

# ИТ-инфраструктура в малом и среднем бизнесе

GetNet

Конференция для  
ИТ-специалистов

# Обо мне:

---



- Основатель и технический директор компании ITMAK
- 15 лет занимаюсь ИТ-Аутсорсингом в Нижнем Новгороде и области
- Опыт работы с более 100 организаций малого, среднего, крупного бизнеса, и государственными структурами

# О чем доклад

- Боль системных администраторов
- Экономия, которая приводит к затратам
- Советы, как построить ИТ-инфраструктуру с минимумом проблем
- Лайфхаки, облегчающие жизнь админам
- Как управлять тем, что, казалось бы, не управляется



# У ИТ-отделов очень разные судьбы

---



# Почему везде разная нагрузка

- Разная инфраструктура, разные требования, разное кол-во объектов и их удаленность
- Различные элементы и технические решения генерируют проблемы с разной частотой
- Спасение айтишников, утопающих в заявках – дело рук самих утопающих

# Дело рук самих утопающих:

- Автоматизация рутины
- Повышение управляемости инфраструктуры
- Ускорение диагностики и решения проблем
- Снижение количества выездов на объекты
- Уменьшение количества аварийных заявок



# Совет №1 – Системный подход



# Инвентаризация и «Источники Правды»

---

- GLPI / OCS для компьютеров
- Zabbix, LibreNMS, NetDisco для сетевого оборудования
- Карты сетей, L1, L2 и L3
- GIT – для хранения файлов конфигураций, скриптов и т.д.
- Wiki и Базы знаний для инструкций и т.п.
- Пароли – храним в менеджере паролей
- NetBox – Для СКС и сетевого оборудования

Альтернатива: «Мы и так все знаем»



# Доступ ко ВСЕМУ из точки управления

---

- Всё оборудование и ПО доступно для управления без дополнительных манипуляций
- Подключаемся по SSH, RDP, VNC, MeshCentral
- VPN для связи с удаленными объектами
- Прямой доступ через интернет только по белым спискам / port knocking

— «У нас же есть AnyDesk»


(а кому надо — дадут доступ)

# Мониторинг


---

- **Мониторим всё, что можно:** от температуры кактуса, до бэкапов бэкапов (и нет, это не ошибка)
- **Zabbix, Prometheus, Grafana** — умеют почти всё и почти бесплатно
- **Раньше узнали** — Быстрее починили
- **Alert'ы** на почту, телеграм, хелпдеск и т.д.

— «Пффф... Без нас всё равно ничего не починят»



**Всё это влияет на  
эффективность и скорость  
работы ИТ-отдела.**



# Как всё чинить – понятно, но почему всё ломается?


---

- **Корень проблемы** – выбор неверных решений и тиражирование этих решений
- **Причины**, как правило экономические

# Что такое хорошо и что такое плохо?

- Единого понимания и стандартов не существует
- Каждый специалист – отдельная «нейросеть» со своей уникальной биг-датой и выводами
- Все осложняется разными требованиями, условиями и бюджетами





# Советы и лайфхаки за 15 лет опыта работы



# Главная боль админа – юзеры

- Да, они могут казаться «тупыми» – это нормально
- Обучение юзеров – мало где возможно и неэффективно
- Короткие инструкции – работают, если размещать их в правильном месте
- Главный совет – нормально общайтесь, но не надо позволять им лишнего

# Стратегический запас ЗиП

---

- В идеале – резерв должен быть абсолютно для всего
- Особенно важен резерв для всего, когда процедура закупок долгая и сложная.
- Обязательно держим резерв для редких, но важных узлов и элементов

# Покупайте нормальное оборудование

- Оборудование «для дома» (SOHO) – используем только дома
- Считаем полную стоимость владения (TCO) на срок от 5 лет, а не тупо смотрим на цену
- Люди, ответственные за эксплуатацию и решение проблем с техникой, обязательно имеют право голоса
- Парк оборудования не превращаем в зоопарк

# Три совета по Принтеры и МФУ

О принтерах часто не задумываются, но с ними связано до 20% заявок на ИТ-отдел



# Принтеры и МФУ: Совет по экономике



## HP LaserJet Pro 4103fdw:

Цена принтера	50000р
Цена заправки W1510X	1200р
Ресурс картриджа W1510X (15%)	3000 лист.

**TCO за 50 тыс. лист. 70 000р**



## HP LaserJet M141w:

Цена принтера	17000р
Цена заправки	500р
Ресурс картриджа (15%)	300 лист.

**TCO за 50 тыс. лист. 100 000р**

# Правильно подключаем принтеры

- По Ethernet
- С постоянным IP-адресом
- Через стандартный порт TCP 9100 (RAW)  
(или фирменный протокол вендора)
- И в качестве бонуса получаем мониторинг печати

Настройка стандартного монитора порта TCP/IP

Параметры порта

Имя порта: ET0021B753C4F7

Имя принтера или IP-адрес: 10.167.14.108

Протокол

☒ 1. RAW ☐ 2. LPR

Параметры RAW

Номер порта: 9100

Параметры LPR

Имя очереди:

☐ Разрешен подсчет байтов в LPR

☒ Состояние SNMP разрешено

Имя сообщества: public

Индекс устройства SNMP: 1

# Лайфхак-Скрипт «Починить печать»

---

- Решает 99% проблем с «застрявшими» заданиями:

```
taskkill /F /IM spoolsv.exe
```

```
taskkill /F /IM printfilterpipelinesvc.exe
```

```
net stop spooler
```

```
del /f /s /q %windir%\system32\spool\printers\
```

```
del /f /s /q %windir%\system32\spool\servers\
```

```
net start spooler
```

# Совет по ПК – не надо брать самые дешевые



+



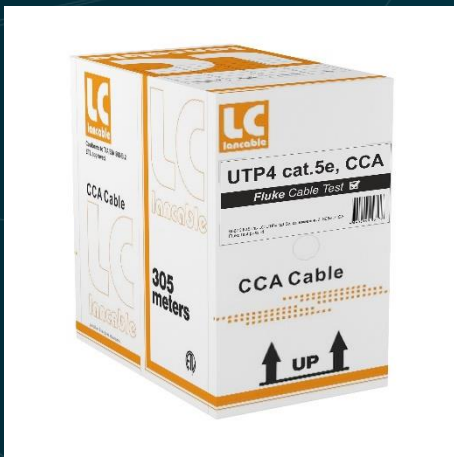
Их век может оказаться недолгим

# Идеальные характеристики новых АРМ

- Запас по производительности 30-50% от текущих потребностей
- Возможность апгрейда CPU / ОЗУ / SSD
- CPU – не ниже актуальных i3 / r3
- ОЗУ – не менее 16 GB / 8GB (закладываем возможность апгрейда)
- Место на диске не менее 50% от текущих потребностей

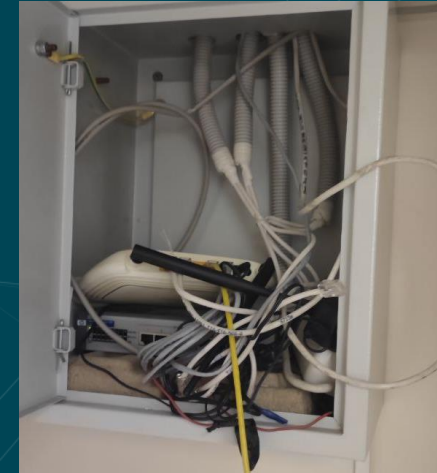
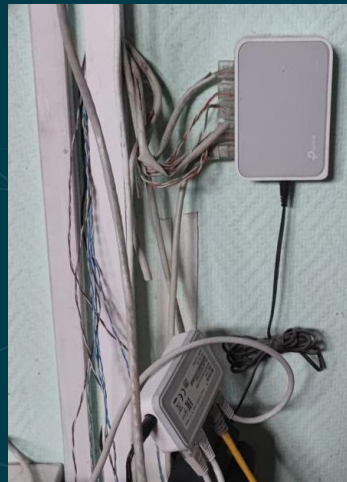
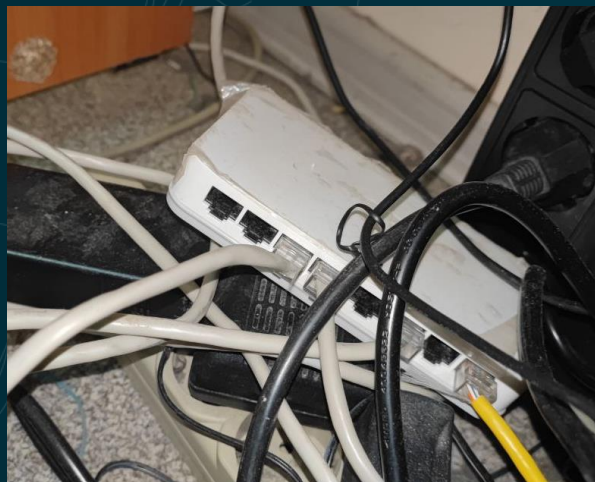
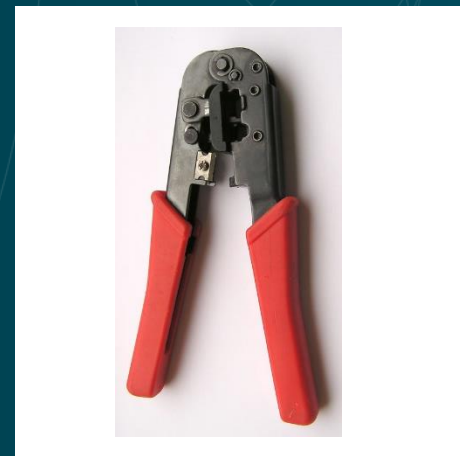


# Совет по Сети – такое надо переделывать



К сожалению, огромное число сетей  
выглядят так

(и работают они не сильно лучше)



# Идеальное решение – Нормальная СКС

- Полностью медный кабель сечением  $\geq 0,50\text{мм}$  (23-24AWG)
- Кабель из бухты – в розетки и патч-панели
- Все оборудование – в коммутационные шкафы
- Конечные устройства – подключаем патч-кордами
- Управляемые свитчи – желательно все



# Управляемый + PoE switch = Идеально



- Мониторинг состояния
- Удаленное управление питанием портов
- Автоматическая перезагрузка «зависших» устройств по питанию



# Совет по питанию – лучше сэкономить



- «Пилот» (или просто в розетку)



- ИБП Бывает полезен в редких случаях\*\*\*\*
- Но «По-умолчанию» ставить их везде = ошибка

# ИБП на рабочих станциях = вредительство

Нет ИБП?

Сэкономили — и счастливы

- **Источники Бесперебойного Писка и потери питания**
- **Расходы на сами ИБП и замены батарей**
- **Экстренные заявки с выездами**


Количество сбоев, мертвого оборудования, падения систем и повреждения файлов за много лет было примерно одинаковым




# ИБП на Серверах и стойках



Нужная и полезная вещь!



# Как управлять неуправляемым?



# Сервер на базе Desktop



Да, это жуткий костыль, но лучше, чем ничего

- Вкл. / Выкл. / Reset / KVM – удаленно по сети
- Виртуальный ISO – для удаленной загрузки / установки любой системы

# Как жить, если нет домена?

- Без коммерческих решений – всё бесплатно
- Автоматизация установки и настройки с помощью авторских скриптов
- Удаленный доступ – просто и безопасно
- Свой домен на Mikrotik – DNS для удаленных сетей

# Удаленный доступ к консоли

PSEXEC и WINRM небезопасны:

- Требуют параметра `LocalAccountTokenFilterPolicy=1`
- Позволяют подключаться с любого хоста
- Можно авторизоваться любым пользователем с правами администратора

# OpenSSH на Windows

- Нативно и устанавливается одной командой:

```
dism /Online /Add-Capability /CapabilityName:OpenSSH.Server~~~~0.0.1.0
```

- Можно выбрать конкретных **AllowUsers**
- Доступна авторизация по ключам и ограничение входа по IP
- Можно авторизоваться под обычным юзером
- Поддерживает работу в домене AD



# OpenSSH + Ansible на Windows

Может запускать любые команды и скрипты **cmd** и **PowerShell**

Управление системой:

**win\_user** — управление пользователями.

**win\_group** — управление группами.

**win\_group\_membership** — членство в группах.

**win\_service** — управление службами.

**win\_regedit** — работа с реестром.

**win\_environment** — переменные окружения.

**win\_scheduled\_task** — задания планировщика.

**win\_updates** — установка обновлений.

Сеть:

**win\_hostname** — имя хоста.

**win\_dns\_client** — настройка DNS.

**win\_firewall\_rule** — правила брандмауэра.

Файловая система:

**win\_copy** — копирование файлов.

**win\_file** — управление файлами.

**win\_share** — сетевые шары.

# OpenSSH + Ansible: а какие минусы?

- Это Push-модель, а значит клиент должен быть доступен, т.к. подключение иницируется извне.
- Хорошо подходит для компьютеров, которые всегда включены
- Если компьютер недоступен – это проблема!
- Да, есть варианты как её обойти, но с кучей компромиссов

# Авторские скрипты на PowerShell

---

- Запускаются по триггеру в планировщике (включение ПК, вход в систему, дата/время)
- Запрашивают на удаленном SMB/FTP сервере скрипт, предназначенный для компьютера
- Запуск скрипта по имени компьютера, дате, версии скрипта или комбинации параметров
- Отслеживают историю версий, отправляет результат выполнения и логи на сервер

# Все скрипты доступны на GitHub



[github.com/itmak-ru](https://github.com/itmak-ru)

# Все локальные хосты в DNS на MikroTik

DHCP Network <192.168.144.0/24>

Address: 192.168.144.0/24

Gateway: 192.168.144.1

Netmask: 24

☐ No DNS

DNS Servers: 192.168.144.1

Domain: company.local

WINS Servers:

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

Script <script1-dns-static>

Name: script1-dns-static

Owner: powerdog

☐ Don't Require Permissions

Policy: ☒ ftp ☒ reboot ☒ read ☒ write ☒ policy ☒ test ☒ password ☒ sniff ☒ sensitive ☒ romon

Last Time Started: May/10/2025 18:29:40

Run Count: 312

Source:

```
# Domain to be added to your DHCP-clients hostname
local topdomain;
set topdomain "company.local";

# Use ttl to distinguish dynamic added DNS records
local ttl;
set ttl "00:59:59";

# Set variables to use
local hostname;
local hostip;
```

Buttons: OK, Cancel, Apply, Comment, Copy, Remove, Run Script

DHCP Server <defconf>

General Queues Script

Lease Script:

/system/script/run script1-dns-static

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

enabled

- В DHCP-сервере прописываем домен
- Добавляем скрипт, который добавляет все DHCP-leases в DNS
- Настраиваем запуск скрипта при получении DHCP-настроек

# Все удаленные хосты в DNS на MikroTik

- Настраиваем Split DNS с Failover:

```
/ip dns static
```

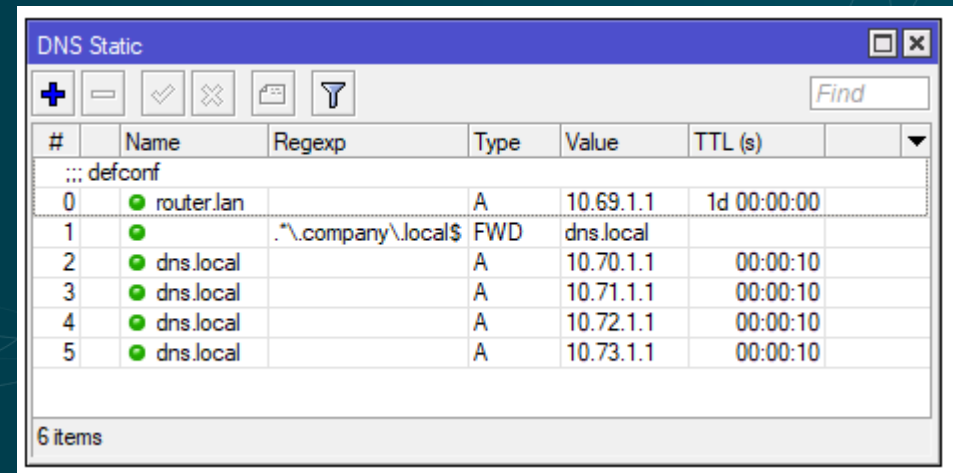
```
add forward-to=dns.local regexp=".*\\.company\\.local\\$" ttl=1h type=FWD
```

```
add address=10.51.1.1 name=dns.local ttl=10s
```

```
add address=10.52.1.1 name=dns.local ttl=10s
```

```
add address=10.53.1.1 name=dns.local ttl=10s
```

```
add address=10.54.1.1 name=dns.local ttl=10s
```



#	Name	Regexp	Type	Value	TTL (s)
0	router.lan		A	10.69.1.1	1d 00:00:00
1		.*\\.company\\.local\\\$	FWD	dns.local	
2	dns.local		A	10.70.1.1	00:00:10
3	dns.local		A	10.71.1.1	00:00:10
4	dns.local		A	10.72.1.1	00:00:10
5	dns.local		A	10.73.1.1	00:00:10

6 items



# А что там с экономией?





# Как можно экономить на оборудовании

- Можно покупать б/у технику, **но только хорошее б/у**
- Помнить про ТСО и экономию на долгой дистанции
- Покупать более простые варианты и модернизировать в будущем
- Отказаться от всех лишних ИБП

# Как донести идею до руководства

---

- Улучшение безопасности – хороший аргумент
- Напоминать о рисках простоев и финансовых потерь из-за экономии
- Рассказать что капитальные расходы приведут к снижению операционных
- Настаивать на важности участия ИТ-отдела в принятии решений о закупках и составлении бюджета

# Немного скептицизма и здравомыслия

- Понимать политику в отношении к капитальным и операционным расходам, в т.ч. на персонал
- Не всех можно спасти
- Не все изменения получится совершить быстро
- Но это не значит, что нужно опускать руки

# Спасибо за внимание!

Буду рад ответить на все ваши вопросы сейчас или свяжитесь со мной в будущем:



Алексей Макаров

am@itmak.ru

+7 929 053-67-03

tg://alexeyzero



[github.com/itmak-ru](https://github.com/itmak-ru)

GetNet

Конференция для  
IT-специалистов