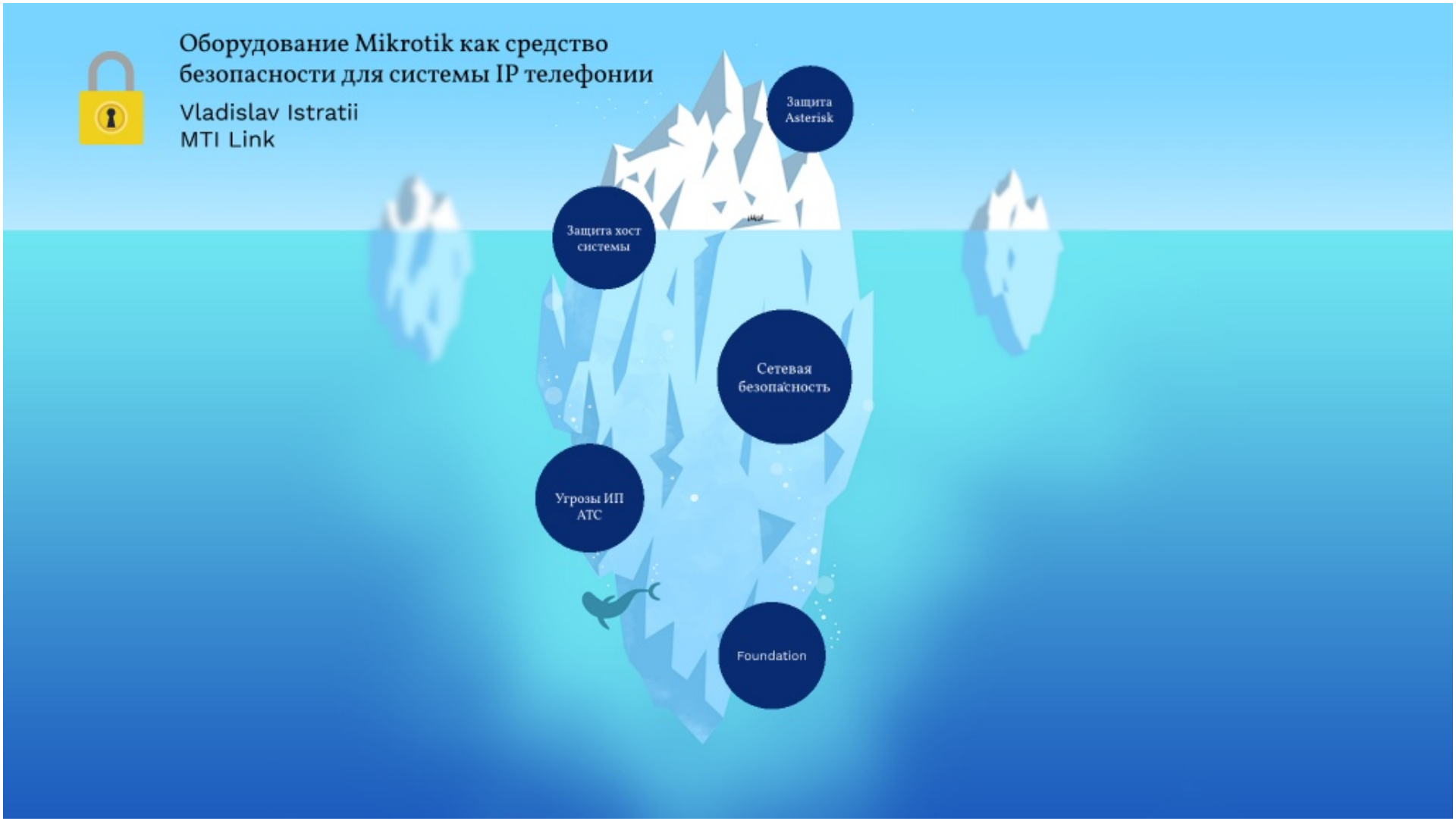
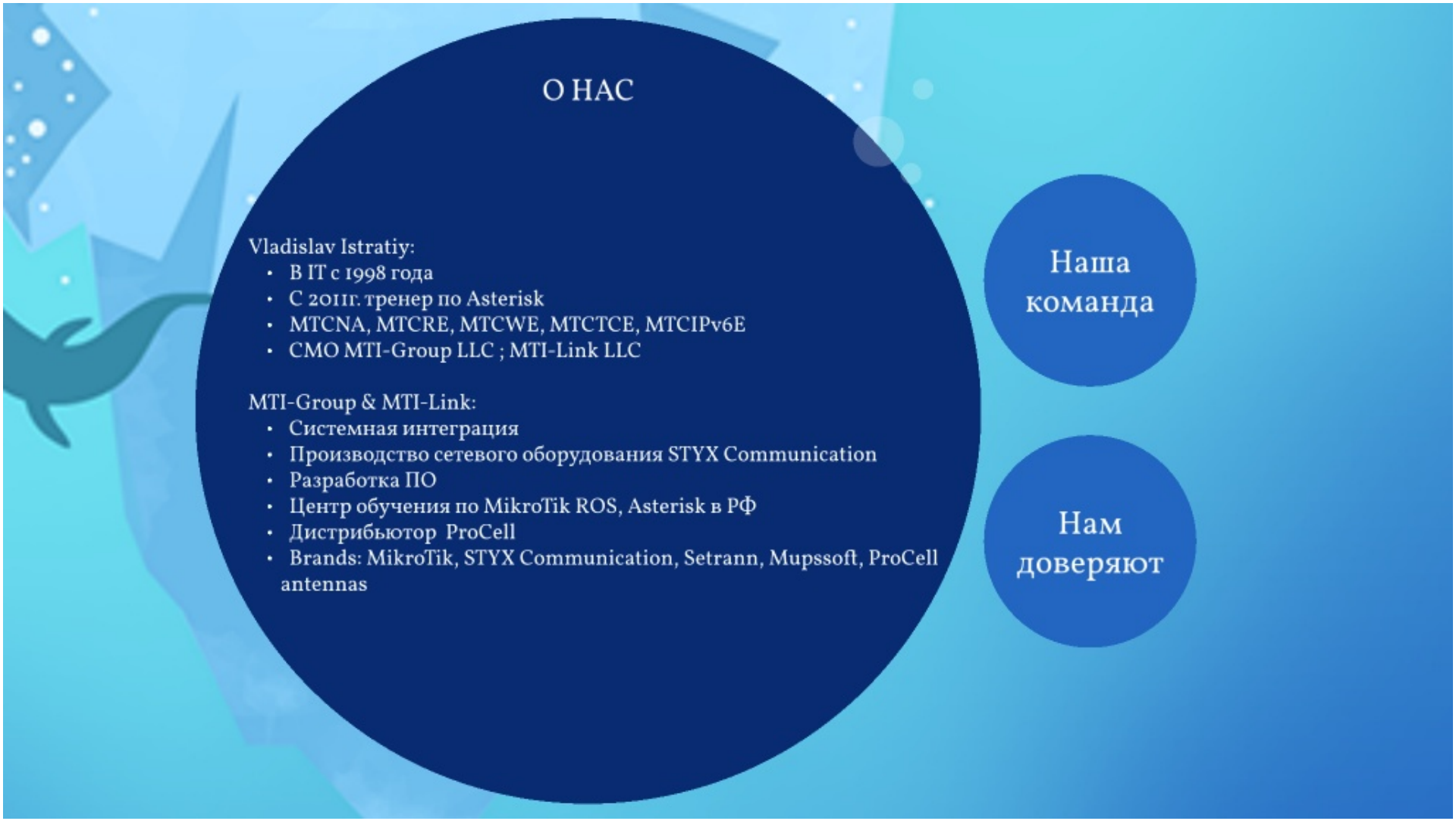

Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation


О НАС
Vladislav Istratiy:
• В IT с 1998 года
• С 2011г. тренер по Asterisk
• MTCNA, MTCRE, MTCWE, MTCTCE, MTCIPv6E
• CMO MTI-Group LLC ; MTI-Link LLC
MTI-Group & MTI-Link:
• Системная интеграция
• Производство сетевого оборудования STYX Communication
• Разработка ПО
• Центр обучения по MikroTik ROS, Asterisk в РФ
• Дистрибьютор ProCell
• Brands: MikroTik, STYX Communication, Setrann, Mupssoft, ProCell antennas
Наша команда
Нам доверяют

Наша команда

Руководящий состав

Irina Tsyapa
CEO "MTI Group" LLC

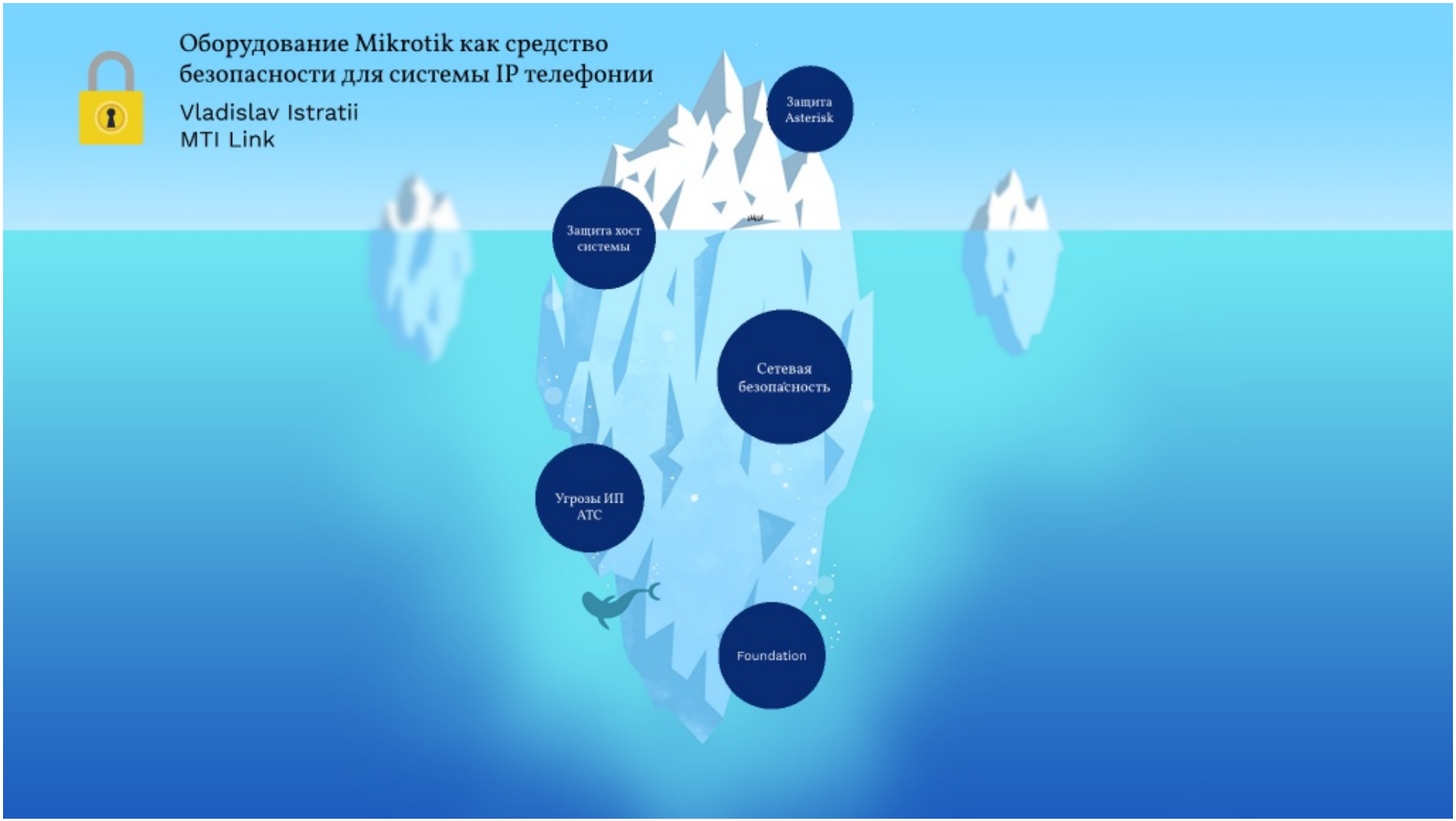
Vladislav Istratii
CMO "MTI Group" LLC

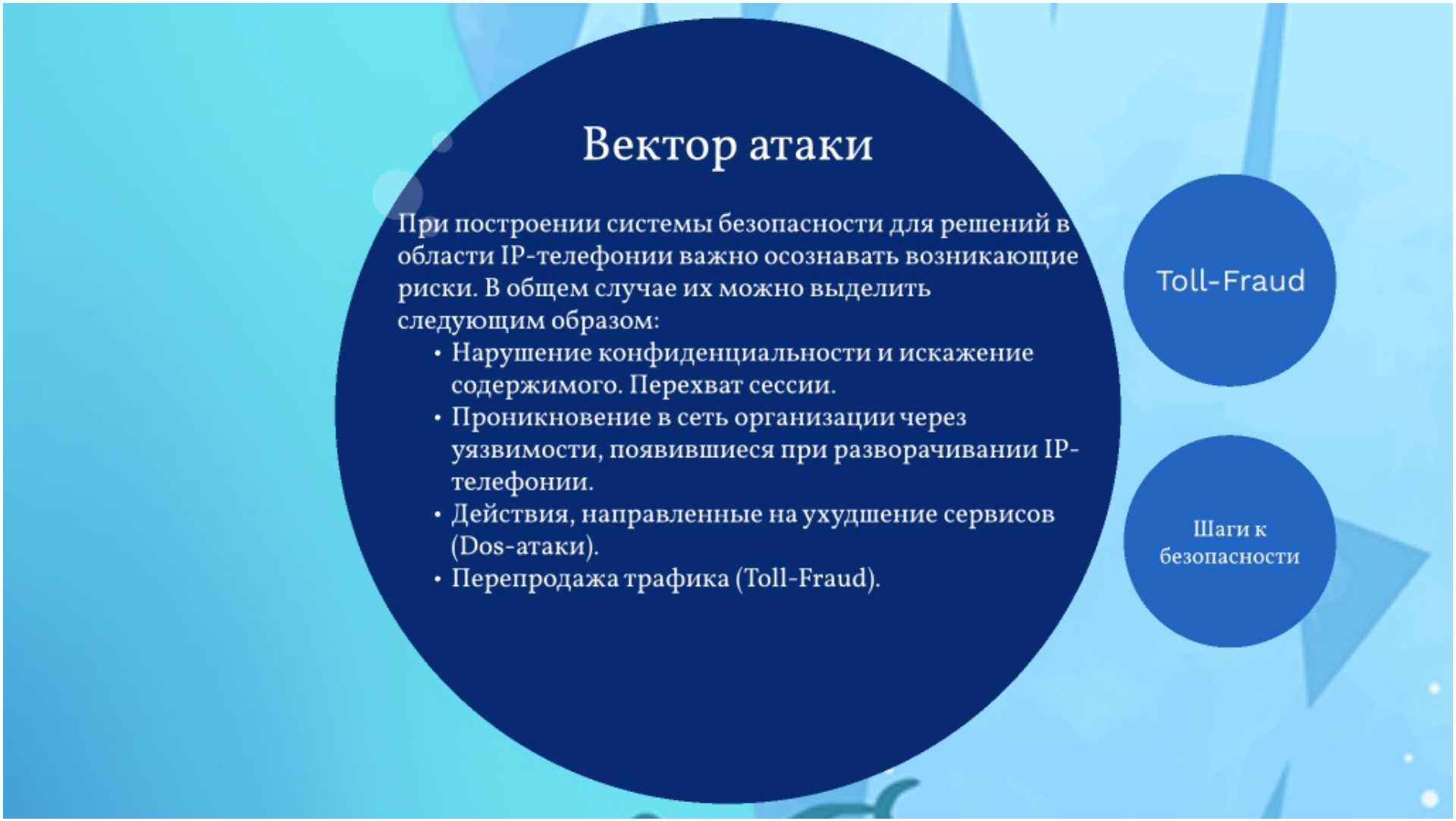
Oleg Tsyapa
CTO "MTI Group" LLC

Sergey Chernosvitov
Head Programmer

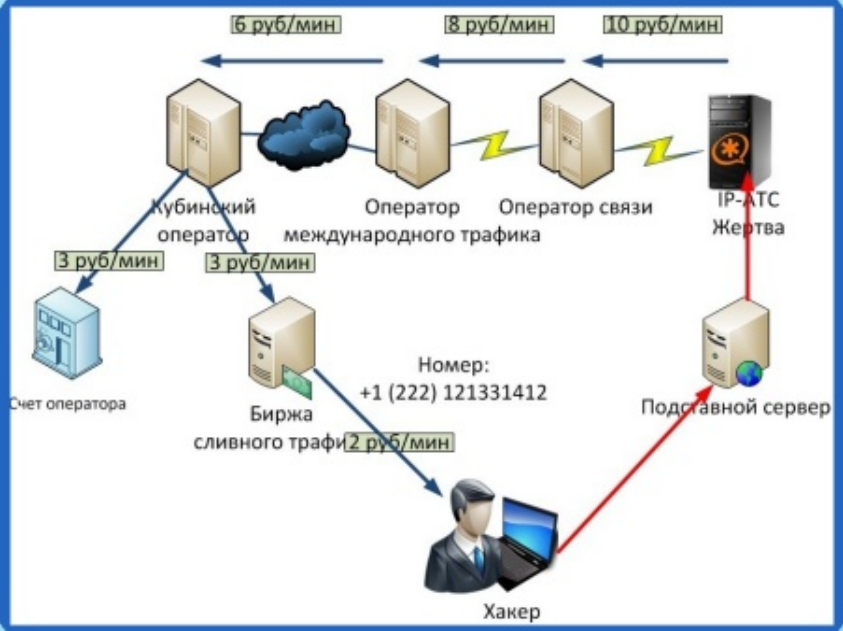
Нам доверяют

наши клиенты


Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation

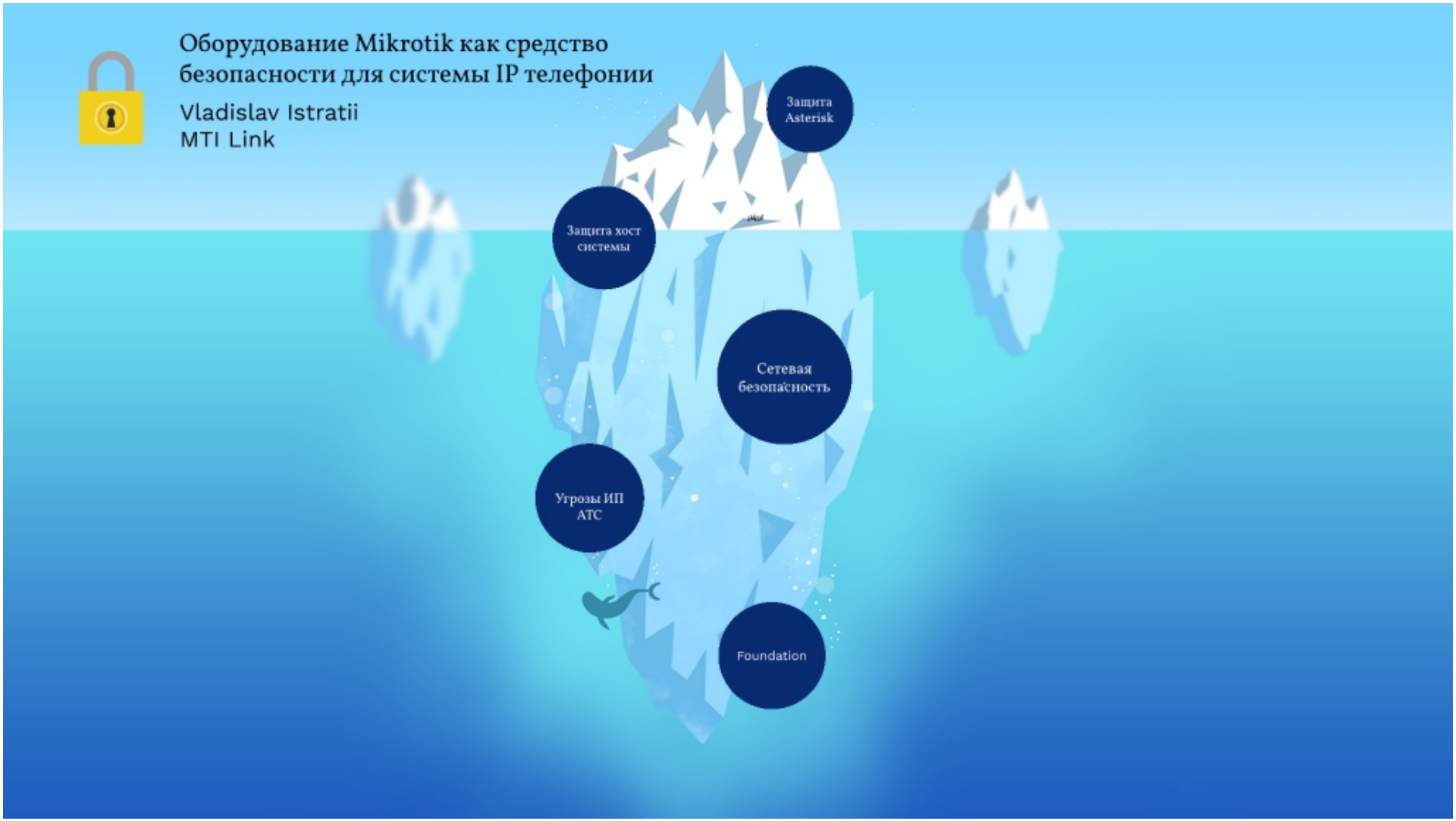

Вектор атаки
При построении системы безопасности для решений в области IP-телефонии важно осознавать возникающие риски. В общем случае их можно выделить следующим образом:
• Нарушение конфиденциальности и искажение содержимого. Перехват сессии.
• Проникновение в сеть организации через уязвимости, появившиеся при разворачивании IP-телефонии.
• Действия, направленные на ухудшение сервисов (Dos-атаки).
• Перепродажа трафика (Toll-Fraud).
Toll-Fraud
Шаги к безопасности

Toll-Fraud

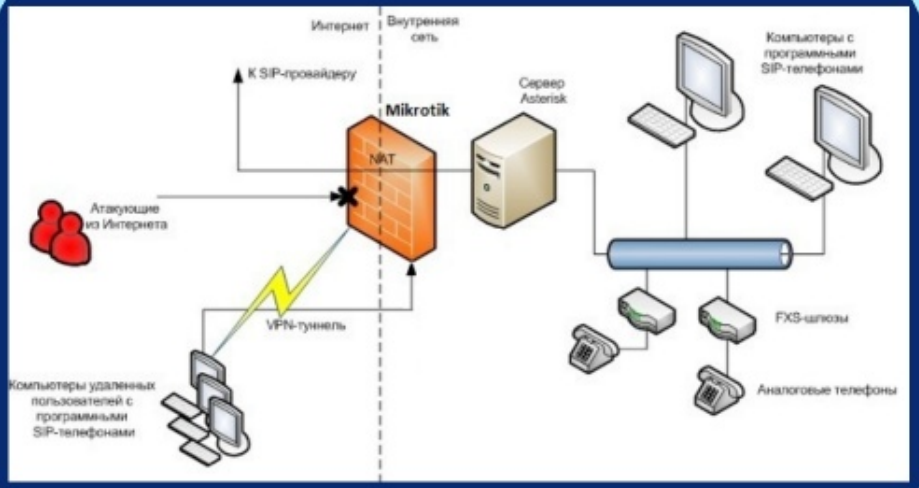

6 руб/мин
8 руб/мин
10 руб/мин
Кубинский оператор
Оператор международного трафика
Оператор связи
IP-АТС Жертва
3 руб/мин
3 руб/мин
Счет оператора
Биржа сливного трафи
Номер:
+1 (222) 121331412
2 руб/мин
Подставной сервер
Хакер

Защита IP АТС включает в себя:

- Организацию сетевой безопасности
- Структуру сети
- Обработку сообщений, логов
- Настройку Asterisk
- План маршрутизации звонков
- Настройку безопасности ОС Linux
- Безопасность периферийных устройств
- Административную организация


Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation

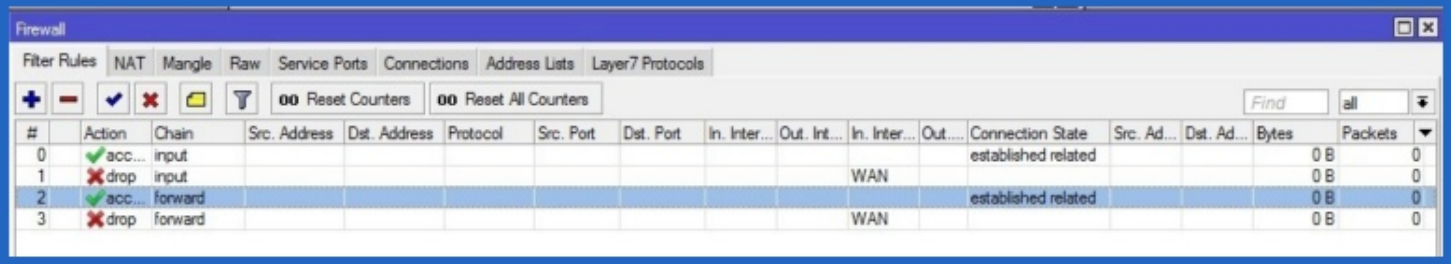
Сетевая безопасность

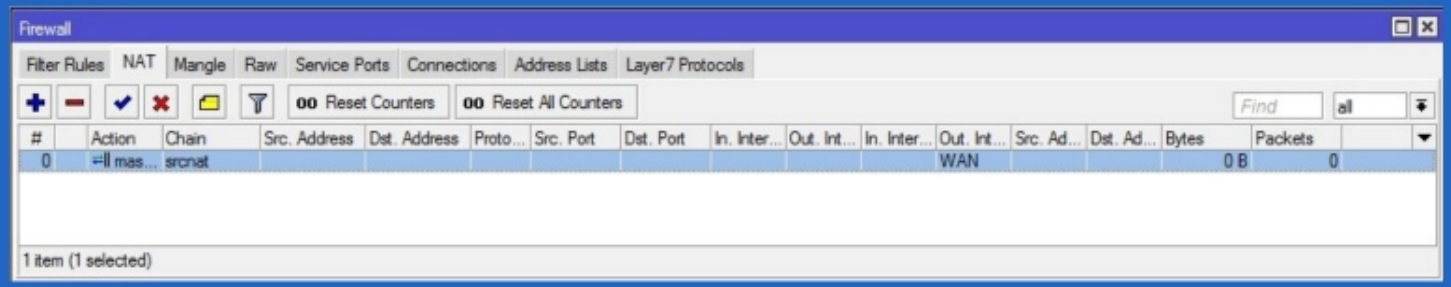


Firewall

Структура сети

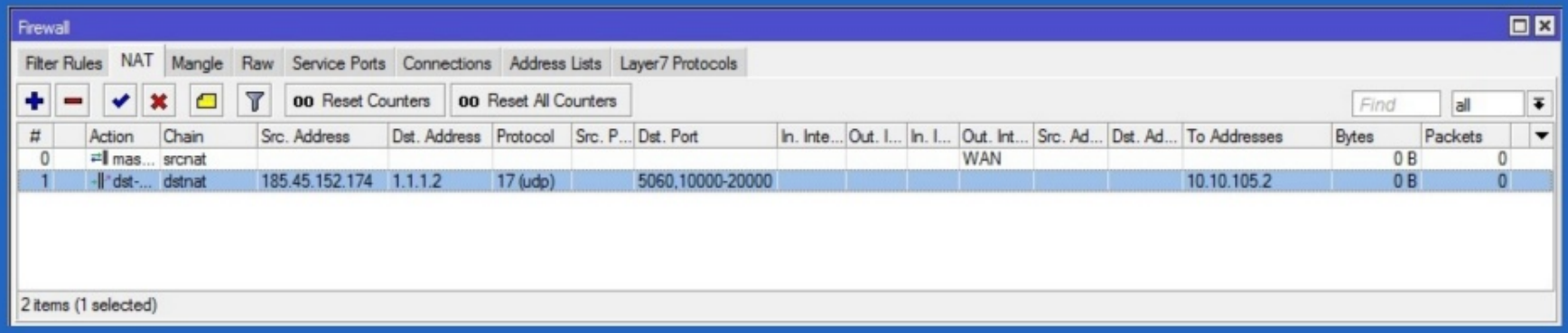
Firewall (Basic)

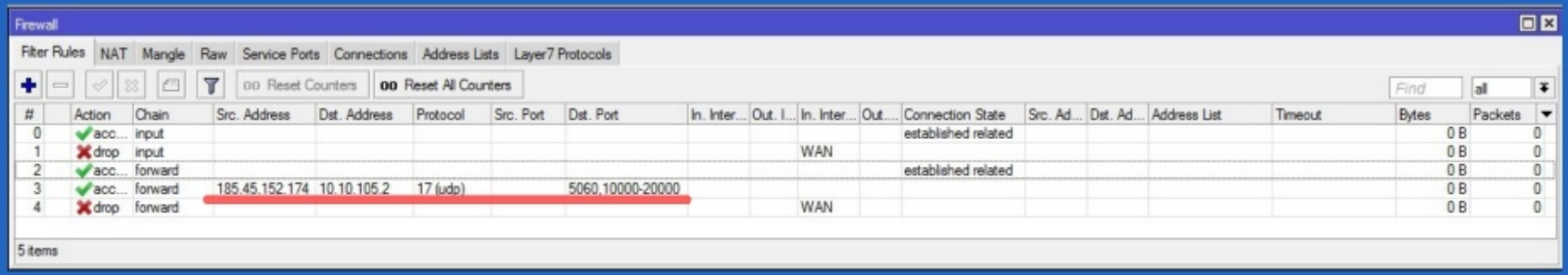




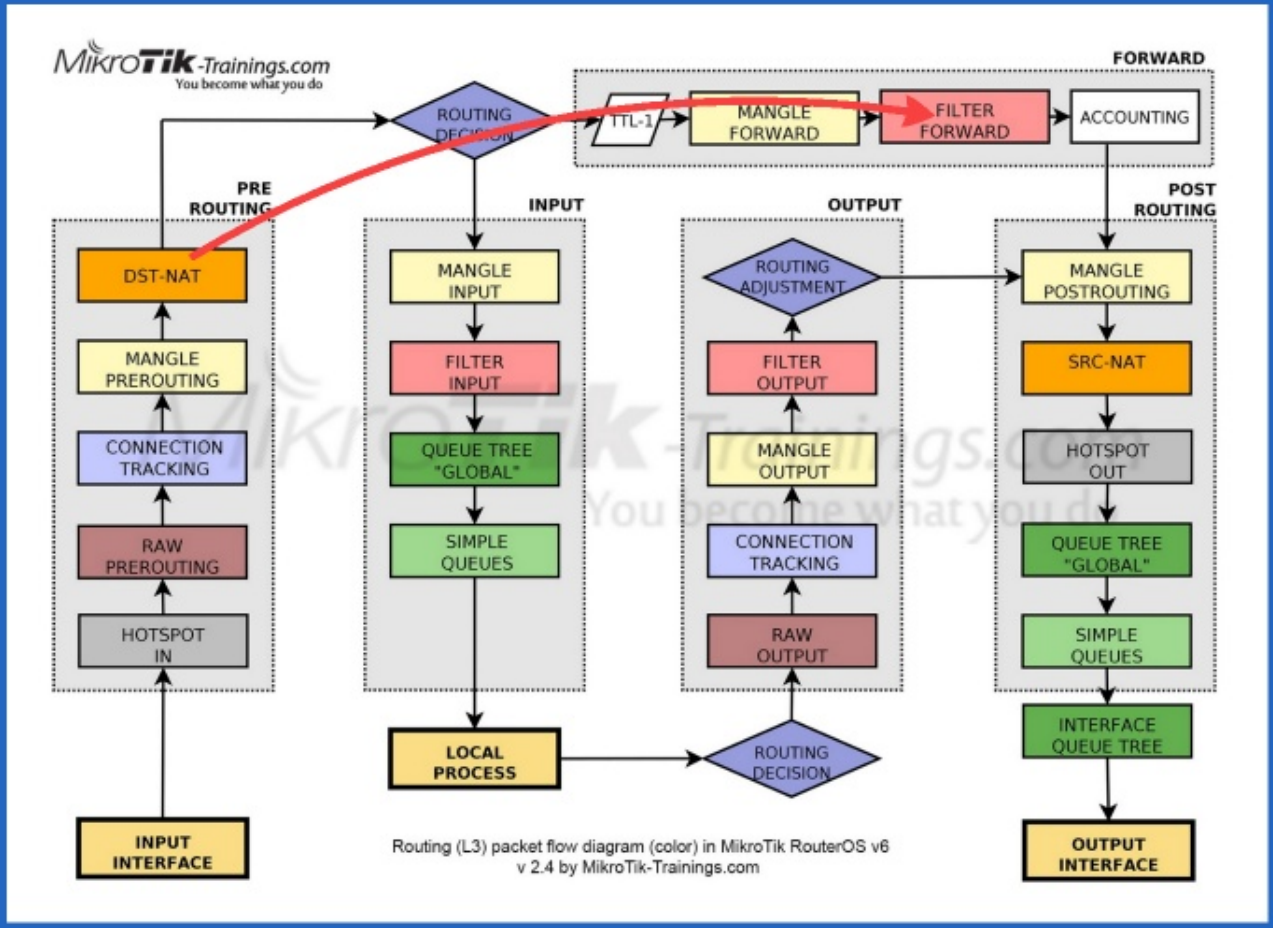
SIP.CONF
nat=comedia,force_rport

Firewall DST-NAT





SIP.CONF
nat=comedia,force_rport

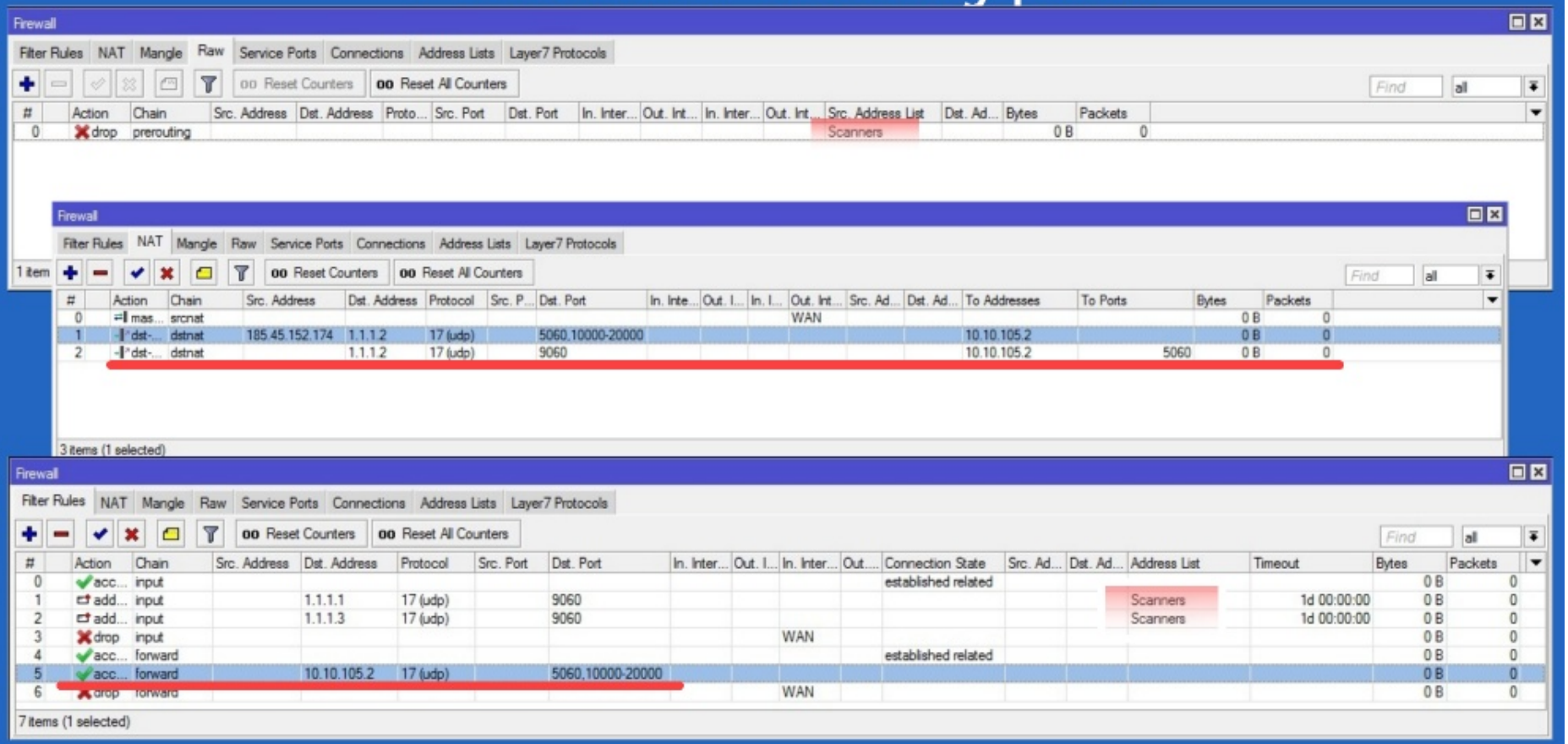


Хочешь такую? Подходи к нашему стенду и возьми бесплатно.

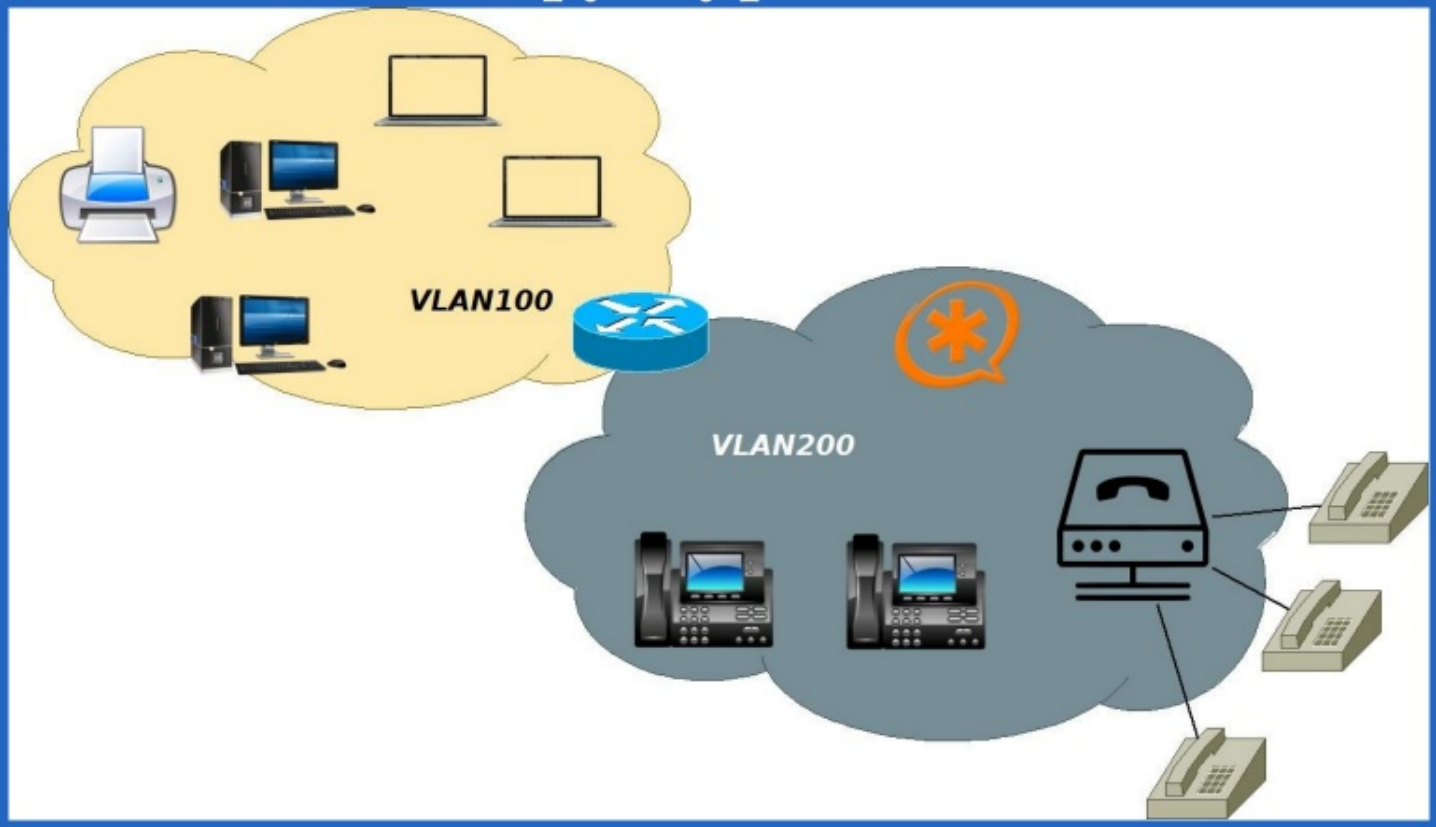
Firewall Honeypot

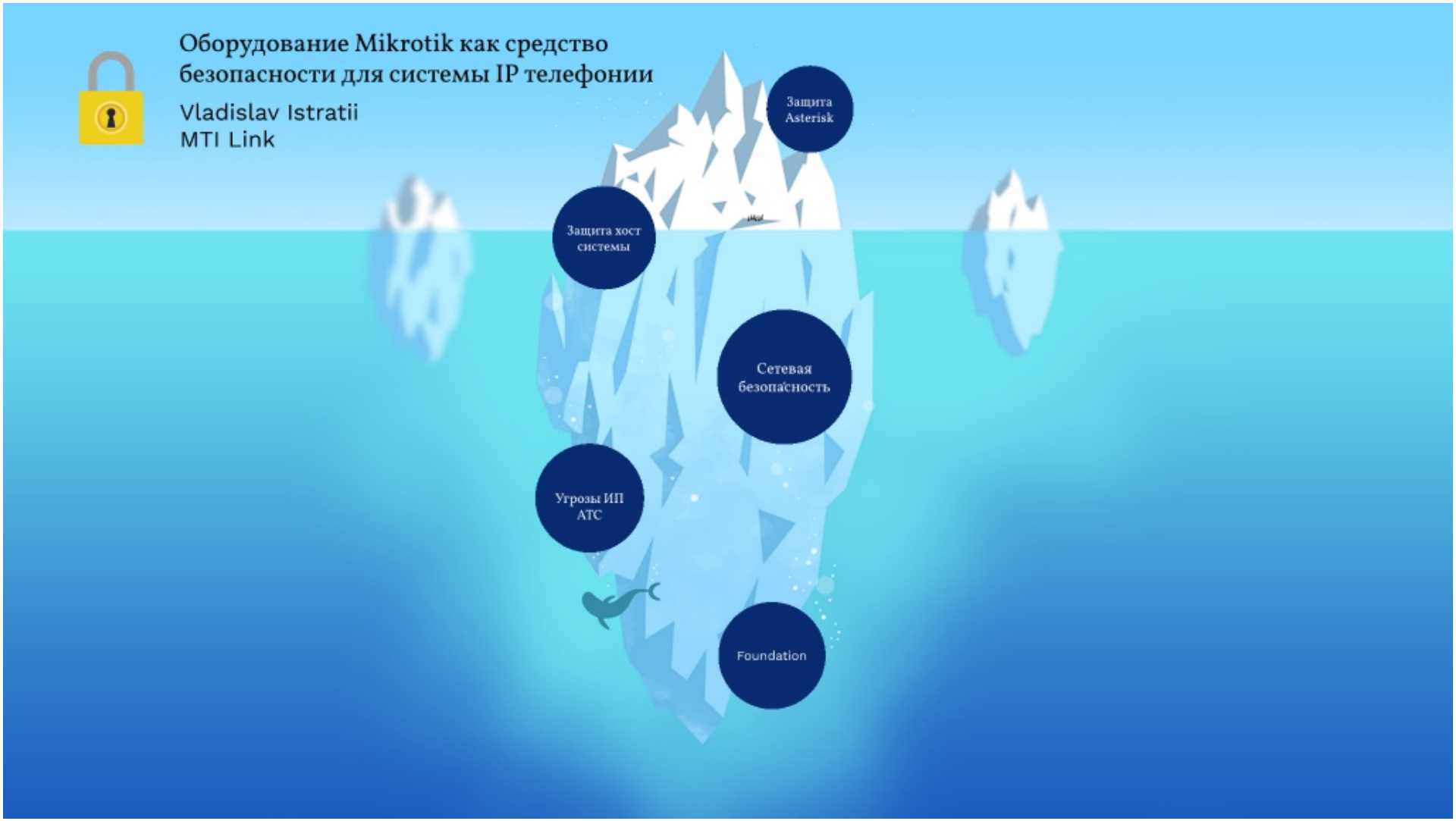
1.1.1.1
1.1.1.2
1.1.1.3
1.1.1.4
1.1.1.5
.....
1.1.1.254

Firewall Honeypot



Структура сети




Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation

Защита хост системы

- SSH
- IPTABLES
- Fail2Ban

SSH

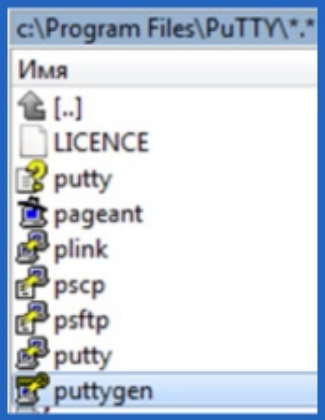
IPTABLES

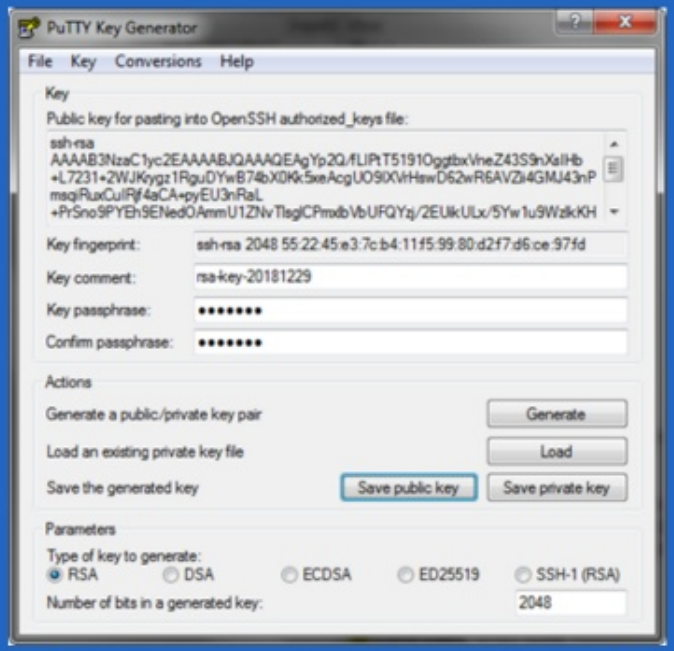
Fail2Ban

SSH

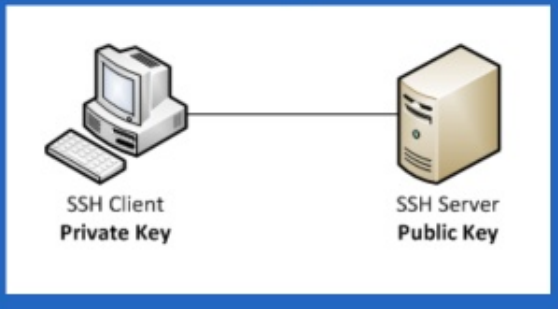
/etc/ssh/sshd_config

```
...
Port 6262
...
PasswordAuthentication yes
...
PermitRootLogin no
...
PubkeyAuthentication yes
```






```
mkdir ~/.ssh
#Импорт публичного ключа
ssh-keygen -i -f key >> .ssh/authorized_keys
chmod og-rwx -Rc ~/.ssh
```



IPTABLES

```
iptables -N input-voip
```
Создаем цепочку файервола

```
iptables -A INPUT -i lo -j ACCEPT
```
Разрешаем трафик по интерфейсу

```
iptables -A INPUT -p icmp -j ACCEPT
```
Разрешаем ICMP трафик (а можно и не разрешать)

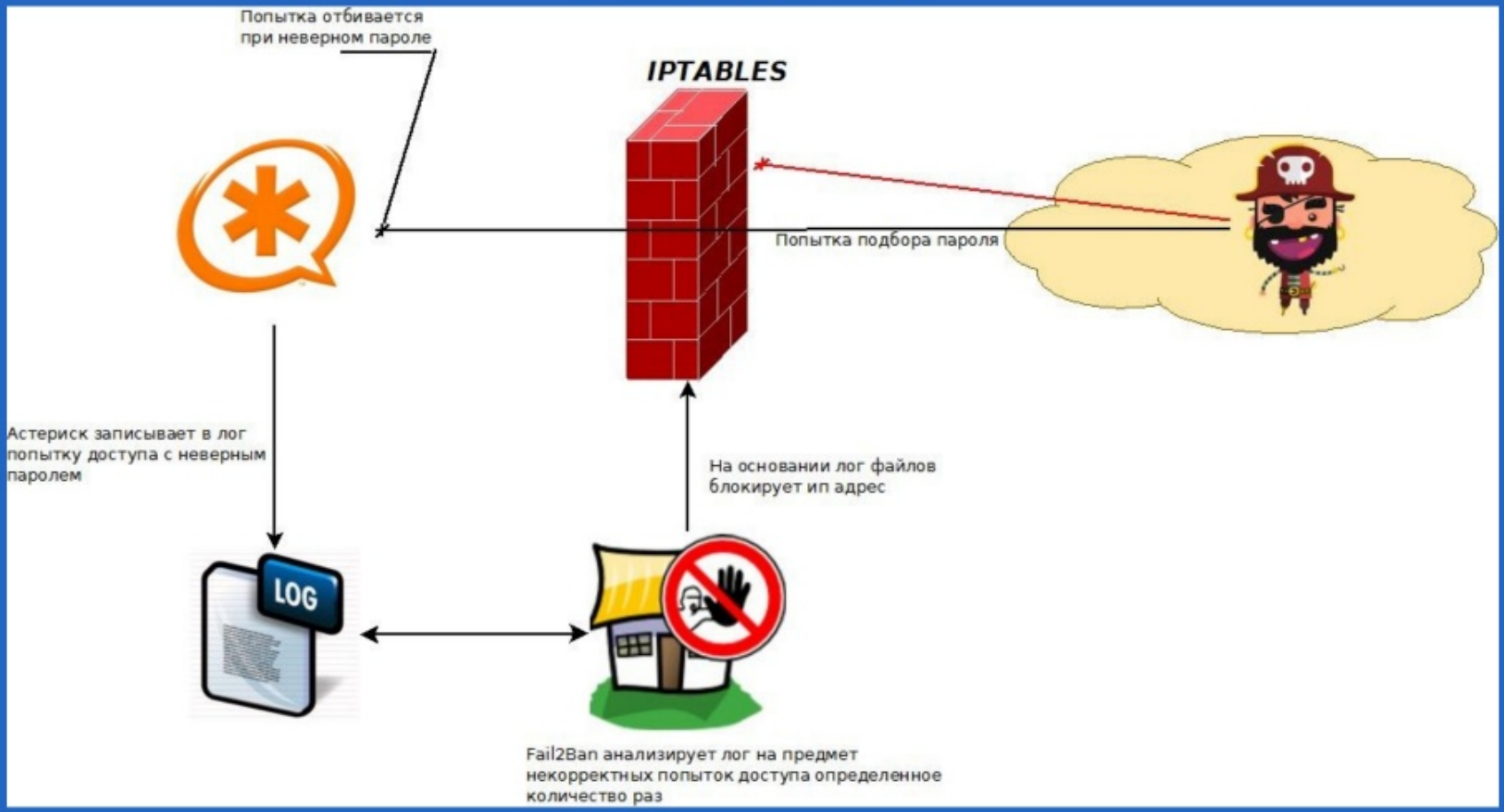
```
iptables -A INPUT -p udp --dport 5060 -j input-voip
iptables -A INPUT -p tcp --dport 5060:5061 -j input-voip
iptables -A INPUT -p udp --dport 10000:20000 -j input-voip
iptables -A INPUT -p udp --dport 4569 -j input-voip
iptables -A INPUT -p tcp --dport 22 -j input-voip
```
При попытке доступа на данные порты перенаправляем в цепочку input-voip

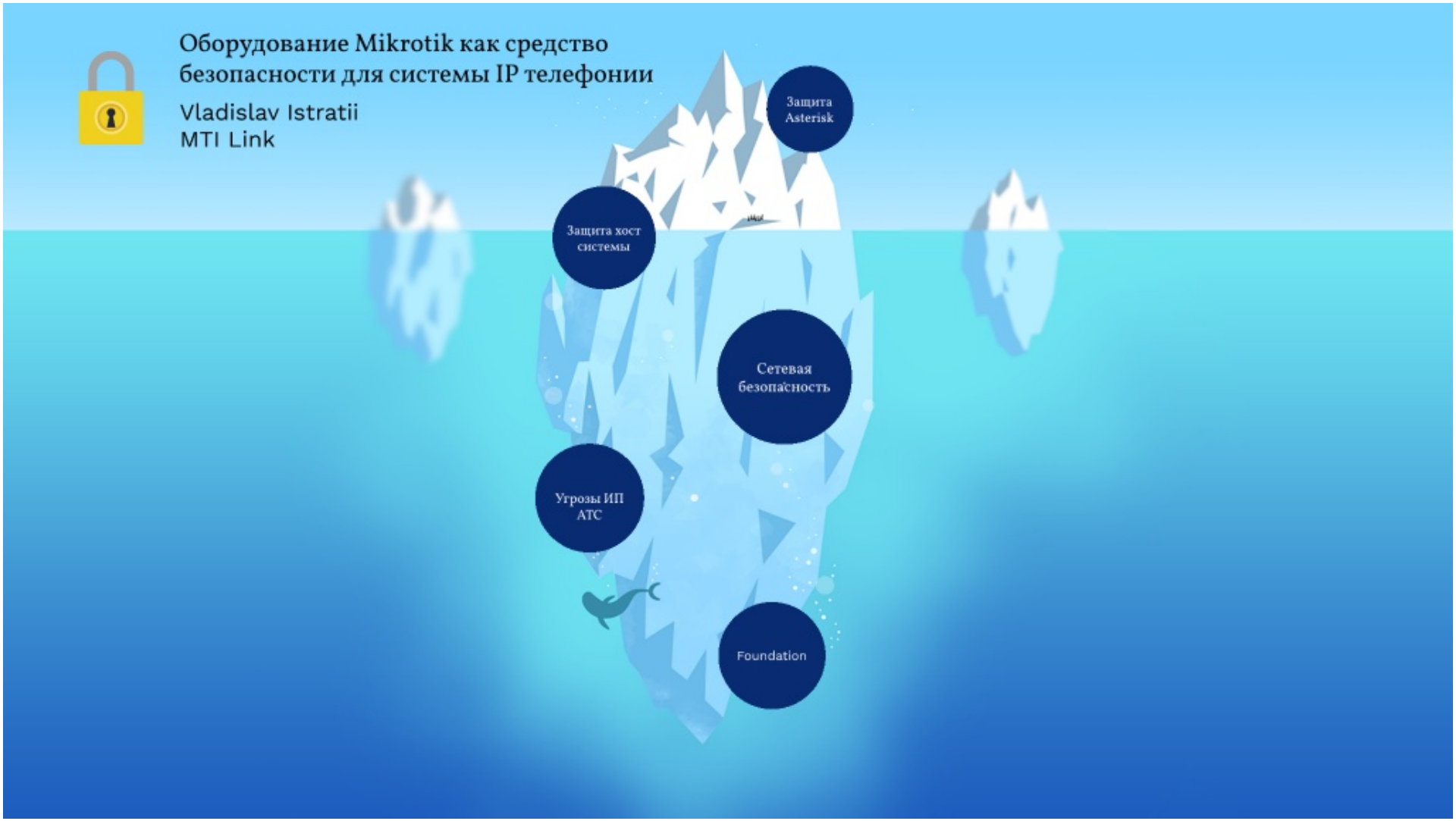
```
iptables -A INPUT -p icmp -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
```
Разрешаем пакеты RELATED, ESTABLISHED

```
iptables -A input-voip -s 10.10.105.0/24 -j ACCEPT
iptables -A input-voip -s 185.45.152.174 -j ACCEPT
```
Цепочка input-voip, где мы проверяем совпадает ли ип адрес запроса с разрешенными

```
iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
```
Блокируем все остальное

Fail2Ban


Попытка отбивается
при неверном пароле
IPTABLES
Попытка подбора пароля
Астериск записывает в лог
попытку доступа с неверным
паролем
На основании лог файлов
блокирует ип адрес
LOG
Fail2Ban анализирует лог на предмет
некорректных попыток доступа определенное
количество раз


Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation

Защита Asterisk

- Безопасная конфигурация sip.conf
- Защита dialplan`ом
- Защита оконечных устройств
- Упреждающие действия

Sip.conf

Dialplan

Оборудование

Упреждающие действия

Вопросы

Sip.conf

```
[general]
;Изменение порта udp
bindport = 7799

;Запретить отправлять сообщения о несуществующем
пользователе
alwaysauthreject=yes

#Маскируем АТС
useragent=Panasonic
sdpowner=Panasonic
sdpsession=Panasonic

[<пользователи>]
;ограничить по ip
deny = 0.0.0.0/0.0.0.0
permit = 192.168.100.0/24
;Использовать стойкий пароль
secret=920332$4nf323:;9asdYioepooALY39mD#dnnw2e
```

Dialplan

- Завершать номера расширения Hangup()'ом
- Устанавливать ограничения на максимальное число линий для пользователя
- Устанавливать ограничения на междугородние и международные вызовы
- Настроить cdr для отслеживания расходов
- Устанавливать ограничения по времени суток
- Высылать оповещения на email/sms на дорогие направления
- и т.д.

Защита оконечных устройств

- Используйте отдельную подсеть и ограничивайте доступ в по web/telnet только для администраторов
- Изменяйте стандартные пароли на вход в интерфейс настройки
- Изменяйте пароль для входа в режим конфигурации с клавиатуры телефона
- Отключайте лишний функционал (переадресации, DND), если он не нужен пользователю

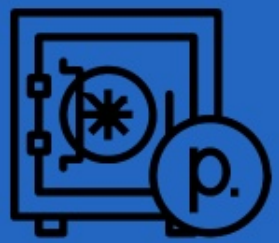
Упреждающие действия

Защита через оператора связи

- Установите ограничения на число минут (или расход средств)
- Не держите большую сумму на балансе
- Установите ограничения (звонок по вводу кода) для дорогих направлений
- Настройте уведомления о расходе средств
- Используйте VPN канал (если есть возможность) до оператора

В организации

- Повышение осведомленности персонала
- Регулярная смена паролей
- Обновление АТС и оконечных устройств

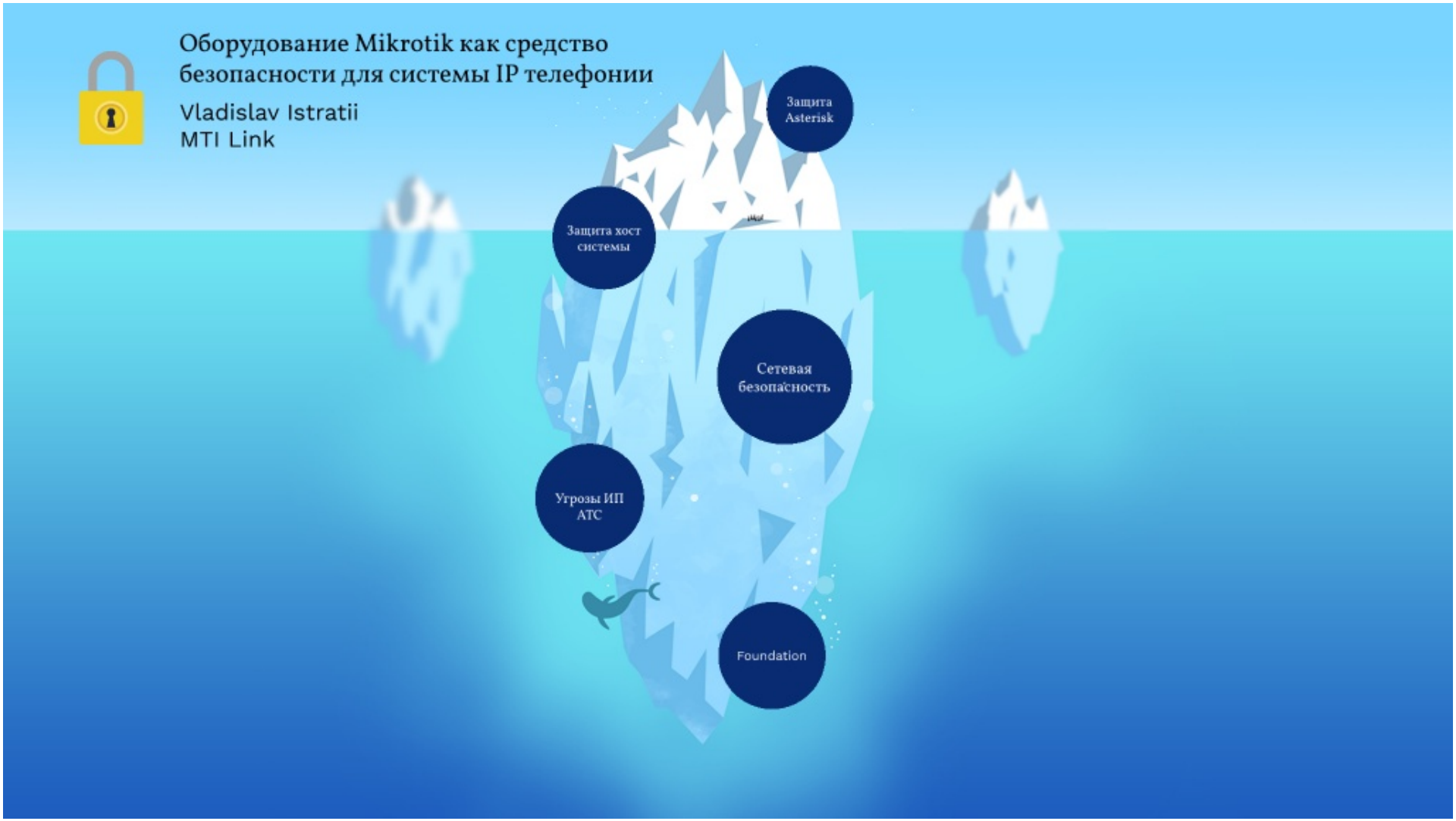


Контакты

Интеграция - mti-group.ru
Оборудование -shop.mti-group.ru
Software - mupssoft.com
Обучение - QTraining.ru
Обучение - MikroTik-Training**S.COM**

Corporate - ISP - WISP - DC
STYX - MikroTik - Procell
MUPSBox, MUPS, MTMS, IPCalc
Asterisk, MikroTik, e.t.c
MikroTik

Вопросы?


Оборудование Mikrotik как средство безопасности для системы IP телефонии
Vladislav Istratii
MTI Link
Защита Asterisk
Защита хост системы
Сетевая безопасность
Угрозы ИП АТС
Foundation