



31/05/2018

РОЛЕВАЯ МОДЕЛЬ МИФ ИЛИ РЕАЛЬНОСТЬ?

**Павел
Кудрин**

Руководитель разработки и внедрения прикладных решений
Центра информационной безопасности «Инфосистемы Джет»
pkudrin@jet.su / +7 926 700-95-92

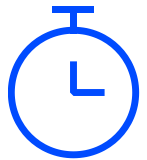
ТРЕБОВАНИЯ И ПОСТАНОВКА ЗАДАЧИ



Отказ от заявок



Полная автоматизация доступа

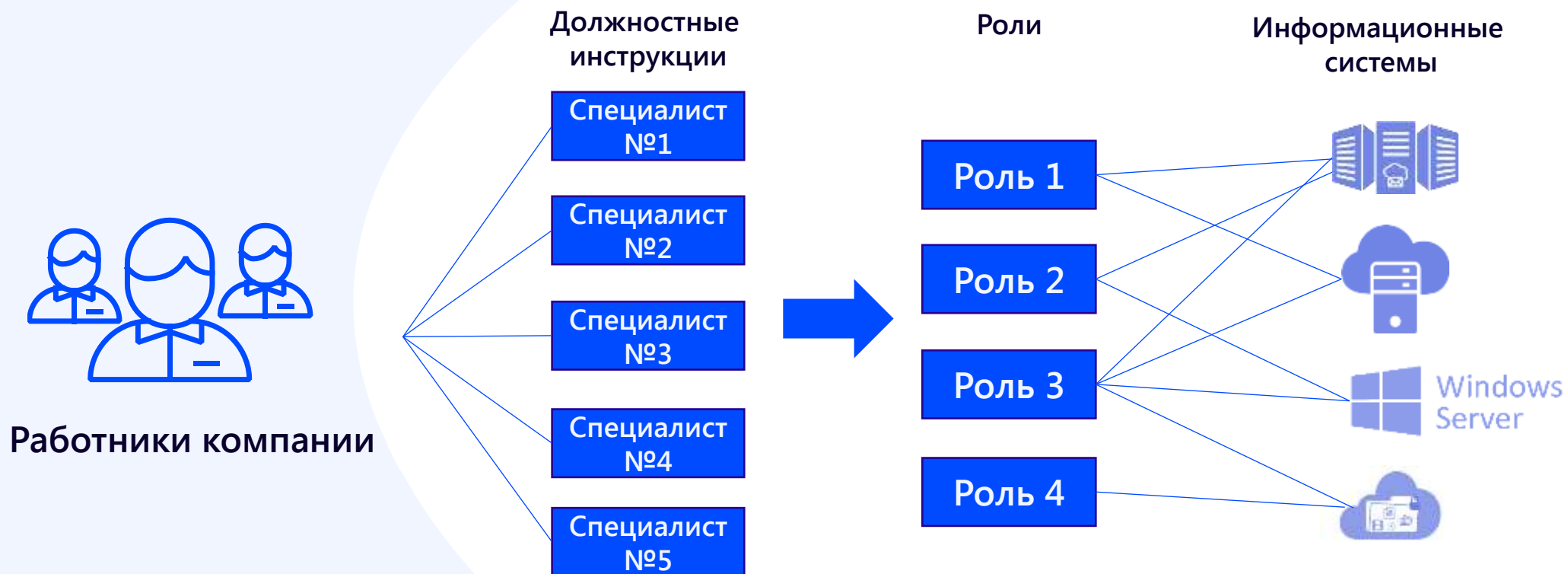


Сделать быстро



Без привлечения ресурсов клиента

ЧТО ЕСТЬ ИДЕАЛЬНАЯ РОЛЕВАЯ МОДЕЛЬ



! *Работники видят только те данные, которые им положено использовать*

ПОЧЕМУ НЕ ПОЛУЧАЕТСЯ ПОСТРОИТЬ ИДЕАЛЬНУЮ РОЛЕВУЮ МОДЕЛЬ



- Стабильный или прогнозируемый рынок**
- 100% обеспечение ресурсами**
- Полное соблюдение должностных инструкций**
- Безопасность важнее прибыли**

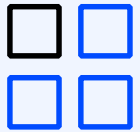
ЭТО НЕ ФАНТАСТИКА И ПРИМЕРЫ МОГУТ БЫТЬ



Некоммерческая структура



НИИ

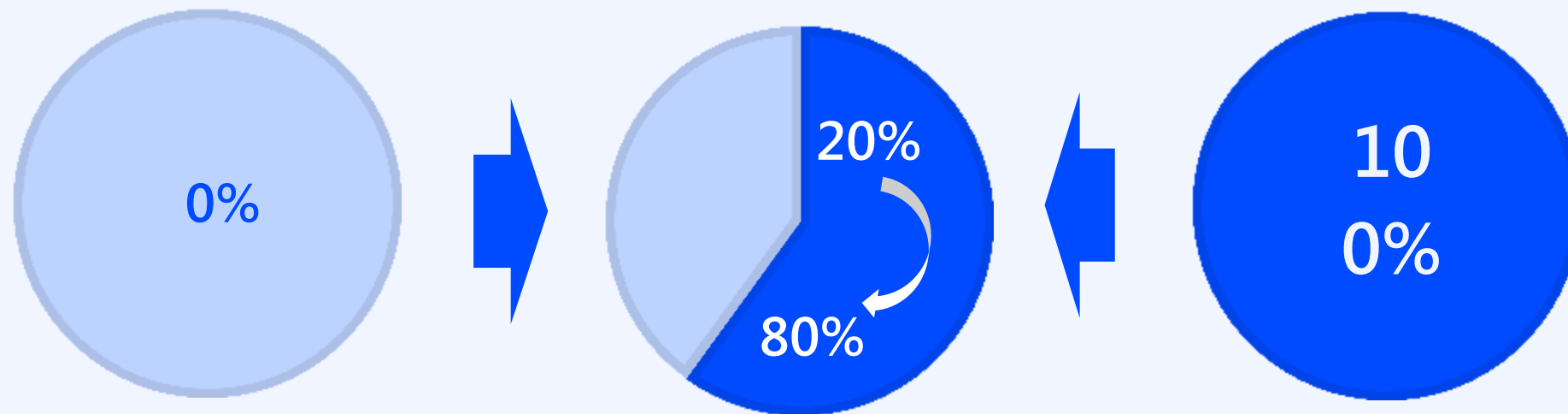


Выделенные подразделения в рамках крупной компании



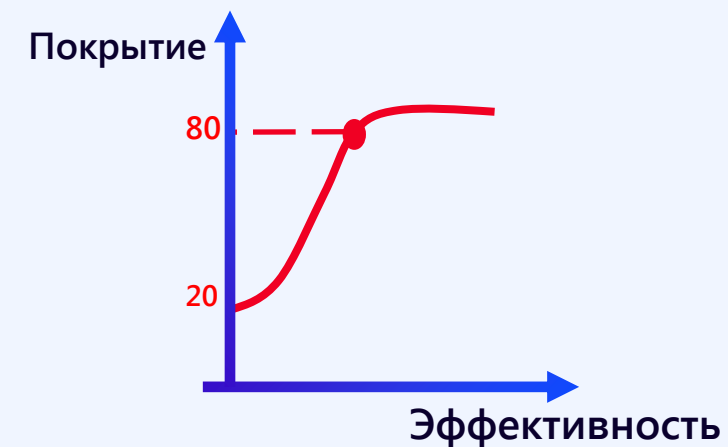
ВПК с высоким уровнем защищенности

ОПТИМАЛЬНАЯ РОЛЕВАЯ МОДЕЛЬ



Даже минимальная ролевая модель позволит:

- Автоматизировать базовый доступ до 100%
- Значительно сократить издержки
- Снизить риски ИБ



ПРАКТИКА РАЗРАБОТКИ РОЛЕВЫХ МОДЕЛЕЙ



Ручной анализ:



Собраться вместе: ИБ, ИТ, Бизнес



Выделить ИС, ИР,



Понять кто с чем должен работать



Разработать регламент и контроли



- 1. Нет ролей в ИС*
- 2. Очень много полномочий*
- 3. Нет специалистов*

ПРАКТИКА РАЗРАБОТКИ РОЛЕВЫХ МОДЕЛЕЙ



Технический анализ:



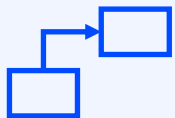
Анализ текущих полномочий и группировка ролей



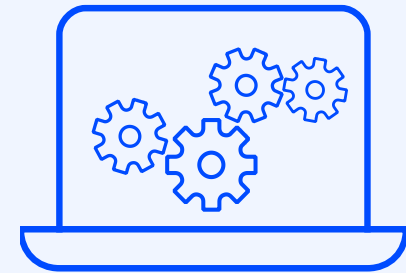
Назначение ответственных и аттестация ролей



Разработать регламент и контроли для обеспечения



Автоматизировать процесс назначения



ПРИМЕР ROLE MINING



The screenshot displays a software interface for role mining. The top menu includes 'Database', 'Analysis', and 'Help'. The main window is titled 'Employees [93]' and is divided into two main sections: 'Cluster' and 'Permissions [1 - 0]'. The 'Cluster' section on the left shows a tree view with 'Cluster analysis' and 'Role01'. The 'Employees' section on the right lists 30 employees with their names and IDs, and a 'Similarity' column represented by green bars. The 'Permissions' section at the bottom lists various system roles, with 'Domain Users' selected.

| Employee | Similarity |
|----------------------------------|------------|
| Aaghaa, Amari (AAGHAAA) | High |
| Aahil, Aamir (AAHIL.A) | High |
| Aaliyah, Abban (AALIYAHA) | High |
| Aalia, Agueda (AALAA) | High |
| Aalim, Alexa (AALAMA) | High |
| Aalok, Ahiga1 (AALOK.A) | High |
| Abagal, Ananya (ABAGAILA) | High |
| Abigal, A (ABIGAILA1) | High |
| Abigal, AB1 (ABIGAIL.A) | High |
| Adams, Alexander (ADAMSA) | High |
| Agent, Ann (AGENTA) | High |
| Agent, Anthony (AGENTA1) | High |
| Aguler, Alan (AGULARA) | High |
| Aktiv, Alfred (AKTIVA) | High |
| Allstar, Anna (ALLSTAR) | High |
| Alleva, Валентина (ALLENA.V) | High |
| BARANOVA, NATASHA (BARANOVA.N) | High |
| BARANOVA, SASHA (BARANOVA.S) | High |
| Doc, John (JOHND) | High |
| Александр, Иванов (AALEKSANDR.I) | High |
| Александр, Гусев (ALEKSANDR.G) | High |

Permissions [1 - 0]

- Domain Users
- Access Control Assistance Operators
- Account Operators
- Administrators
- Allowed RODC Password Replication...
- Backup Operators
- Cert Publishers
- Certificate Service DCOM Access
- Cloneable Domain Controllers
- Compliance Management
- Cryptographic Operators
- Delegated Setup
- Denied RODC Password Replication G...
- Discovery Management
- Distributed COM Users
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests

ИТОГО



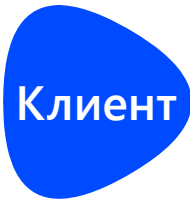
Отказаться не получится, но можно сократить до 80%



Полная автоматизация не получится, но она и не нужна



Можно быстро с оптимальным результатом



Потребуется ресурс заказчика

ГДЕ IDM ПОМОЖЕТ: УСКОРИТ И УПРОСТИТ



- Создать первоначальный доступ
- Пересмотр ролей (ресертификация)
- Автоматизация и контроль версий ролей
- Контроль на базе кадровых мероприятий
- Автоматическое назначение доступа



СПАСИБО ЗА ВНИМАНИЕ!

31/05/2018

**Павел
Кудрин**

Руководитель разработки и внедрения прикладных решений
Центра информационной безопасности «Инфосистемы Джет»
pkudrin@jet.su / +7 926 700-95-92