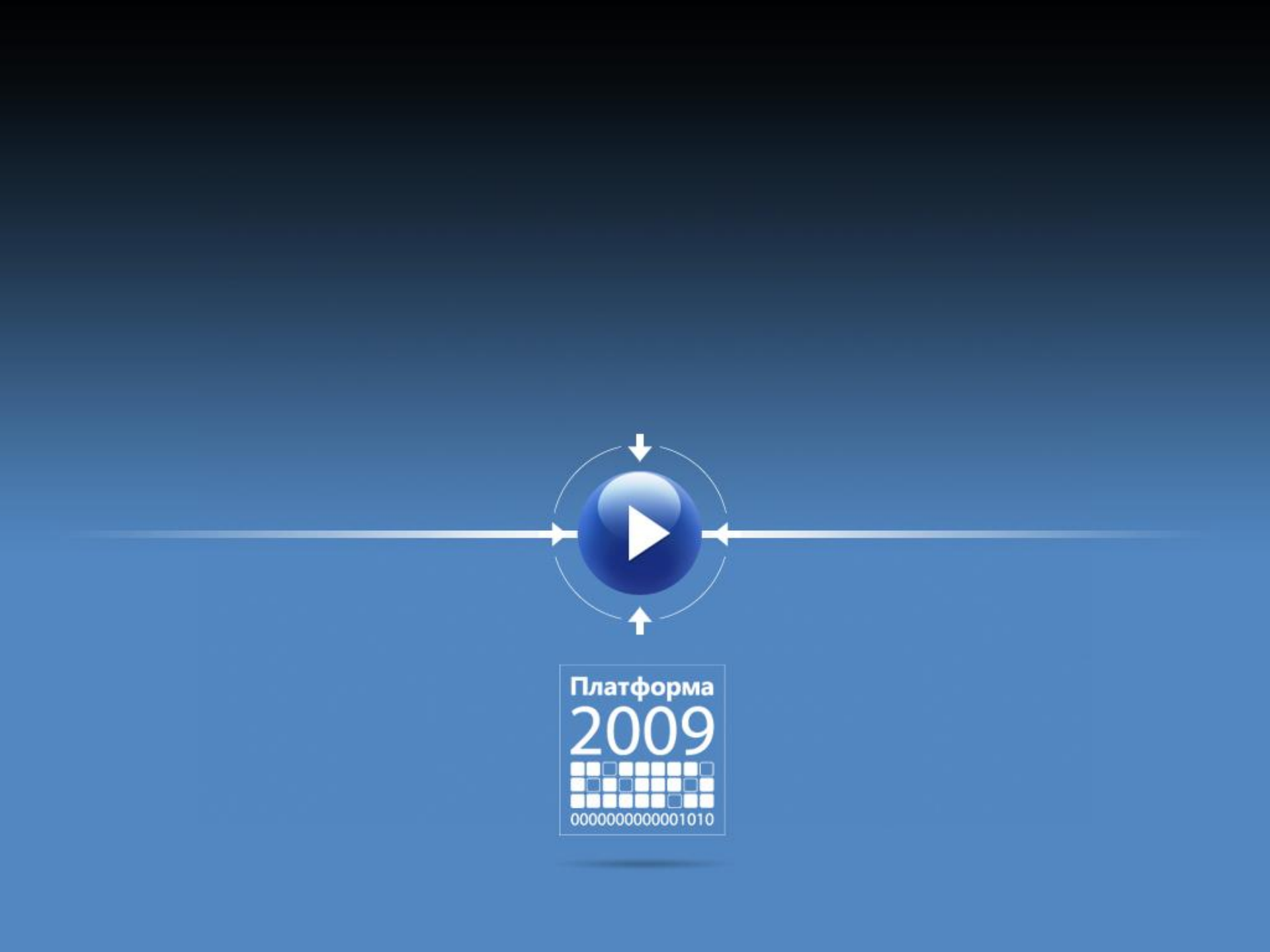

Платформа
2009
0000000000001010

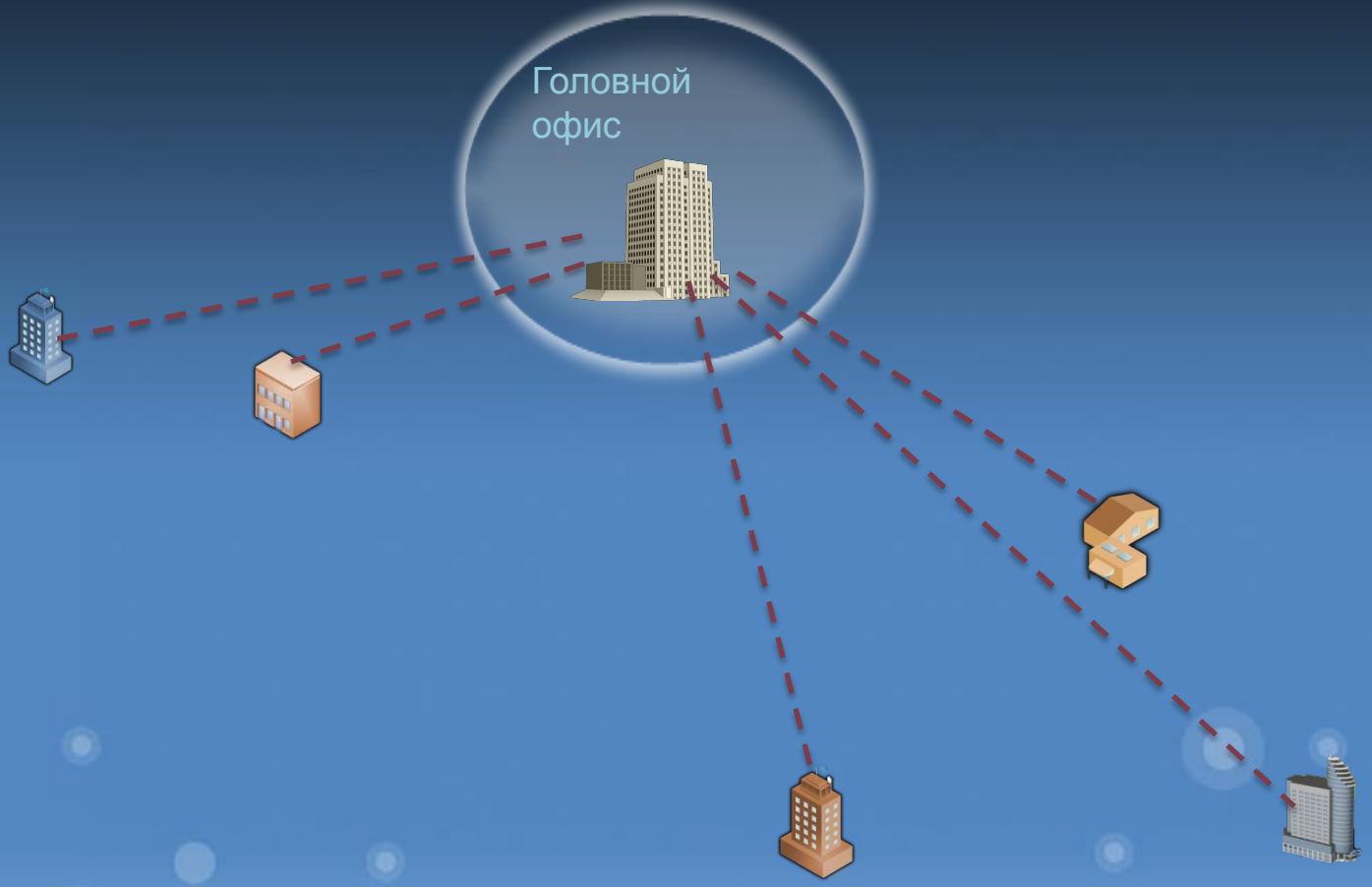
# Что в филиале мне твоём?

**Бешков Андрей**
Microsoft RUS
abeshkov@microsoft.com

**Станкевич Александр**
Stanky@stanky.ru

Платформа 2009
0000000000001010

# Дилема филиалов

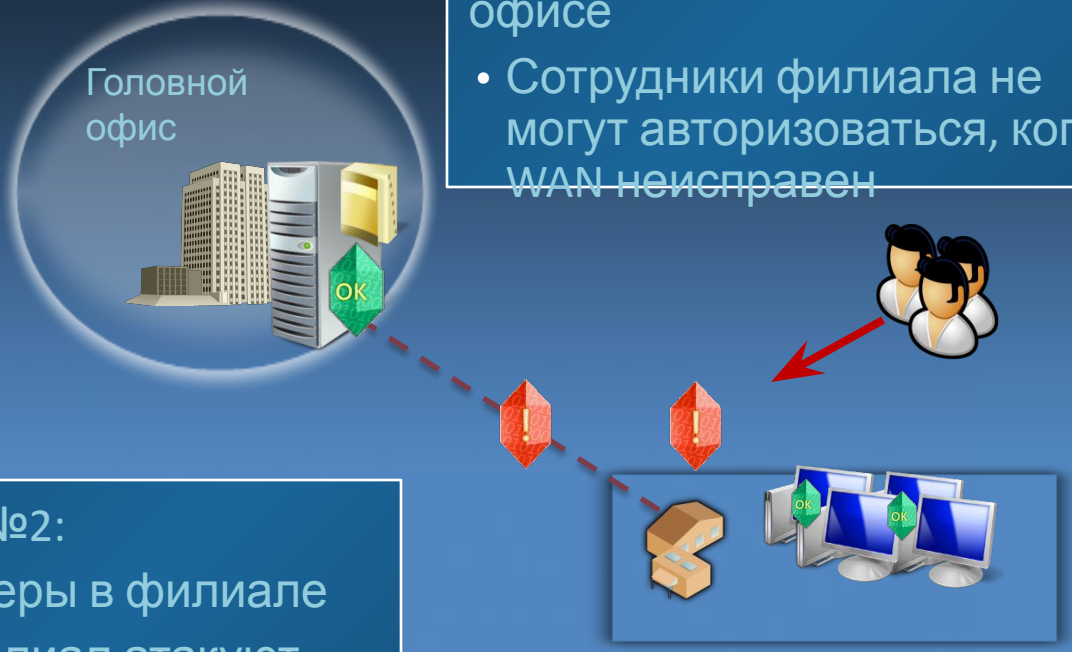


# Дилема филиалов

Вариант №1:

Контроллеры в головном офисе

- Сотрудники филиала не могут авторизоваться, когда WAN неисправен




Вариант №2:

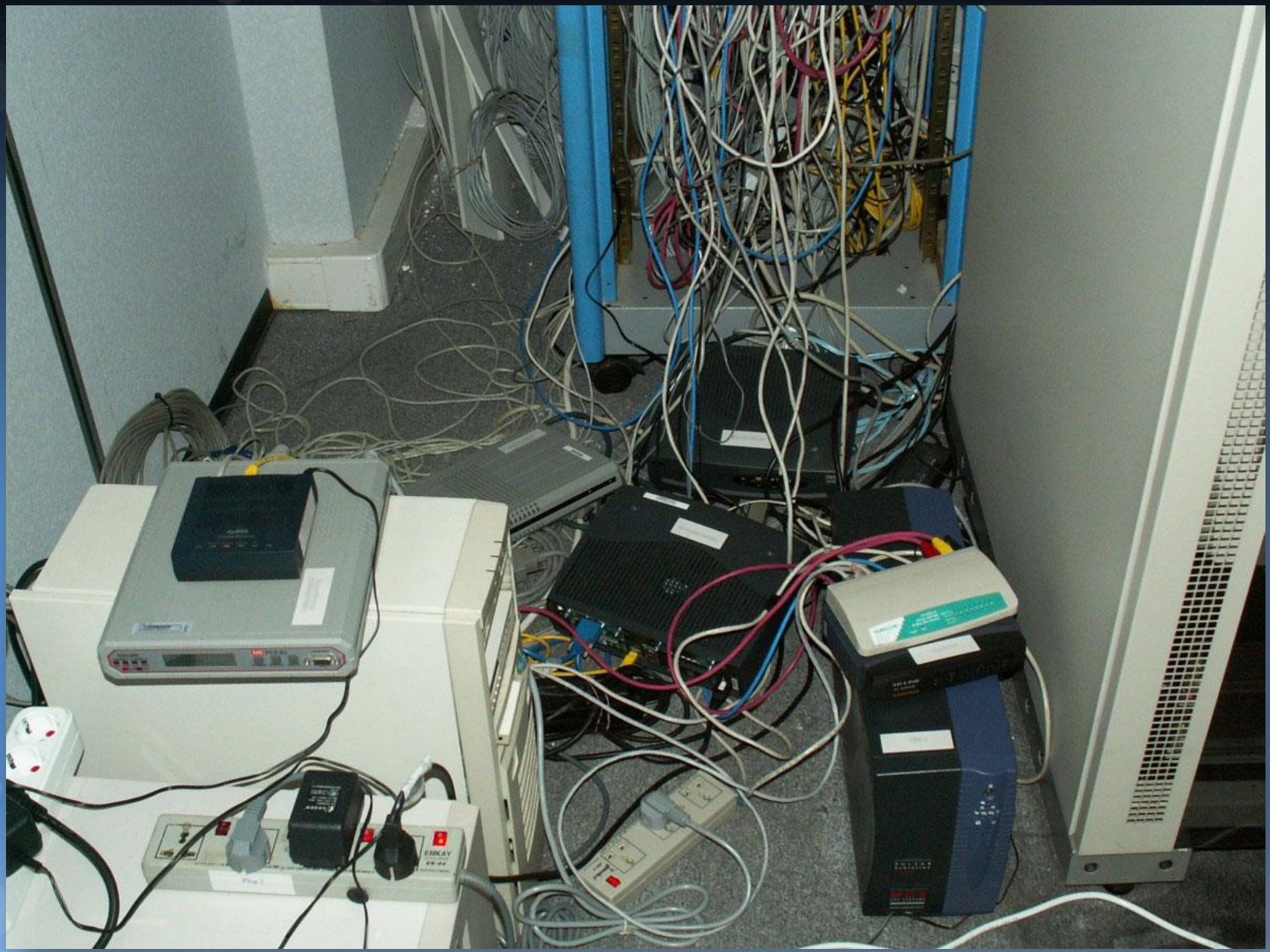
Контроллеры в филиале

- Если филиал атакуют, вся организация может стать уязвимой

# Это ваш филиал?

# Это ваш филиал?

# Это ваш филиал?



# Это ваш филиал?

*** Дверь закрывающая доступ в помещение не**

# Это ваш филиал?

Тогда мы идём к вам ☺️ ...

# Демонстрация

«Взлом»
контроллера домена

Платформа
2009
0000000000001010

# Контроллеру домена необходимо обеспечить...


**ФИЗИЧЕСКУЮ БЕЗОПАСНОСТЬ!**

# Read-Only Domain Controller

## Разделение администрирования

- Администратору RODC не нужно быть членом группы Domain Admins
- Предотвращение порчи AD филиальным администратором

## Однонаправленные реплики

- Нет репликаци от RODC к полноценному DC
  - Изменения на RODC не попадают в AD


## Секреты не хранятся

- Можно настроить хранение паролей филиальных пользователей
- Предотвращение репликации специфичных атрибутов схемы на RODC

# RODC против злоумышленника

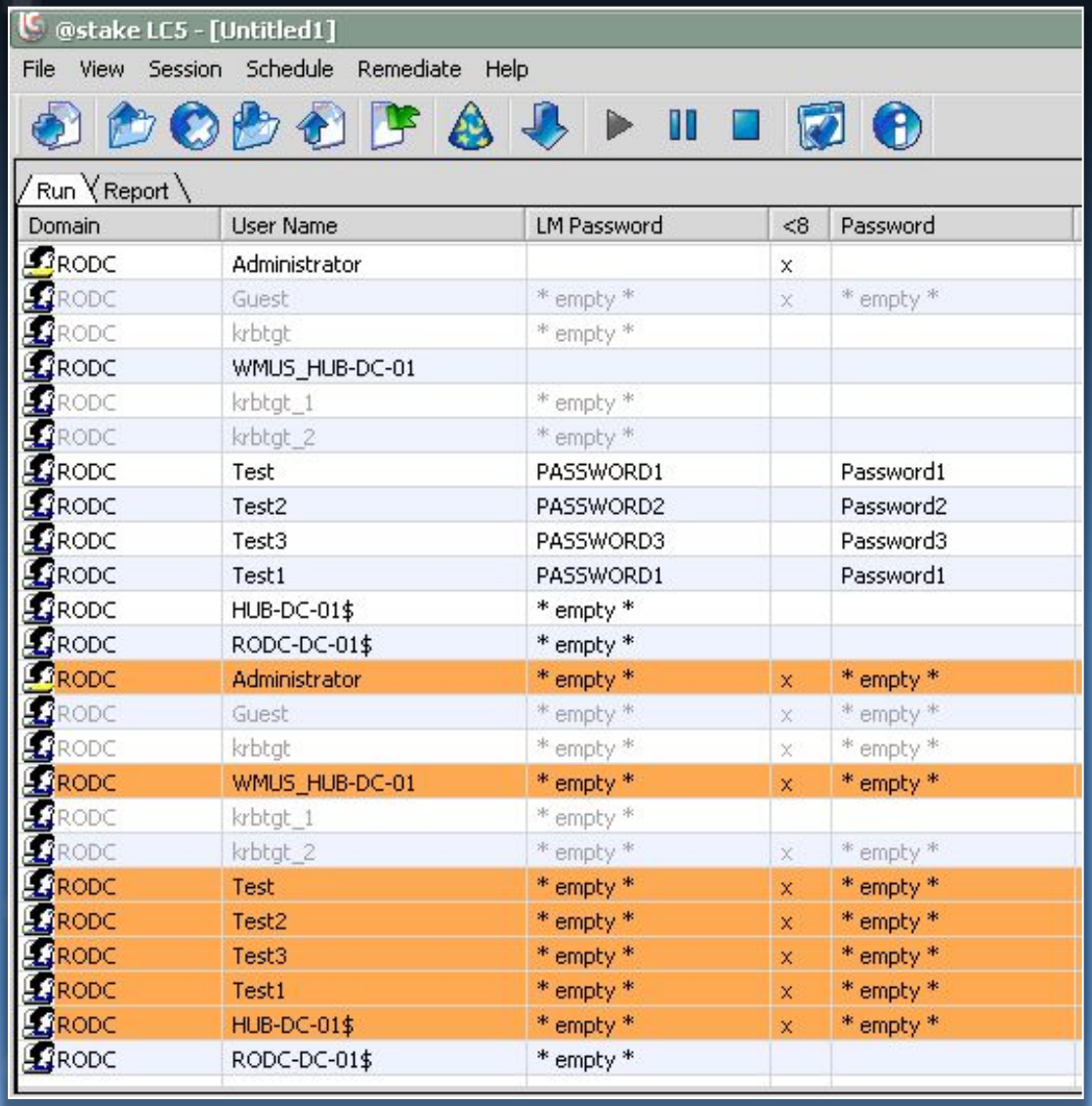
Давайте украдём RODC.

Злоумышленник

**По умолчанию, я не храню пароли, а так же специфичные атрибуты.**


RODC

# RODC против злоумышленника




| Domain | User Name | LM Password | <8 | Password |
|---|---|---|---|---|
| RODC | Administrator | | x | |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | | |
| RODC | WMUS_HUB-DC-01 | | | |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | | |
| RODC | Test | PASSWORD1 | | Password1 |
| RODC | Test2 | PASSWORD2 | | Password2 |
| RODC | Test3 | PASSWORD3 | | Password3 |
| RODC | Test1 | PASSWORD1 | | Password1 |
| RODC | HUB-DC-01$ | * empty * | | |
| RODC | RODC-DC-01$ | * empty * | | |
| RODC | Administrator | * empty * | x | * empty * |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | x | * empty * |
| RODC | WMUS_HUB-DC-01 | * empty * | x | * empty * |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | x | * empty * |
| RODC | Test | * empty * | x | * empty * |
| RODC | Test2 | * empty * | x | * empty * |
| RODC | Test3 | * empty * | x | * empty * |
| RODC | Test1 | * empty * | x | * empty * |
| RODC | HUB-DC-01$ | * empty * | x | * empty * |
| RODC | RODC-DC-01$ | * empty * | | |

# RODC против злоумышленника

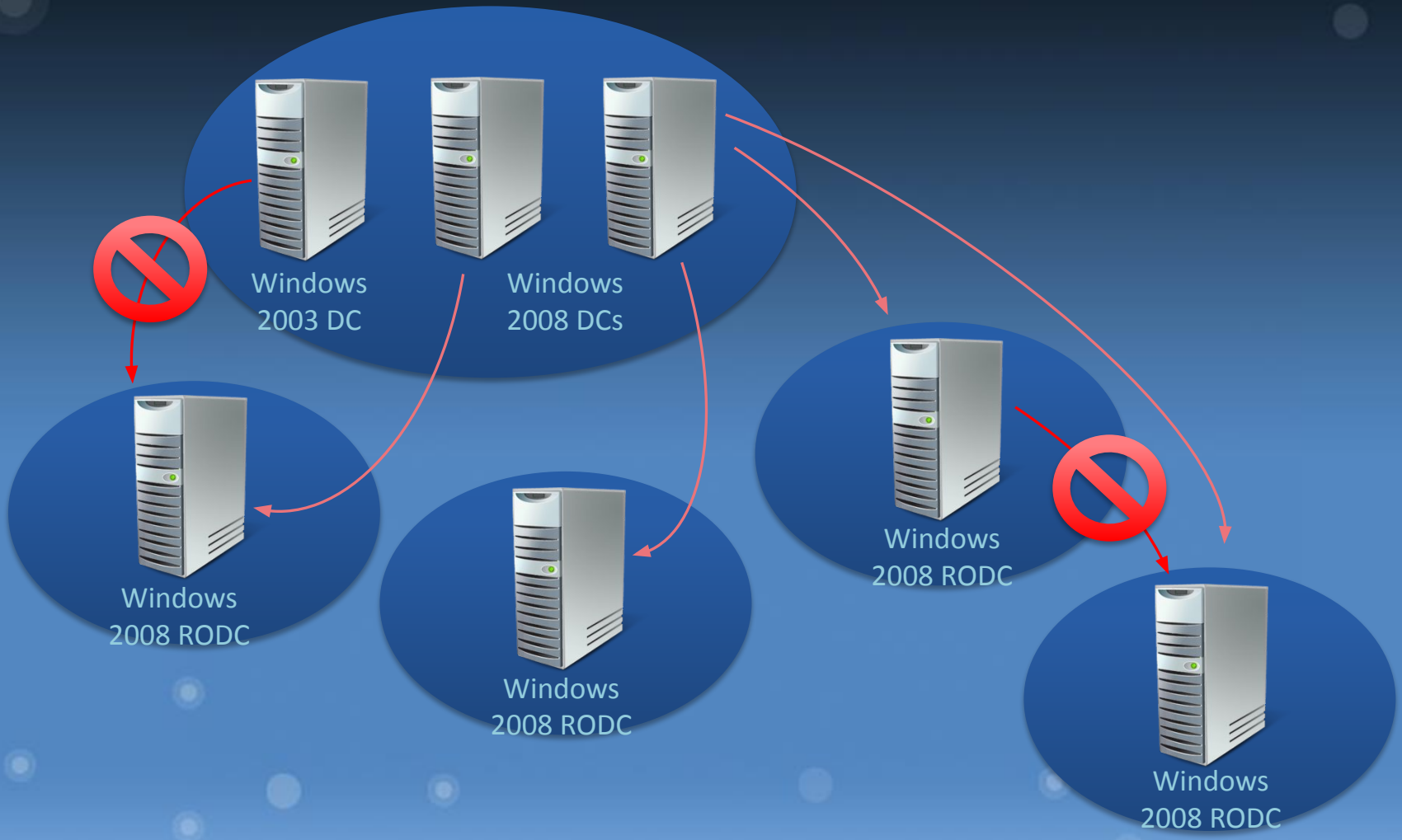
Добавим данные на RODC и используем его учётную запись.

Злоумышленник

**Моя база только для чтения, а другие контроллеры не реплицируют данные с меня.**

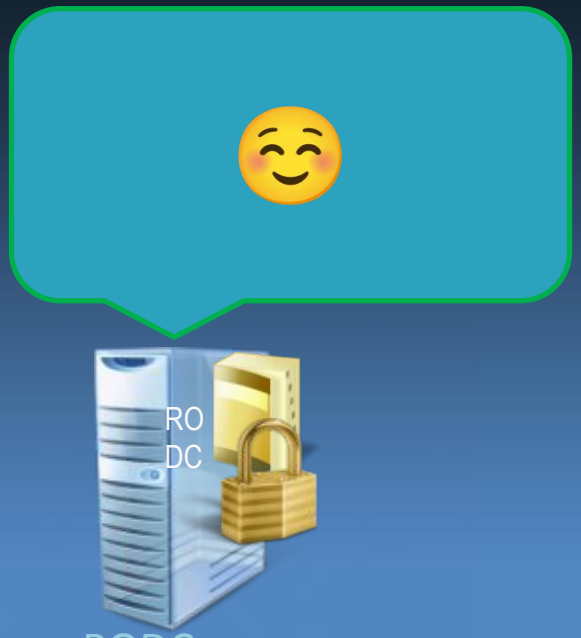

RODC

# RODC против злоумышленника



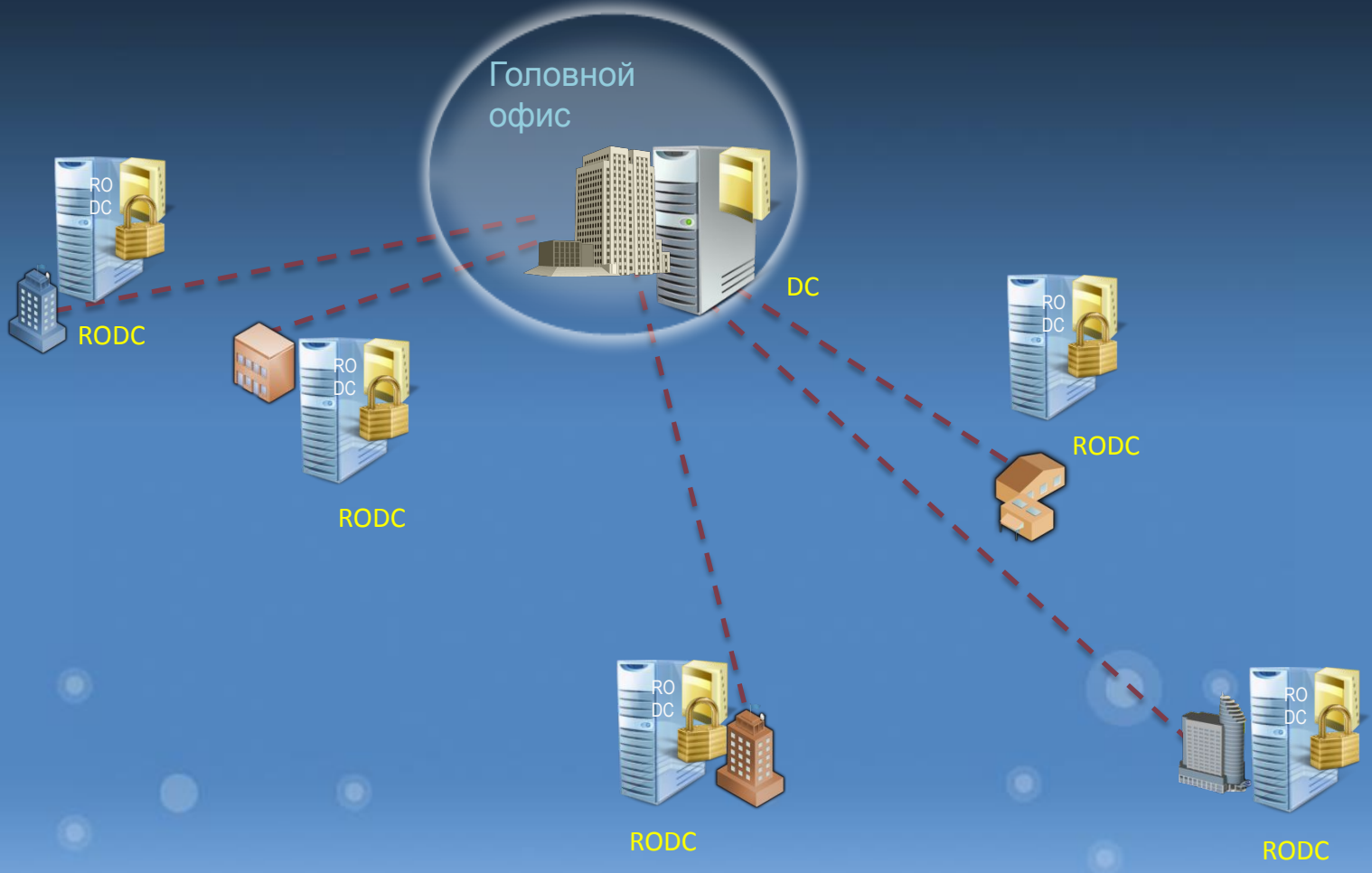
# RODC против злоумышленника


Злоумышленник




RODC

# Безопасные филиалы



# Варианты применения RODC

- **Пароли не хранятся** (по умолчанию)
  - **За**: Наиболее безопасно
  - **Против**: Никто не сможет работать, если WAN неисправен
- **Некоторые пароли хранятся**
  - **За**: Хороший баланс между безопасностью и непрерывной работой филиала
  - **Против**: Необходимо управлять хранением паролей
- **Большинство паролей хранится**
  - **За**: Простое управление паролями
  - **Против**: Малый выигрыш в безопасности, по сравнению с полноценным контроллером

# Демонстрация

## Установка и настройка RODC

Платформа 2009
0000000000001010

# Шифрование

- Физическая безопасность по-прежнему на низком уровне
- Кража учётных данных сотрудников филиала также не исключена
- На сервере, кроме Active Directory, хранятся и другие данные (возможно конфиденциальные)
- Было бы неплохо всё зашифровать!

# Виртуализация

- В целях...
  - сокращения количества серверов
  - изоляции задач
  - получения большей управляемости
  - сокращения затрат (особенно в условиях кризиса)

# Что это?

# Ключ шифрования в памяти!

Оригинальный ключ:

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 9C | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 30 | 00 | 00 | 00 | 9C | 00 | 00 | 00 |
| 00000010 | BA | 70 | 41 | D7 | 53 | 7E | 3C | 4A | 9A | 5B | B8 | E2 | F8 | A8 | 2F | 1C |
| 00000020 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | E0 | 25 | 28 | A9 | C0 | 56 | C9 | 01 |
| 00000030 | 6C | 00 | 06 | 00 | 09 | 00 | 01 | 00 | 92 | 54 | 23 | 43 | 69 | 37 | 7D | 42 |
| 00000040 | 82 | 5C | 55 | CA | 4A | 04 | B0 | F2 | 50 | 81 | F3 | A8 | C0 | 56 | C9 | 01 |
| 00000050 | 20 | 00 | 00 | 00 | 02 | 00 | 01 | 00 | 45 | 00 | 78 | 00 | 74 | 00 | 65 | 00 |
| 00000060 | 72 | 00 | 6E | 00 | 61 | 00 | 6C | 00 | 4B | 00 | 65 | 00 | 79 | 00 | 00 | 00 |
| 00000070 | 2C | 00 | 00 | 00 | 01 | 00 | 01 | 00 | 02 | 20 | 00 | 00 | 86 | 28 | 3F | 5F |
| 00000080 | 26 | 21 | 29 | 89 | 64 | A2 | D0 | 98 | D7 | BD | 1D | 40 | 4C | 8B | A0 | A5 |
| 00000090 | BE | 82 | B4 | C5 | CD | C5 | 1D | 2A | 2F | 36 | CC | 95 | | | | |

Дамп памяти:

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 04D3D270 | 18 | 00 | 59 | 00 | BA | 70 | 41 | D7 | 53 | 7E | 3C | 4A | 9A | 5B | B8 | E2 |
| 04D3D280 | F8 | A8 | 2F | 1C | D9 | 00 | 01 | 00 | E0 | 25 | 28 | A9 | C0 | 05 | 00 | 80 |
| 04D3D290 | 00 | 56 | C9 | 01 | 6C | 00 | 06 | 00 | 09 | 88 | 01 | 92 | 54 | 23 | 43 | 69 |
| 04D3D2A0 | 37 | 7D | 42 | 82 | 5C | 55 | CA | 4A | 04 | B0 | F2 | 50 | 81 | F3 | A8 | F9 |
| 04D3D2B0 | 00 | 20 | 58 | 01 | 54 | 05 | 00 | 00 | 02 | 00 | 01 | 00 | 45 | 00 | 78 | 00 |
| 04D3D2C0 | 74 | 00 | 65 | 00 | 72 | 00 | 6E | 00 | 61 | 00 | 6C | 00 | 4B | 58 | 00 | 79 |
| 04D3D2D0 | D8 | 00 | 2C | 18 | 00 | 01 | 08 | 00 | 02 | 40 | 01 | 86 | 28 | 03 | 00 | 00 |
| 04D3D2E0 | 00 | 3F | 5F | 26 | 21 | 29 | 89 | 64 | A2 | D0 | 98 | D7 | BD | 1D | 40 | 4C |
| 04D3D2F0 | 8B | A0 | A5 | BE | 82 | B4 | C5 | CD | C5 | 1D | 2A | 2F | 36 | CC | 95 | 50 |
| 04D3D300 | 01 | 07 | 00 | 0F | FF | 5E | 0F | FF | FF | FF | FF | 97 | 0D | 00 | 00 | 00 |

# Что делать?

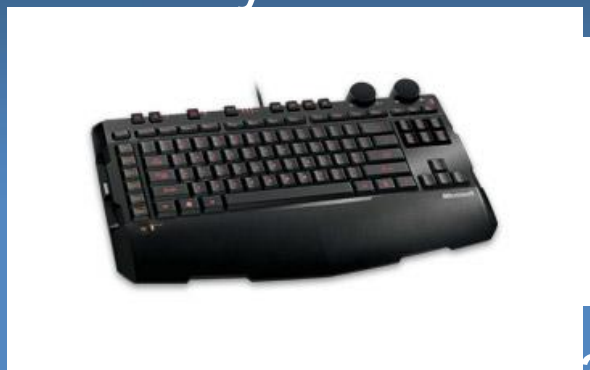
- Обследовать филиальную инфраструктуру
- Определить филиалы для внедрения RODC
- Внедрить BitLocker
- Использовать виртуализацию и ServerCore?

Вопросы?

# Не забывайте заполнять анкеты по докладам

## Ваше мнение очень важно!

1. Заполните анкету: http://platforma2009.ru/Eval.aspx
   Терминалы – холлы конференции и интернет-кафе на 1 этаже
2. Чтобы участвовать в розыгрыше призов



3. Результаты – на сайте конференции и в голосовых объявлениях после розыгрышей в 14:30, 16:00, 17:30 и 19:00

*Подробная информация по заполнению анкет – на сайте конференции*

Запись доклада на
www.platforma2009.ru