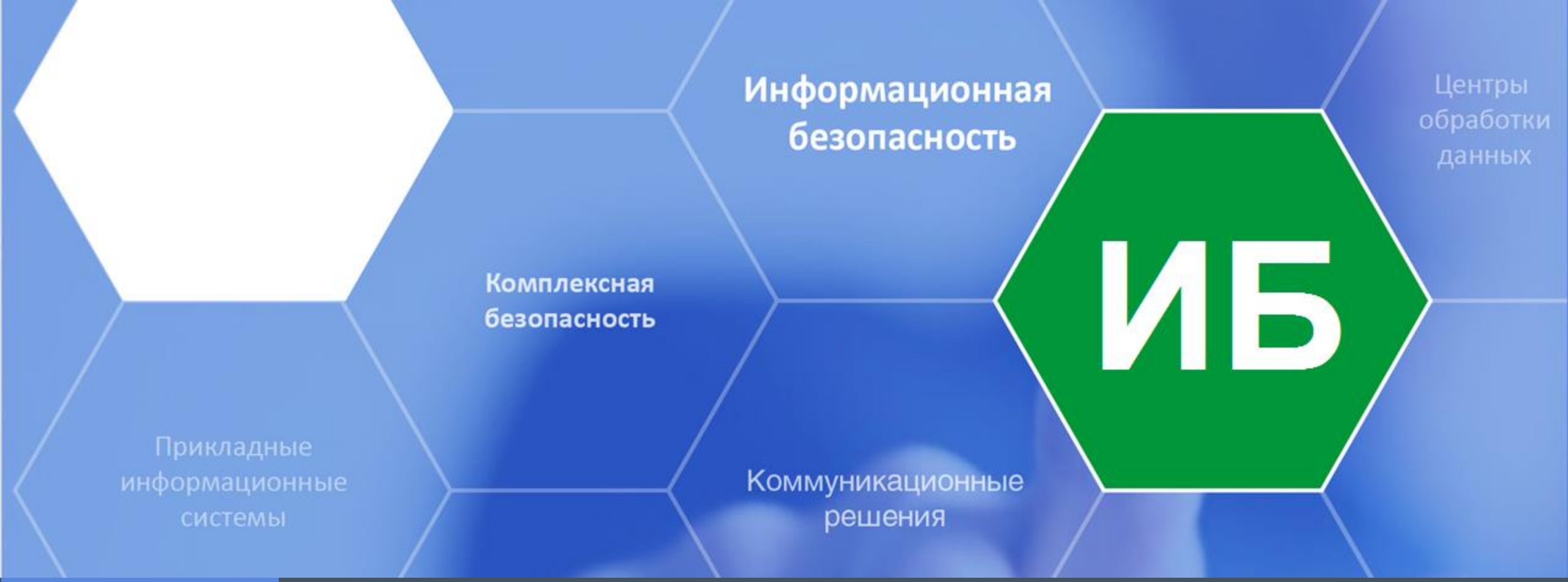


21.10.2021

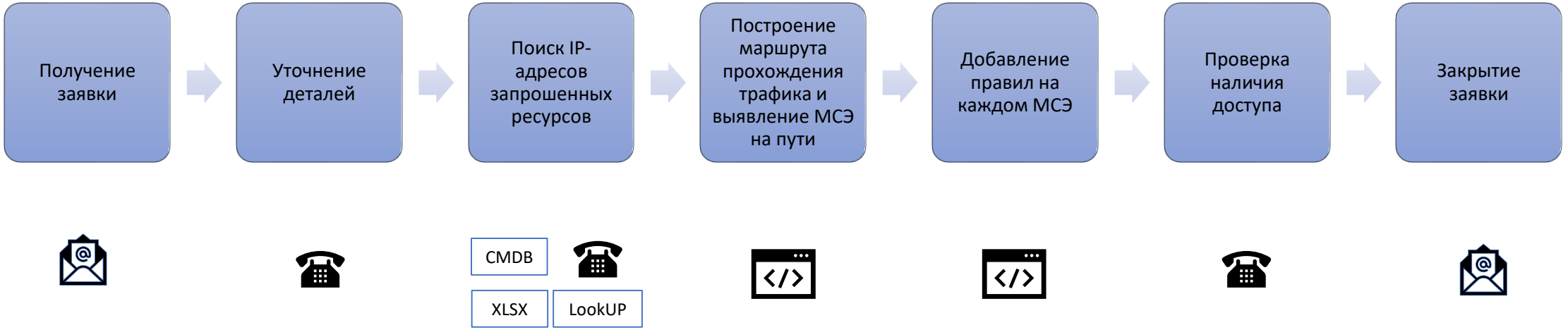
АМТ-ГРУП

Firewall Management или как открыть сетевой доступ за 60 секунд

План

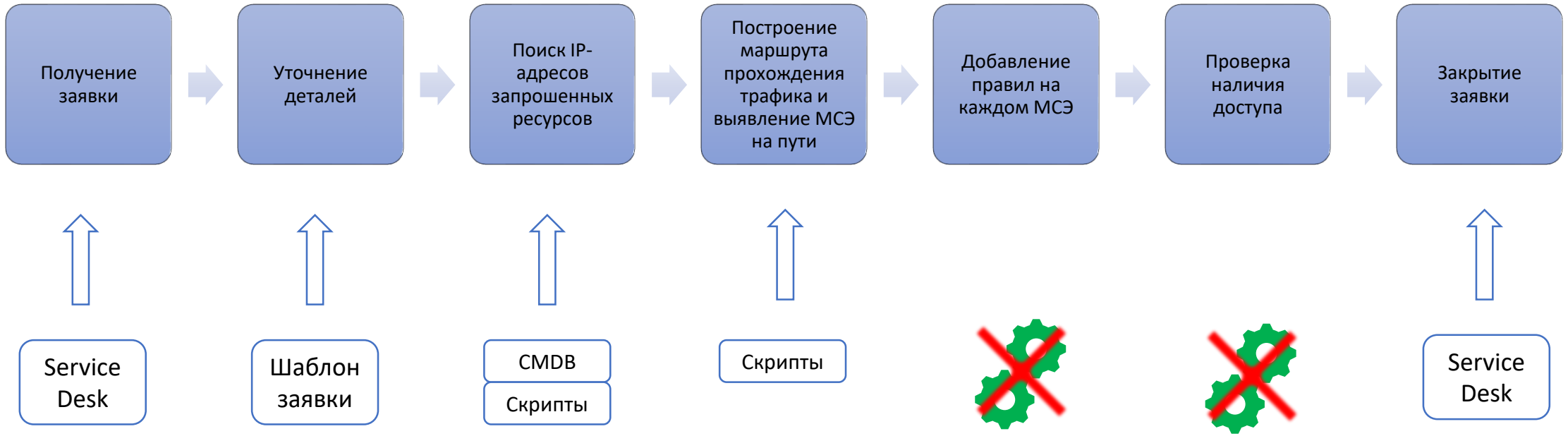
- Стандартный процесс открытия сетевого доступа
- А сколько времени это может занять?
- Частичная автоматизация операций
- Как можно улучшить процесс?
- Готовые решения Firewall Management и их состав
- Этапы внедрения Firewall Management решений
- Особенности управления доступом, найденные у Заказчика и результаты внедрения

Стандартный процесс открытия сетевого доступа



А сколько времени это может занять?

Частичная автоматизация процесса



Как можно улучшить процесс?

Автоматический этап

Автоматизированный этап

Готовые решения Firewall Management и их состав

- Firewall Analyzer
- AppViz
- Fireflow

- Network Assurance
- Change Manager
- Firewall Assurance
- Vulnerability Control

- SecureTrack
- SecureApp
- SecureChange

AMT GROUP

Этапы внедрения Firewall Management решений

1. Обследование/выявление сетевых устройств
2. Установка
3. Добавление сетевых устройств, постройка карты сети
4. Настройка процесса обработки заявок на открытие доступа
5. (skybox) Добавление информационных активов и подключение сканеров уязвимостей
6. (algosec/tufin) Добавление приложений
7. Использование

Особенности управления доступом, найденные у Заказчика

Особенность	Решение
❑ Сетевые администраторы не знали все устройства своей сети	Algosec автоматически обнаруживал неподключенные устройства
❑ Процесс управления сетевым доступом был слабо формализованы	По результатам работ процесс был доработан и реализован в Algosec
❑ Безопасность доступа оценивалась «на глаз»	Был внедрен формализованный этап оценки рисков доступа
❑ Доступ добавлялся, даже если уже был открыт ранее	Проверка «already works» отсеяла часть таких заявок
❑ Правила на МСЭ практически не удалялись	Algosec позволяет анализировать использование правил Для данного механизма был формализован процесс удаления правил

Результаты

- ✓~60% Правил на МСЭ были лишними
- ✓Снизилось число заявок за счет проверки already works (17% запрошенных доступов уже были открыты)
- ✓Добавился формализованный процесс оценки рисков
- ✓Была разработана и добавлена в Algosec ролевая модель для процесса управления доступом
- ✓Доступы, открываемые в обход стандартного процесса обработки заявок, стали автоматически обнаруживаться в Algosec
- ✓Среднее время на обработку заявок не изменилось за счет добавления новых операций
- ✓Рекордное время обработки заявки:
  - 1 минута на заявки already works;
  - 3 минуты для заявок с изменениями;

AMT GROUP