



РОСАТОМ

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

## **Актуальные проблемы и решения инфраструктуры открытых ключей в атомной отрасли**

Ольшаников Алексей Владимирович

PKI-Forum 2018





Анализ больших данных (big data)



Искусственный интеллект



Интернет вещей (IoT)



Технология «Блокчейн»



Виртуальная реальность



Дополненная реальность



Нейроинтерфейсы



Аддитивные технологии



Роботы



Облачные технологии

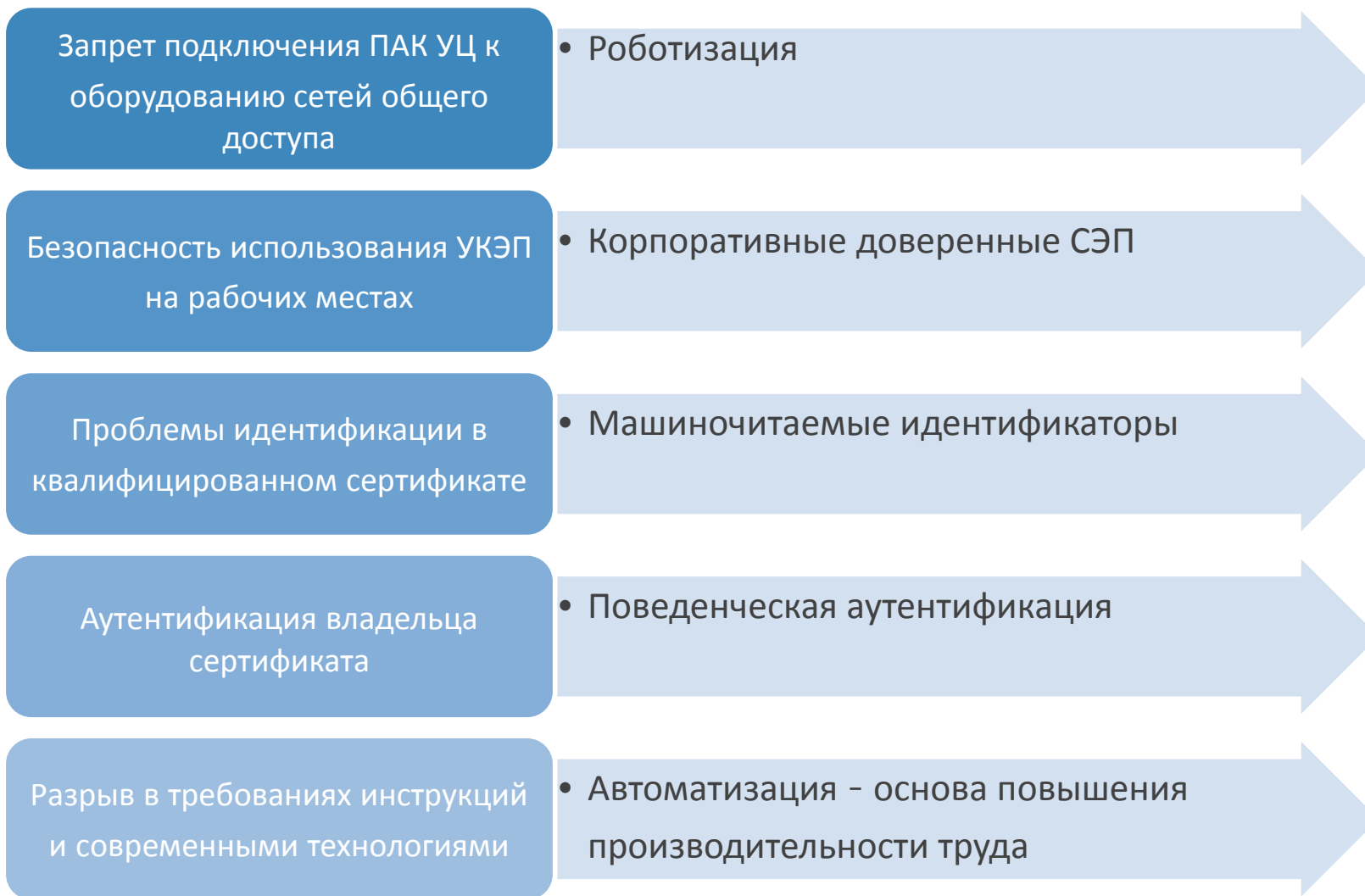


Датчики (сенсоры)



Беспилотные устройства





Приказ ФСБ РФ от 27 декабря 2011 г. N 796  
"Об утверждении Требований к средствам электронной подписи и  
Требований к средствам удостоверяющего центра"

35. При подключении средств УЦ к информационно телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса КВ2 или КА1.

## Вариант 1

Сохранить подключение средств УЦ

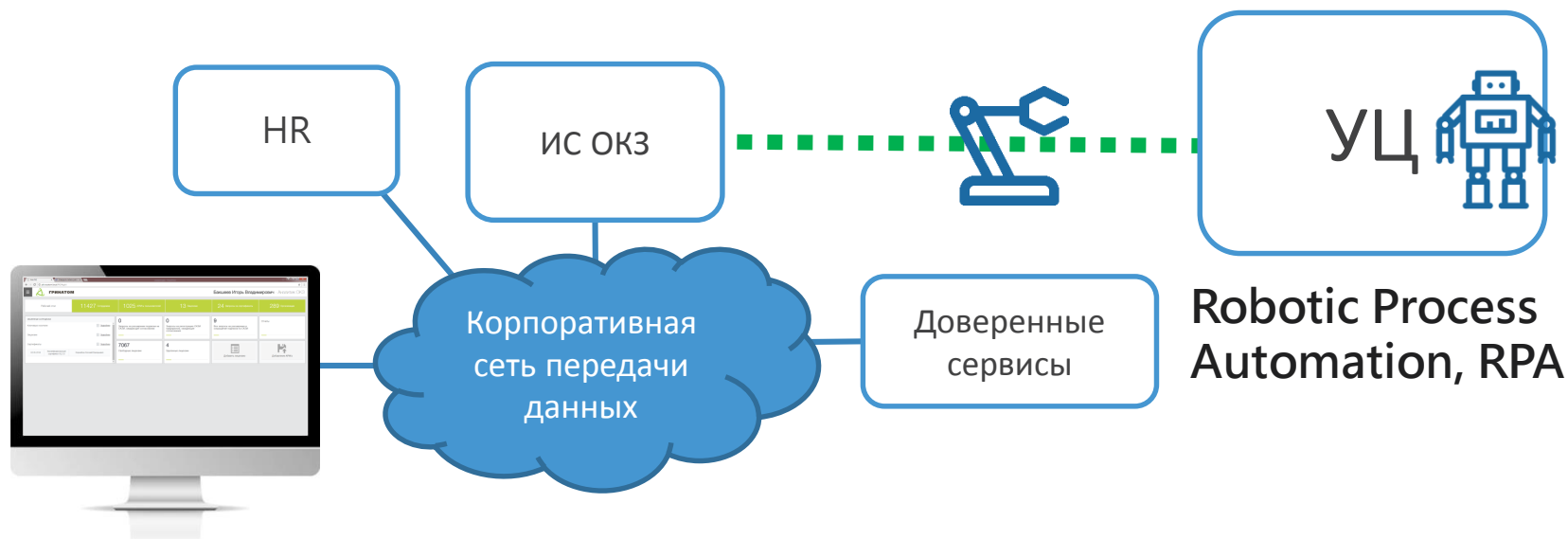
Закупить средства УЦ класса  
КВ2

## Вариант 2

Отключить средства УЦ от сетей

Производить перенос данных  
вручную

Роботизация процесса



При использовании технологии остаются неизменными существующие контроли, регламентные процедуры и отчетность

1. Запрет подключения ПАК УЦ к оборудованию сетей общего доступа

• Роботизация

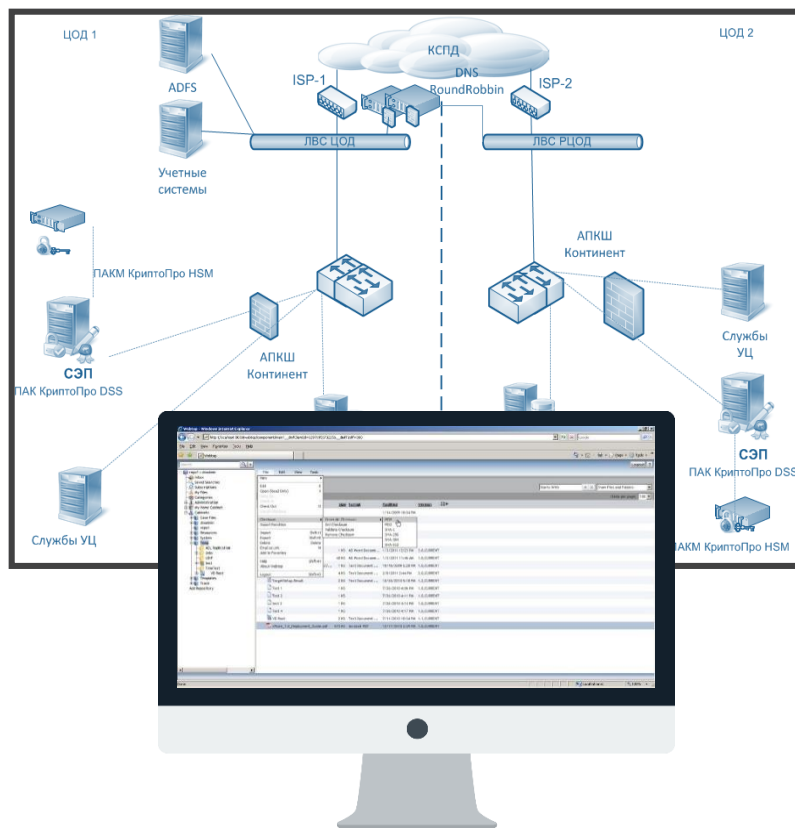


1. Идентификация представительств и филиалов крупных корпораций
2. Поле commonName
3. Поле localityName
4. Поле organizationUnitName
5. Поле title
6. Справочники значений для stateOrProvinceName, streetAddress

2. Проблемы идентификации в квалифицированном сертификате

- Машиночитаемые идентификаторы
- Оптимизация для автоматической проверки





Упрощение процессов:

1. СКЗИ на АРМ (лицензия, учёт, обучение, допуск)
2. Наличие ОКЗ на месте
3. Доступ к СОС ГУЦ
4. Доступ у СОС КУЦ
5. Доступ к службе времени, статусов
6. Доступ к сервису валидации

Выгоды:

1. Экономия средств
2. Экономия времени
3. Повышение уровня безопасности

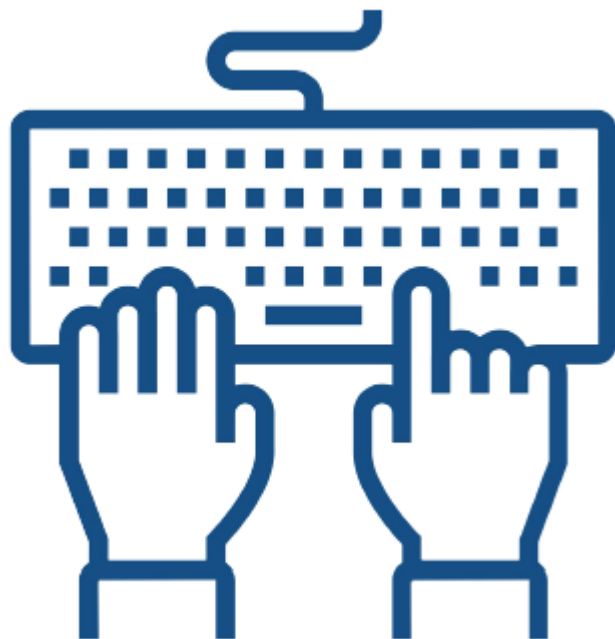
3. Безопасность использования УКЭП на рабочих местах

- Корпоративные доверенные СЭП



**В алгоритмах поведенческой биометрии используются технологии:**

- математической статистики для извлечения индивидуальных особенностей пользователей
- нейронных сетей для определения веса каждой особенности в наборе
- машинного обучения для построения поведенческого профиля пользователя
- Artificial Immunity (искусственный иммунитет) для обнаружения аномалий



Вместо заполнения множества полей пользователь заполняет тривиальную информацию о себе. При этом каждый символ содержит индивидуальные биометрические данные.

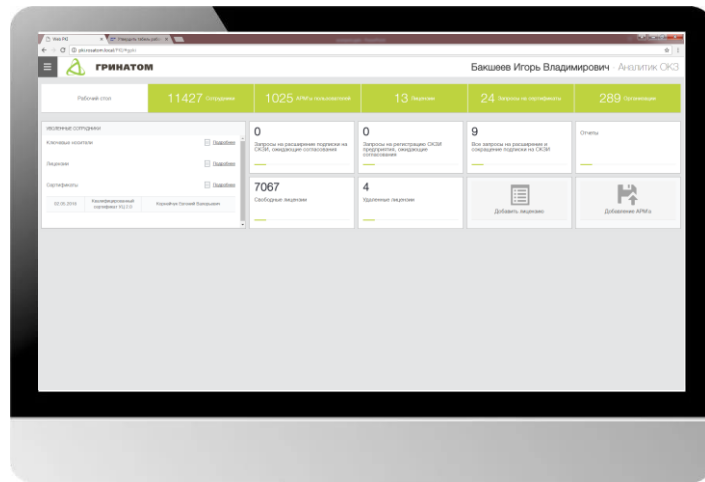
В нужный момент система идентифицирует клиента и безопасно передаст данные пользователя для проведения операции с ЭП.

Реальный способ связать подпись с пользователем.

4. Аутентификация владельца сертификата

• Поведенческая аутентификация

# Повышение роли Администратора безопасности ОКЗ для средних и крупных компаний. Организационные и технические аспекты.



Обеспечение сертификатами ЭП

Обеспечение СКЗИ

1. Автоматическое планирование регламентных работ
2. Автоматический учёт
3. Облачная подпись электронных документов
4. Автоматический сбор информации об АРМ
5. Автоматическое обновление и блокирование СКЗИ

5. Разрыв в требованиях инструкций и современными технологиями

• Автоматизация - основа повышения производительности труда



**Ольшаников Алексей Владимирович**

**Ведущий специалист**

**Тел: +7(985) 998-44-84**

**[avolshanikov@greenatom.ru](mailto:avolshanikov@greenatom.ru)**