

DECK

**Контроль за сетевыми подключениями
при помощи dot1x и не только?
Уже сегодня? Как?**

Хаванкин Максим
mkhavank@deck.lc

Факты о DECK.AUTH

- Архитектура и кодовая база DECK.AUTH развиваются начиная с 2014 года
- DECK - постоянный участник конференции Cisco Connect с 2014 года
- DECK.AUTH отлично справился с высокой нагрузкой во время ЧМ 2018 для аутентификации на различных объектах
- DECK.AUTH внесен в реестр отечественного ПО в 2020 году



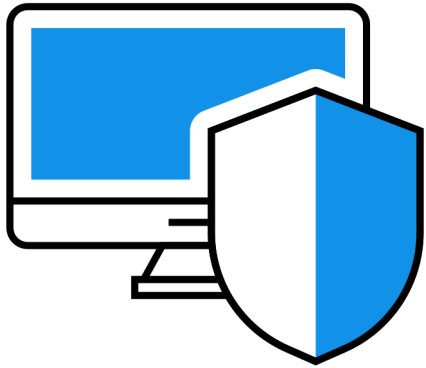
Запись в реестре №6091 от 13.01.2020 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.01.2020 №4

Класс программного обеспечения по классификатору программного обеспечения, утвержденному приказом от 31.12.2015 № 621

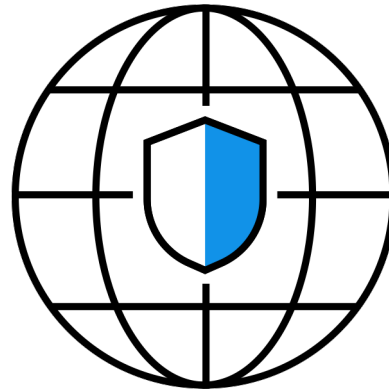
Основной класс:

02.07 Серверное и связующее программное обеспечение

Комплексный подход к обеспечению безопасности



Защита рабочего
места сотрудника



Защита
подключения



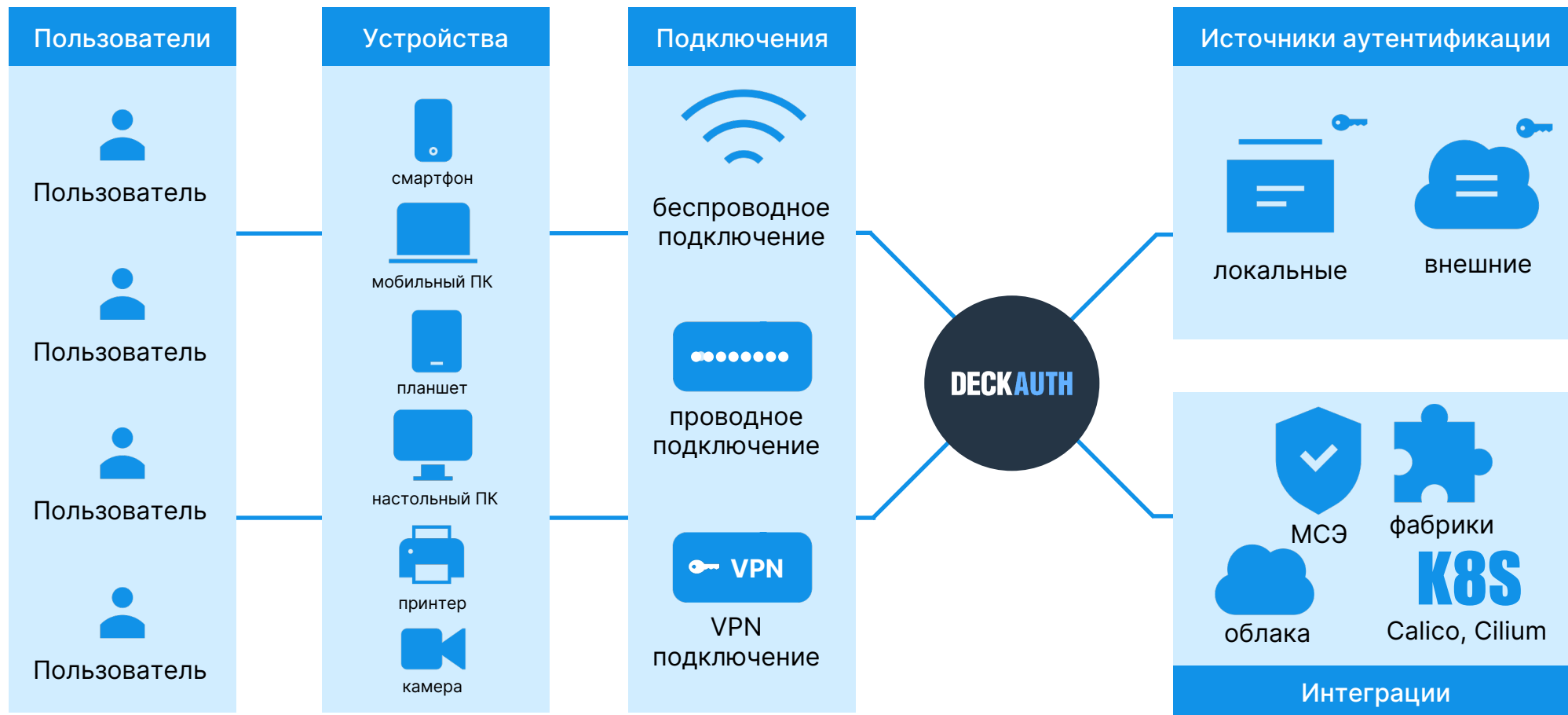
Защита
приложения

Представляем DECK AUTH



Система управления политиками для проводных, беспроводных и VPN-подключений с поддержкой 802.1x и RADIUS

Общая архитектура системы



Гостевой доступ

Управление организацией гостевого доступа



Сценарии реализации гостевого доступа в организации

Базовый сценарий

- Идентификация гостей и их подключение к Интернет при помощи беспроводной сети в зонах публичного доступа
 - Посетители
 - Конференции, выставки, семинары, обучение

Расширенный сценарий

- Гранулярная идентификация гостей в беспроводных и проводных сетях
 - Подрядчики
 - Контракторы
 - Временные сотрудники
- Без увеличения количества SSID

Примеры реализации гостевого доступа

- Базовый сценарий



- Расширенный сценарий
 - Один SSID



Гостевой доступ на 100%



- **Задача**

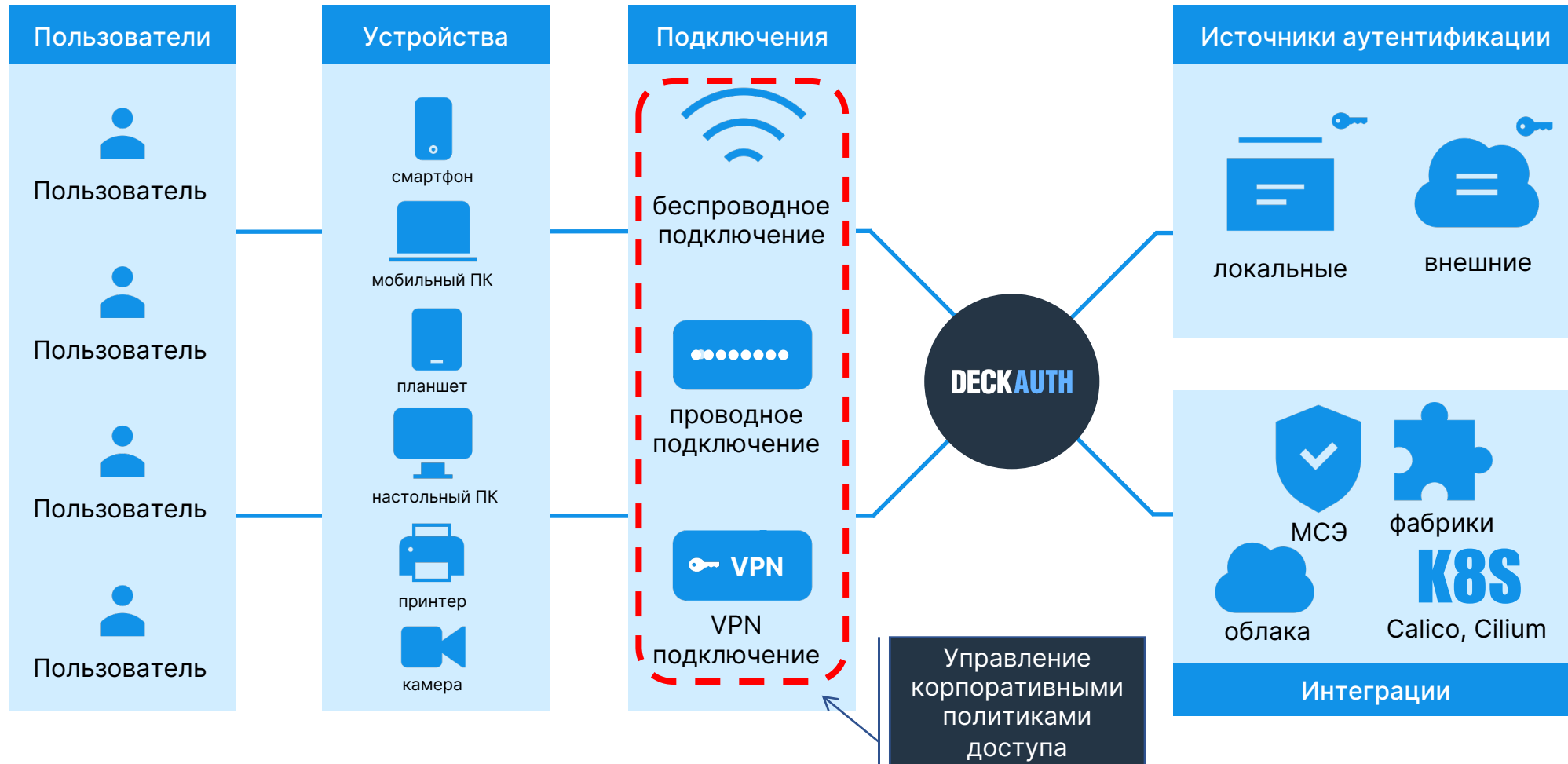
- Идентификация пользователей беспроводных сетей согласно Ф3 и постановлений Правительства РФ
- Реализация контролируемого подключения гостей, партнеров и подрядчиков к проводной и беспроводной сети организации

- **Решение**

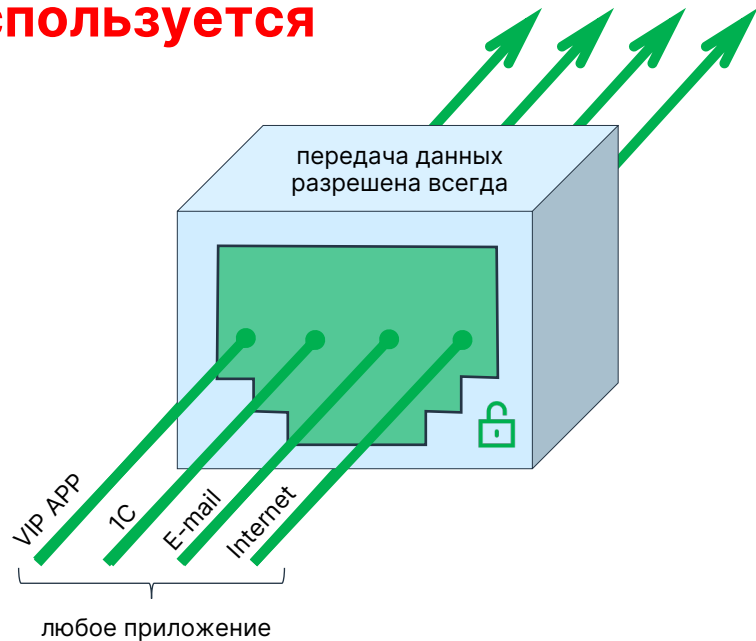
- Гибкие методы идентификации пользователей включая ЕСИА, рассылку СМС и ваучеры
- Конструктор captive-портала для индивидуального стилового оформления
- Поддержка широкого спектра сетевых устройств

Корпоративные политики на основе dot1x

Управление организацией политик на основе dot1x

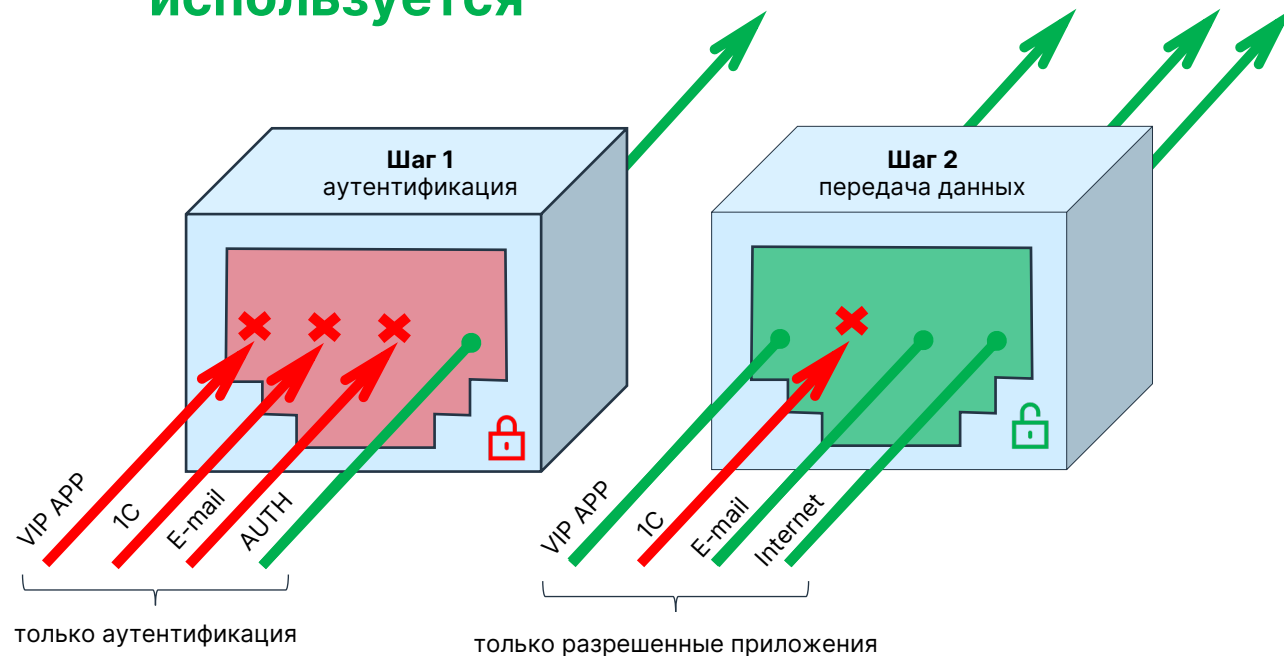


Контроль доступа на основе dot1x **не** используется



- Сеть всегда готова передавать данные **без аутентификации**
- К сети в любом момент подключается **любое** устройство и пользователь
- Физически подключения **никак не контролируются**
- Никаких ограничений на подключение не накладывается – если пользователь имеет физическое соединение, то он может попробовать подключиться **к любому приложению**

Контроль доступа на основе dot1x **используется**



- Сеть всегда готова передавать данные **только после аутентификации**
- К сети **может попытаться** подключиться любое устройство или пользователь
- Все подключения **контролируются** DECK AUTH при помощи процесса аутентификации
- По результатам аутентификации на возможности подключения к приложениям **могут быть** наложены ограничения на уровне сети

Сценарии реализации политик доступа на основе dot1x в организации

Базовый сценарий

- Идентификация «свой/чужой»
- Отдельное управление гостями

Расширенный сценарий

- Гранулярная идентификация (группы)
- Авторизация - доступность сетевых ресурсов и приложений в зависимости от группы

Примеры реализации сегментации

Базовый сценарий



Расширенный сценарий



Сегментация и управление политиками

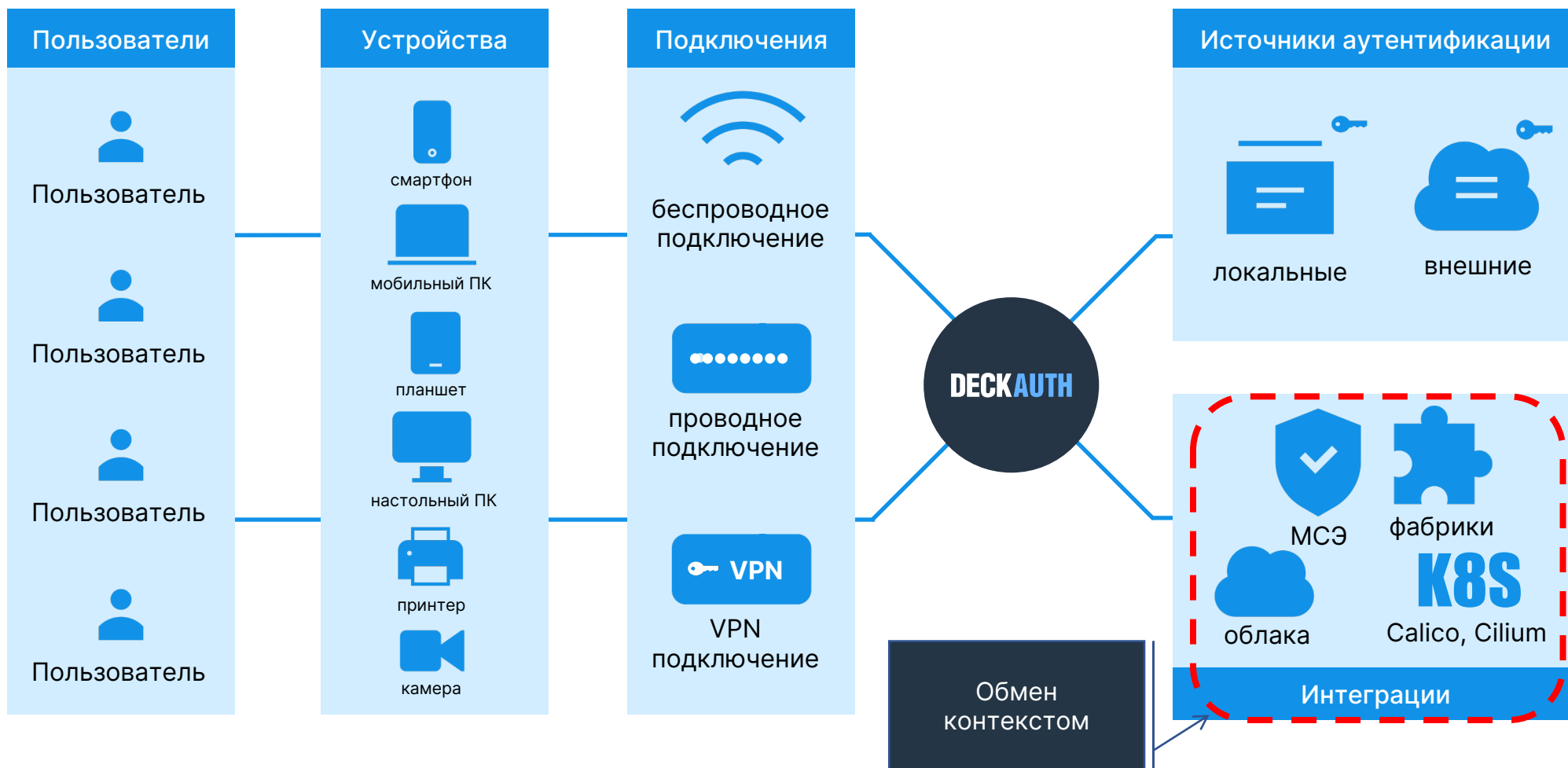


- Задача
 - Сегментация на основе бизнес-правил
 - Контроль за подключениями к сети передачи данных
 - Уменьшение зоны доверия при помощи автоматизации
- Решение
 - Использование существующей сетевой инфраструктуры с поддержкой Radius – нет необходимости в дорогостоящих обновлениях сетевого оборудования
 - Широкий спектр источников информации для идентификации
 - Интуитивно понятный конструктор политик аутентификации и авторизации
 - Гибкость в определении и назначении политик авторизации

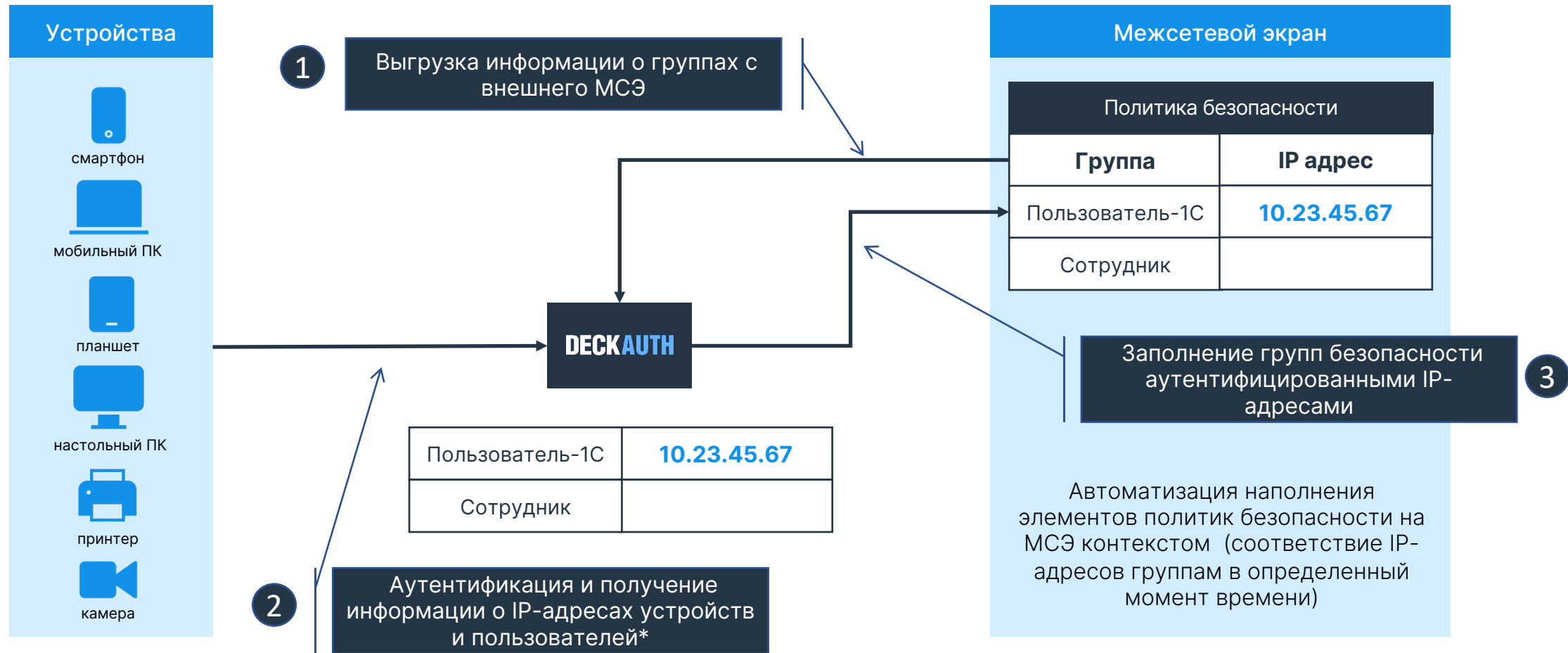
The background of the slide is a dark blue field filled with a complex, wavy pattern of small, light blue dots. These dots are arranged in concentric, overlapping circles and lines that create a sense of depth and movement, resembling a digital or network visualization.

**Интеграция с существующей
инфраструктурой ИТ и ИБ**

Интеграция



Интеграция с внешними системами ИТ и ИБ



* требуется поддержка со стороны AAA-подсистемы оборудования, которое выполняет аутентификацию

Мультивендорное решение с инновационными интеграциями

- Технологическая нейтральность для 802.1x и RADIUS



- Органично вписывающиеся в архитектуру системы инновационные интеграции
 - МСЭ
 - Сетевые фабрики
 - Публичные облака
 - CNI-плагины для K8S

Почему DECK AUTH?

- Мультивендорное решение с инновационными интеграциями
- В отличие от конкурентов, в ядре системы мы не стремимся сделать кальку с западных решений, а опираясь на опыт делаем лучше!
- Предсказуемое и последовательное развитие продукта, без попытки «объять необъятное»



DECK

<https://auth.deck.lc>