АЙТИБАСТИОН

www.it-bastion.com

2024

ПРАКТИКА ПОСТРОЕНИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ СКДПУ НТ И ШЛЮЗА БЕЗОПАСНОГО ОБЪЕДИНЕНИЯ СЕТЕЙ СИНОНИКС.

ШИРИКАЛОВ АЛЕКСЕЙ
Руководитель группы
Поддержки продаж

КОМПАНИЯ
АЙТИ БАСТИОН

2014

300+

ОСНОВАНИЕ КОМПАНИИ

Более 9 лет на российском рынке информационной безопасности

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

300+

250+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ

Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

250+

>70%

ЗАКАЗЧИКОВ И ПРОЕКТОВ

Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до геораспределенных площадок

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

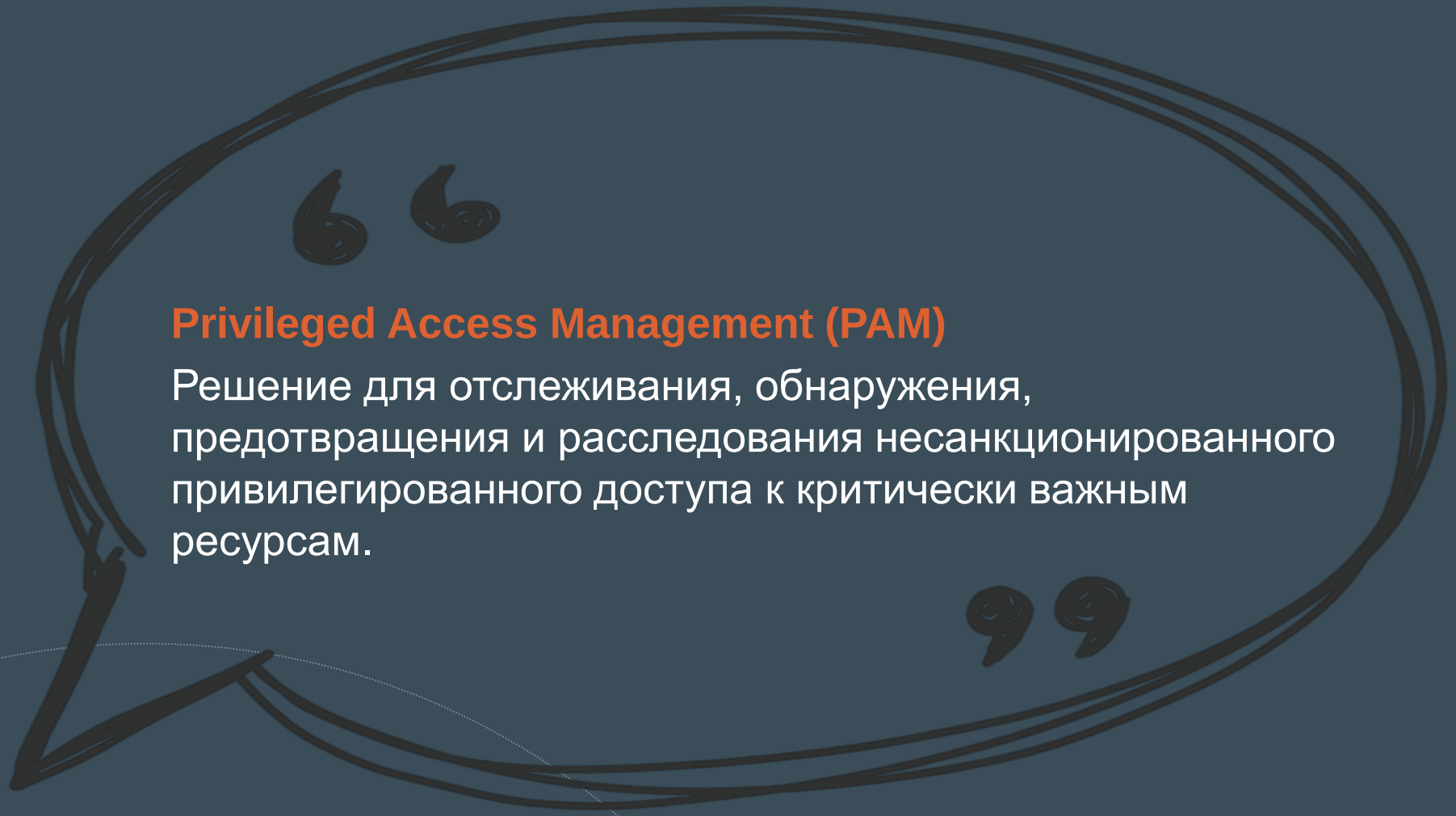
>70%

РАМ-РЫНКА РФ

Комплекс СКДПУ НТ решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

www.it-bastion.com

PAM



Privileged Access Management (PAM)

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам.

www.it-bastion.com

АЙТИБАСТИОН

АЙТИБАСТИОН

СКДПУ НТ

МА

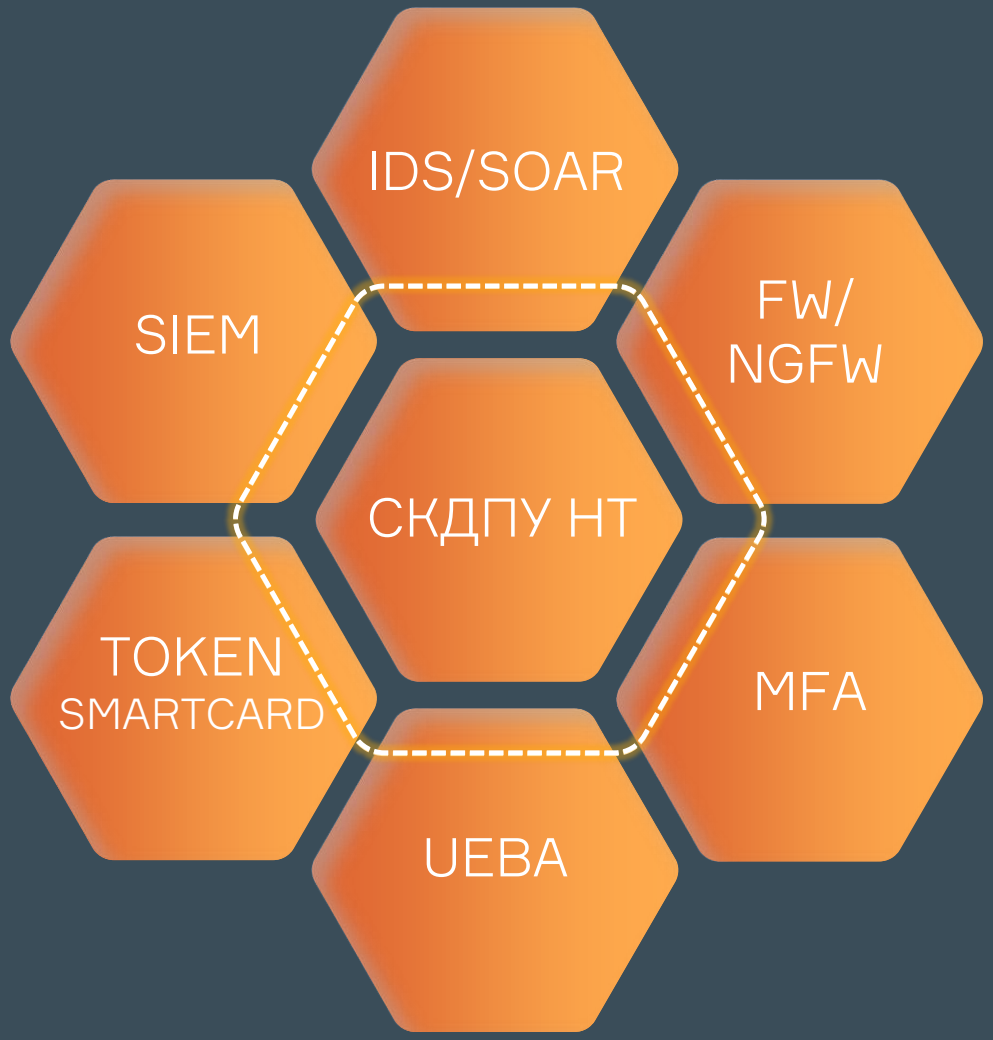
- Центр анализа
- Мониторинг
- Поведенческая модель
- Уровень доверия
- Инцидент
- Аномалии
- Отчетность

ШД

- Контроль доступа
- 2FA
- Профилирование
- Логирование
- Менеджер паролей
- Паттерны
- Видеозапись
- Политики доступа

www.it-bastion.com

АЙТИБАСТИОН



Платформенность

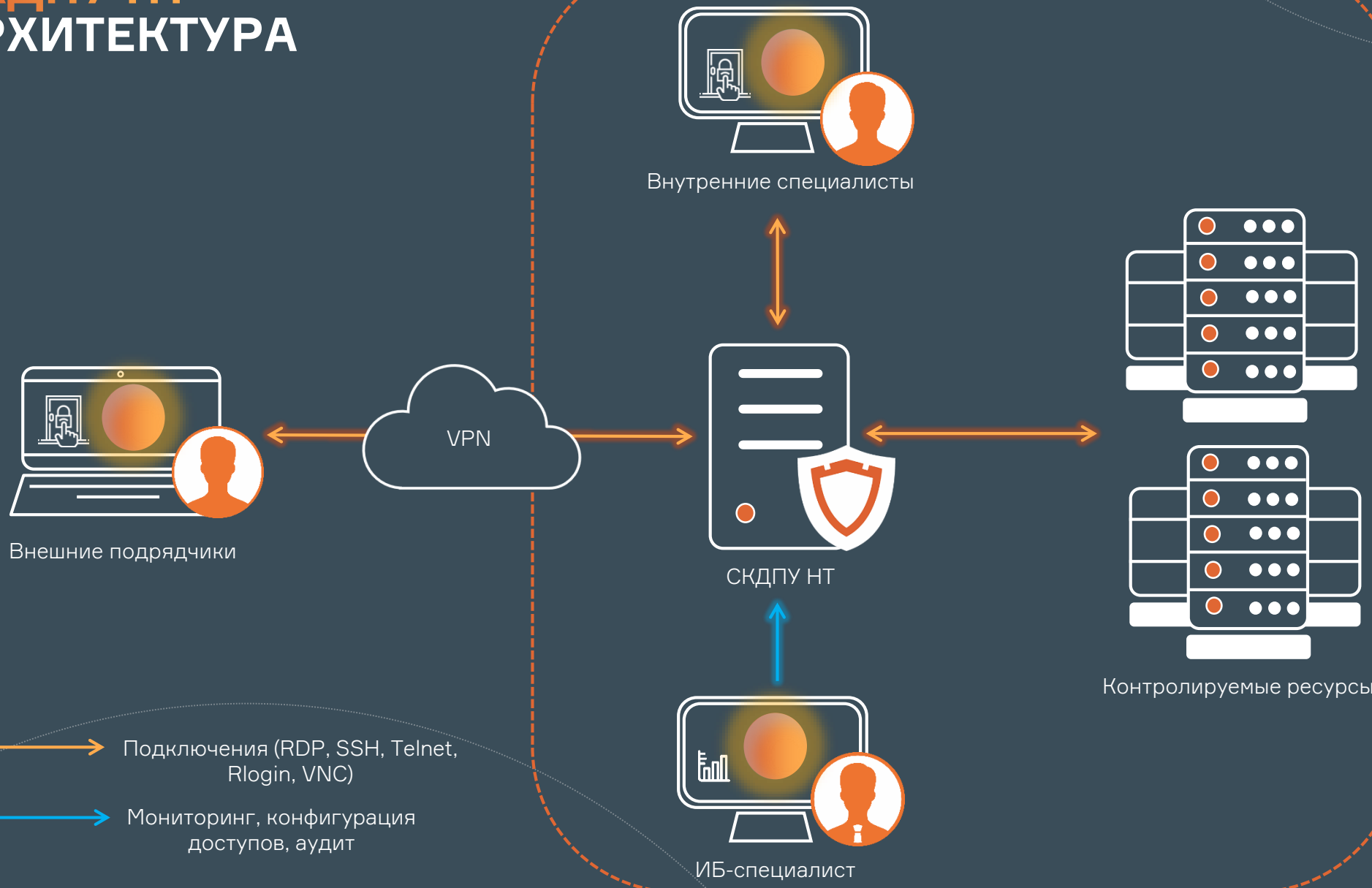
Обширная возможность интеграции с различными классами решений ИБ от лидеров рынка

КОГО КОНТРОЛИРУЕМ?

- ПОДРЯДЧИКОВ
- СИСТЕМНЫХ АДМИНИСТРАТОРОВ
- ИНЖЕНЕРОВ ВЕНДОРА
- АУДИТОРОВ

СКДПУ НТ
АРХИТЕКТУРА

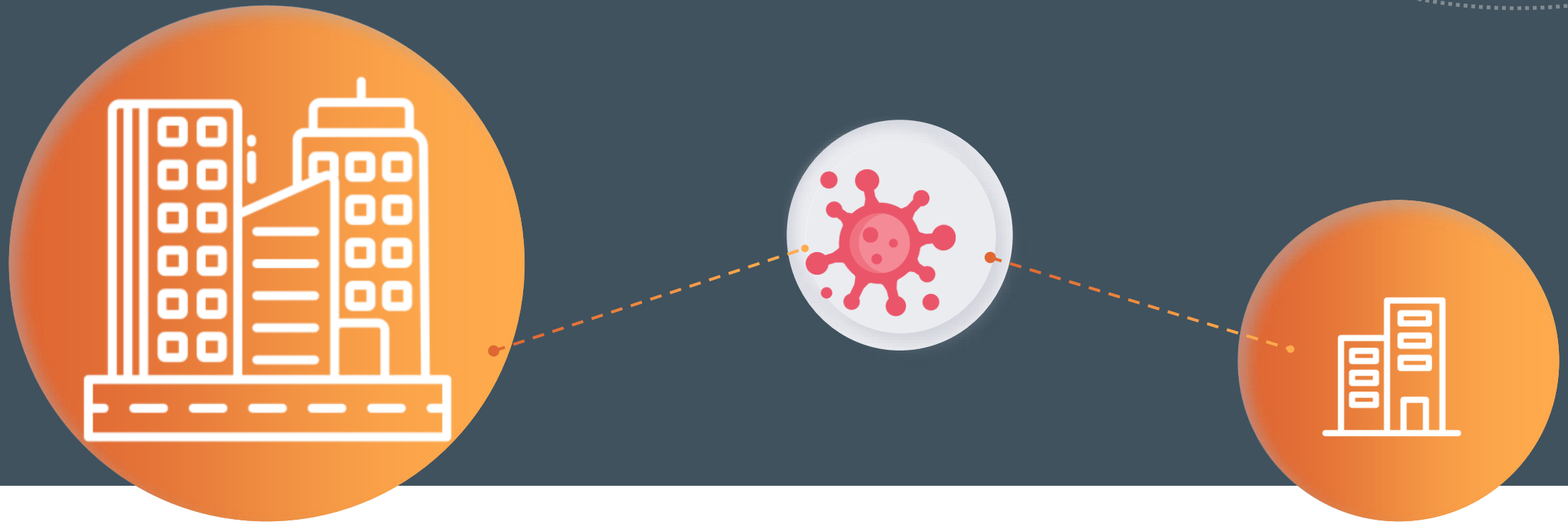
АЙТИБАСТИОН



www.it-bastion.com

АТАКИ
SUPPLY CHAIN

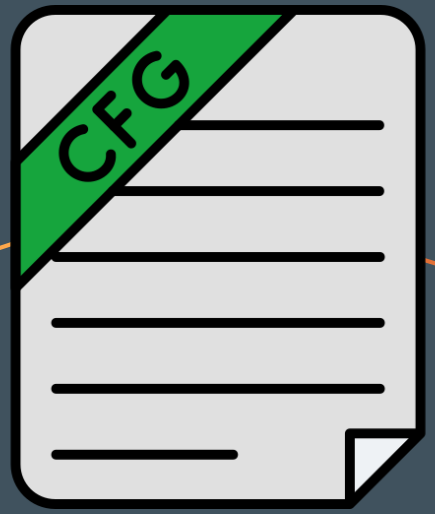
АЙТИБАСТИОН



NL-1093826	13-06-2023 13:45:02	[redacted]	Сканеры	Средний
CLM-1093819	13-06-2023 13:36:15	[redacted]	Подозрительные команды	Низкий

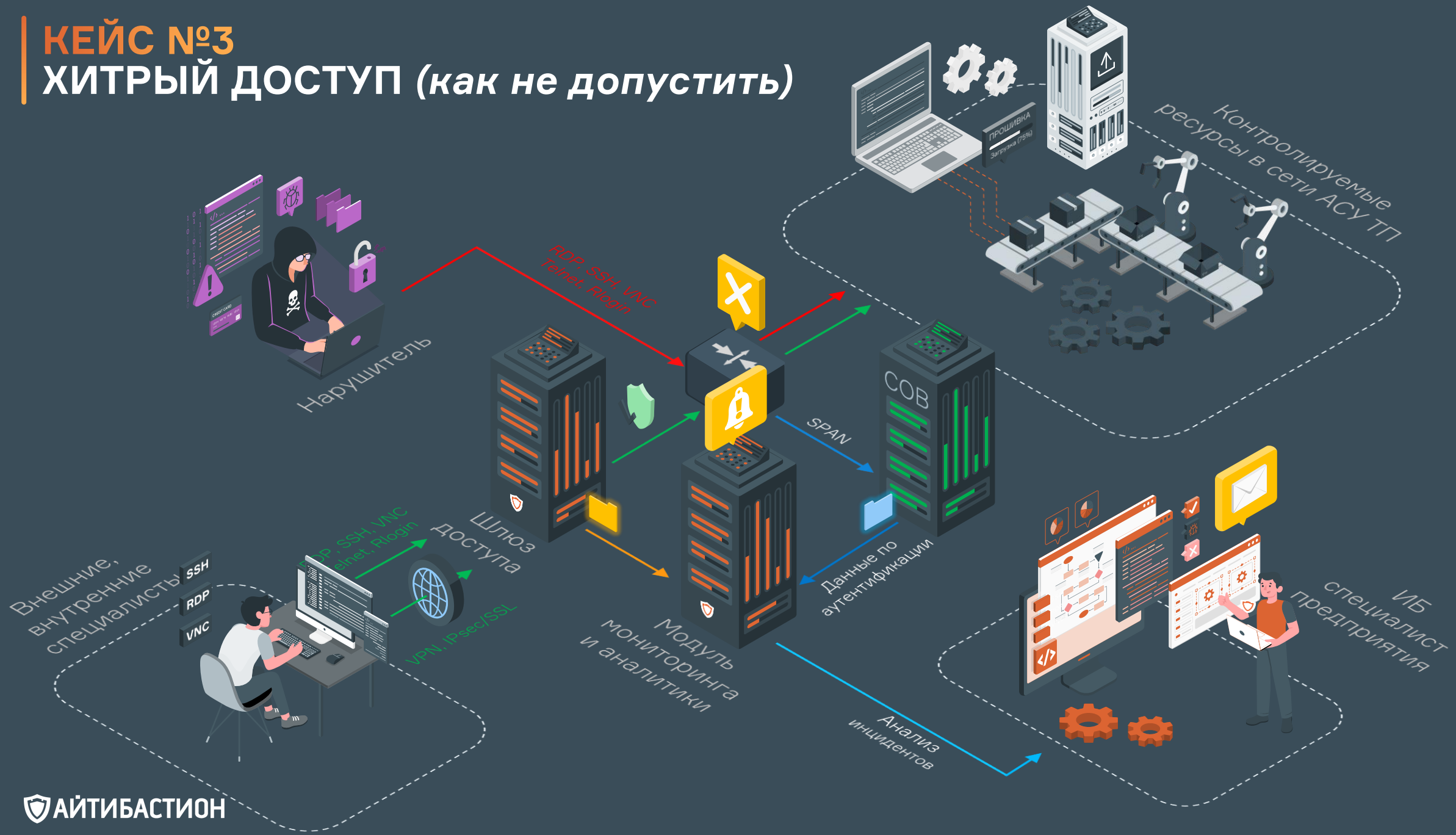
www.it-bastion.com

АТАКИ
SUPPLY CHAIN



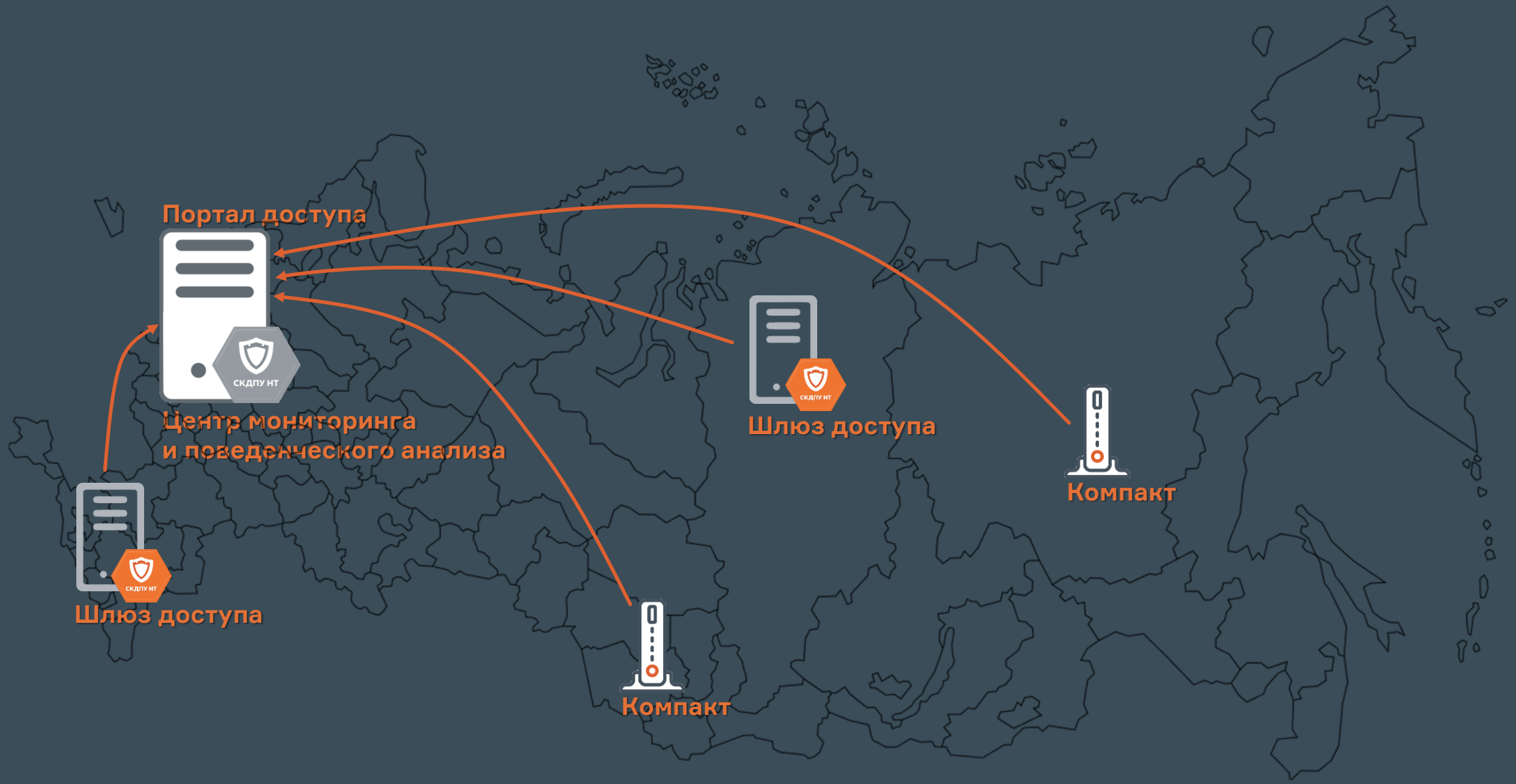
```
#                                   o means only IPv6 on loopback
# ac                                then 'enable' the firewall for
# the
IPV6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT.  Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="DROP"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"

# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
# manage the built-in chains too. Warning: setting this to 'yes' will break
# non-ufw managed firewall rules
```

КЕЙС №3
ХИТРЫЙ ДОСТУП (*как не допустить*)



АЙТИБАСТИОН

www.it-bastion.com


Портал доступа
СКДПУ НТ
Центр мониторинга
и поведенческого анализа
Шлюз доступа
СКДПУ НТ
Шлюз доступа
Компакт
Компакт

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

АЙТИБАСТИОН

Внешние, внутренние специалисты

VPN, IPsec/SSL

www.it-bastion.com

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

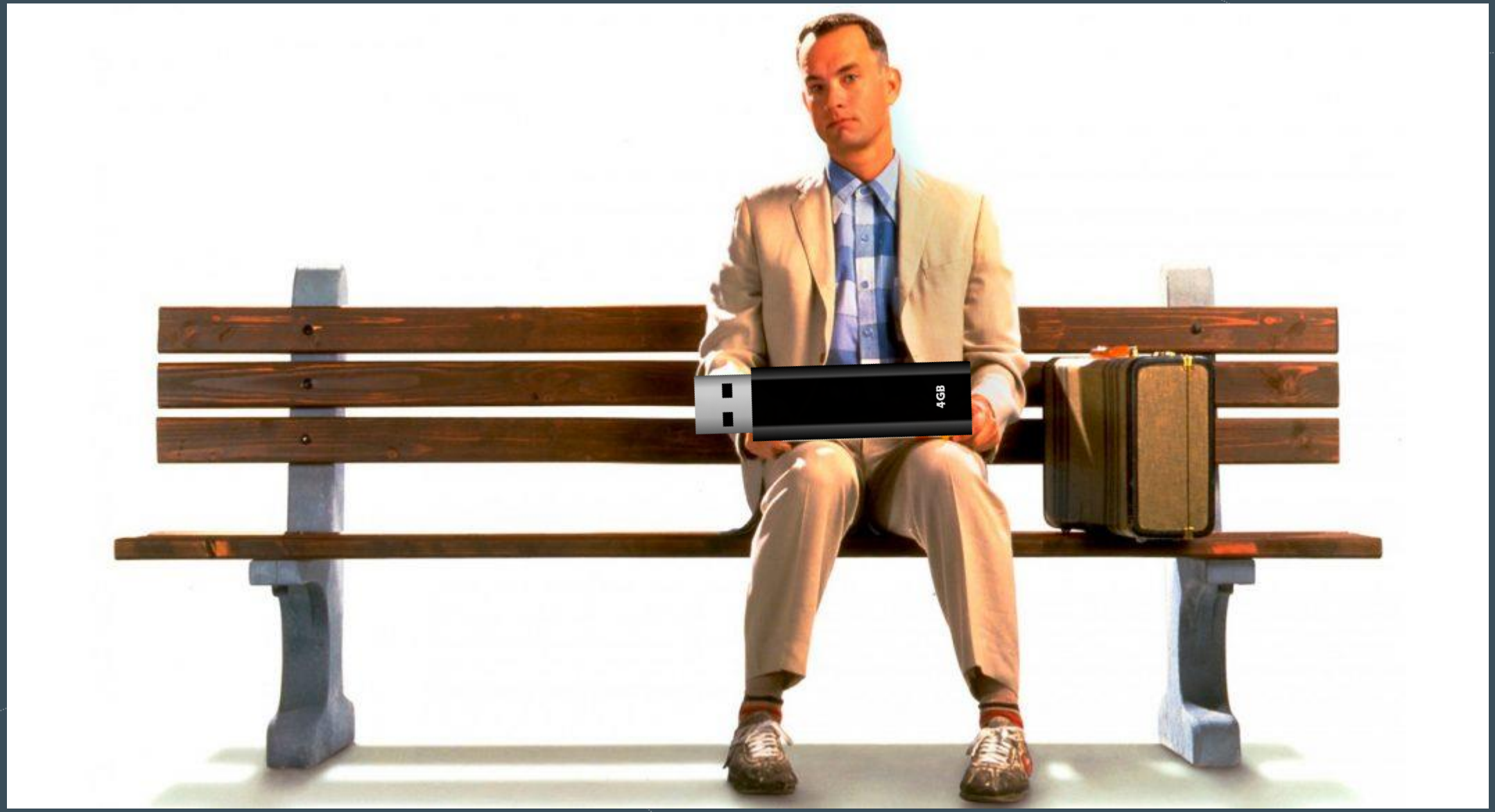
АЙТИБАСТИОН

Передача в контур

Обновление
Настройка
Базы
Файлы
Иные данные

Внешние, внутренние специалисты

www.it-bastion.com


4GB

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СЕТЯХ

АЙТИБАСТИОН

Передача из контура

Телеметрия

Логи

Базы

Иные данные

Внешние, внутренние специалисты

www.it-bastion.com

«Особенности» изолированных сетей

- ТРУДОЗАТРАТЫ
- ВРЕМЯ
- БЕЗОПАСНОСТЬ
- АКТУАЛЬНОСТЬ

СИНОНИКС

АЙТИБАСТИОН

•Изолирует сети. Сети остаются невидимыми друг для друга.

•Ограничивает количество взаимодействующих систем.

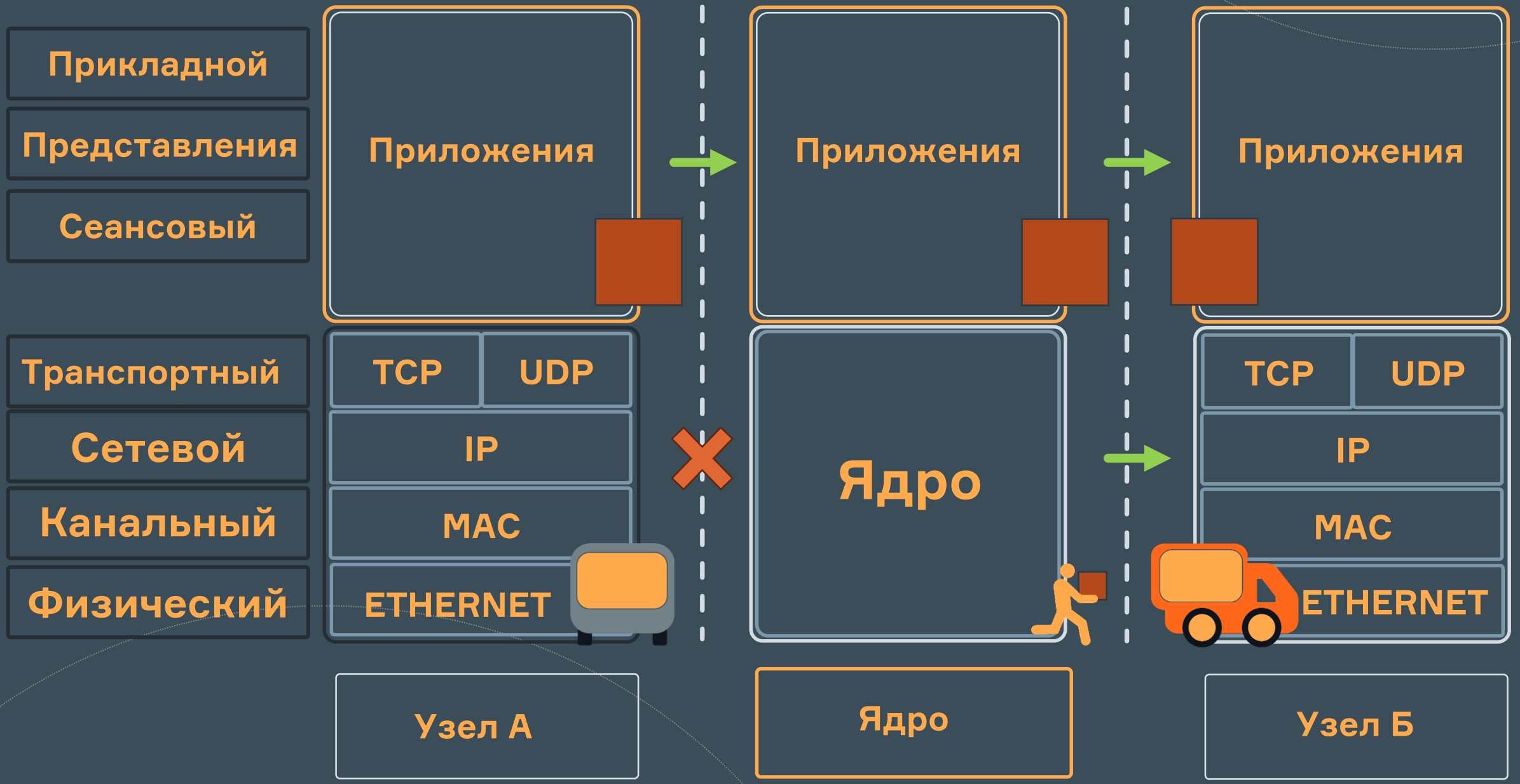
•Проверка сертификата.

•Согласование правил между сетями.

•Дополнительная физическая блокировка.

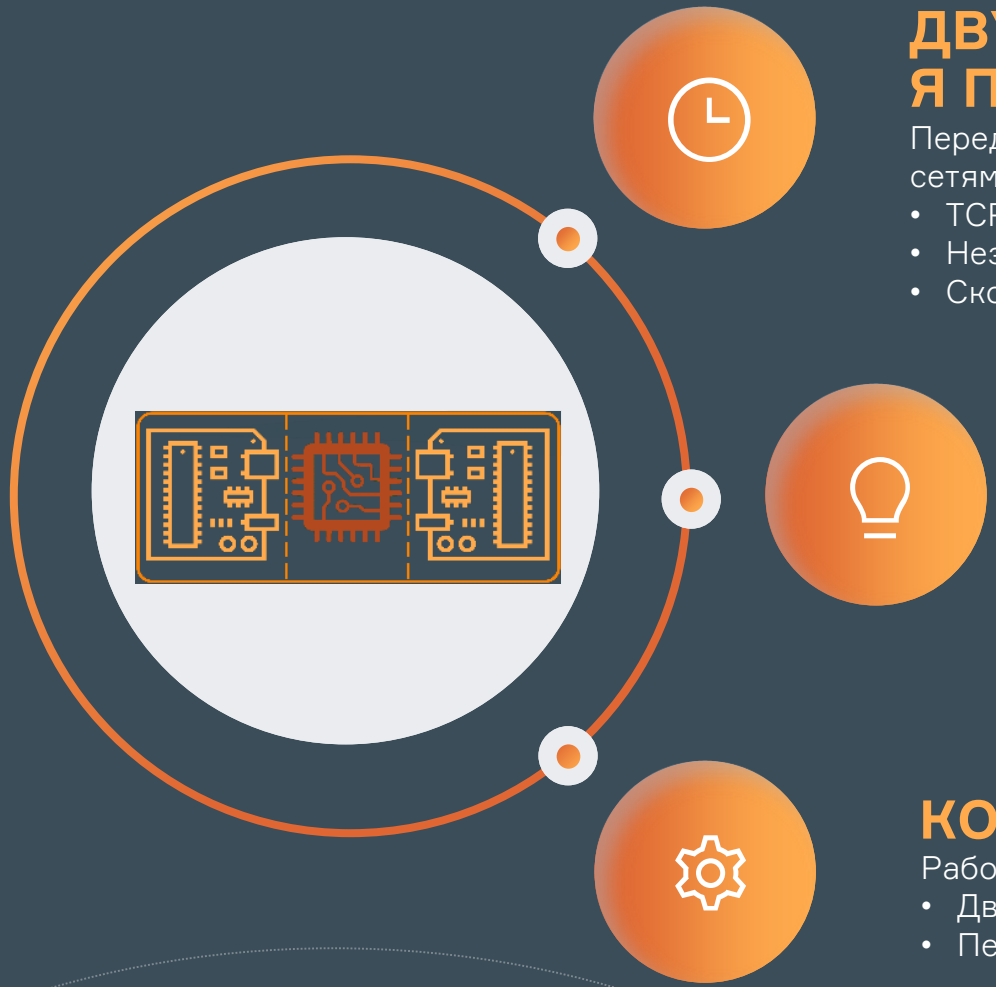
•Нейтрализует сетевые атаки на 1 - 4 уровнях семиуровневой модели OSI.

www.it-bastion.com



СИНОНИКС
ВОЗМОЖНОСТИ

АЙТИБАСТИОН



ДВУНАПРАВЛЕННАЯ/ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА

Передача данных между изначально ИЗОЛИРОВАННЫМИ сетями.

- TCP, UDP
- Независимые политики для двух контуров
- Скорость до 1 Гб/с

ПЕРЕДАЧА ФАЙЛОВ

Передача файлов между изначально ИЗОЛИРОВАННЫМИ сетями с дополнительными правилами проверки файлов на соответствие политикам передачи.

- SFTP
- Выбор направления передачи (A->B, A<-B, A<->B)
- Проверка маски, ЭЦП
- Внешняя валидация по ICAP (DLP, Sandbox, AV и др.)

КОМБИНИРОВАННЫЙ РЕЖИМ

Работа в обоих режимах:

- Двунаправленная передача данных
- Передача файлов

www.it-bastion.com

Механизм передачи

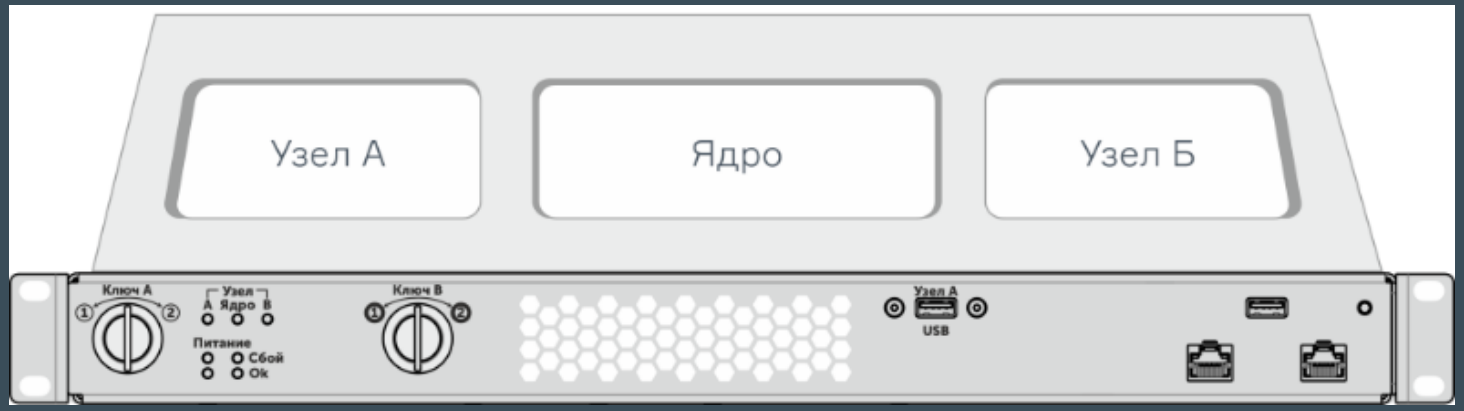
АЙТИБАСТИОН

01

Доступ к управлению – через консоль соответствующей сети.

Доступ к ядру системы ограничен пломбами и доп. контролем.

Контроль запуска
Работа каждого узла контролируется физически.



02

Передача данных определяется путем установки правила для СЛОТА передачи:

Указания IP источника и Порта назначения, на который придут данные.
Указание IP назначения и Порта, куда требуется передавать данные.

03

Передача файлов

1. Профиль передачи – стороны определяют тип проверки файлов ДО передачи (маска, ЭЦП).
2. Правила передачи – определяет направление с А на Б, с Б на А или в обе,.
3. Пользователь – определяет пользователя, который может подключиться для передачи.

АЙТИБАСТИОН

Внешние, внутренние специалисты

www.it-bastion.com

АЙТИБАСТИОН

Благодарю за внимание!

ШИРИКАЛОВ АЛЕКСЕЙ

a.shirikalov@it-bastion.com

+7 499 322 3667

it-bastion.com