Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Организация криптографической защиты информации в интеллектуальной системе учета электрической энергии

Костромин Игорь Сергеевич,
Начальник отдела встраиваемых доверенных систем АО «ПКК Миландр»

Основные направления развития интеллектуальных систем учёта элеткроэнергии (ИСУЭ)

- Учёт предоставления электрической энергии через «интеллектуальную» систему (национальная программа «Цифровая экономика»).
- Приборы учёта (ПУ) станут собственностью снабжающих компаний, а не граждан (522-ФЗ).
- 522-ФЗ определяет расширение гарантированного функционала в т.ч. и по защите информации (детализирован в проекте ПП РФ).
- Постепенное повышение доли отечественных микросхем в приборах учёта до 90% к 1 января 2022 года (ПП РФ №719 от 17.07.2015).

Основные потребители ИСУЭ

В России по состоянию на 2019 год 76 млн. точек подключения электрической энергии.

Эти счётчики согласно 522-ФЗ постепенно будут заменяться за счёт энергоснабжающих компаний. Срок начала установки определённый в законе – 01 июня 2020 года.

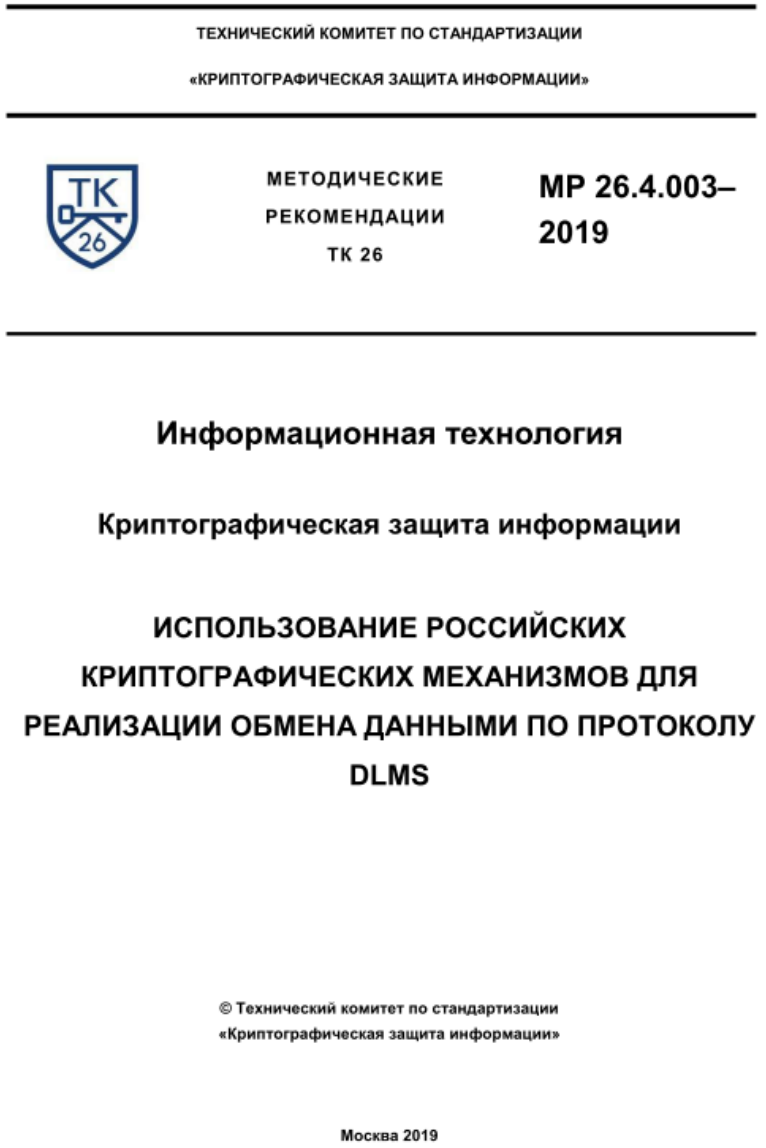
Крупные энергоснабжающие компании станут основными потребителями электросчётчиков. Например, у ПАО Россети планы по замене 22 млн. счётчиков.

Стандартизация

ПТК 706 представило 2-ю редакцию ГОСТ Р «Требования к протоколам обмена информации между компонентами интеллектуальной системы учета и приборами учета» (фактически СПОДЭС – адаптация DLMS)

ТК 26 утверждены МР 26.4.001–2019 - методические рекомендации, описывающие использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS.

На уровне Министерства Энергетики обсуждается создание типовой модели угроз ИСУЭ.



ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ

«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

ТК 26

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ТК 26

МР 26.4.003–2019

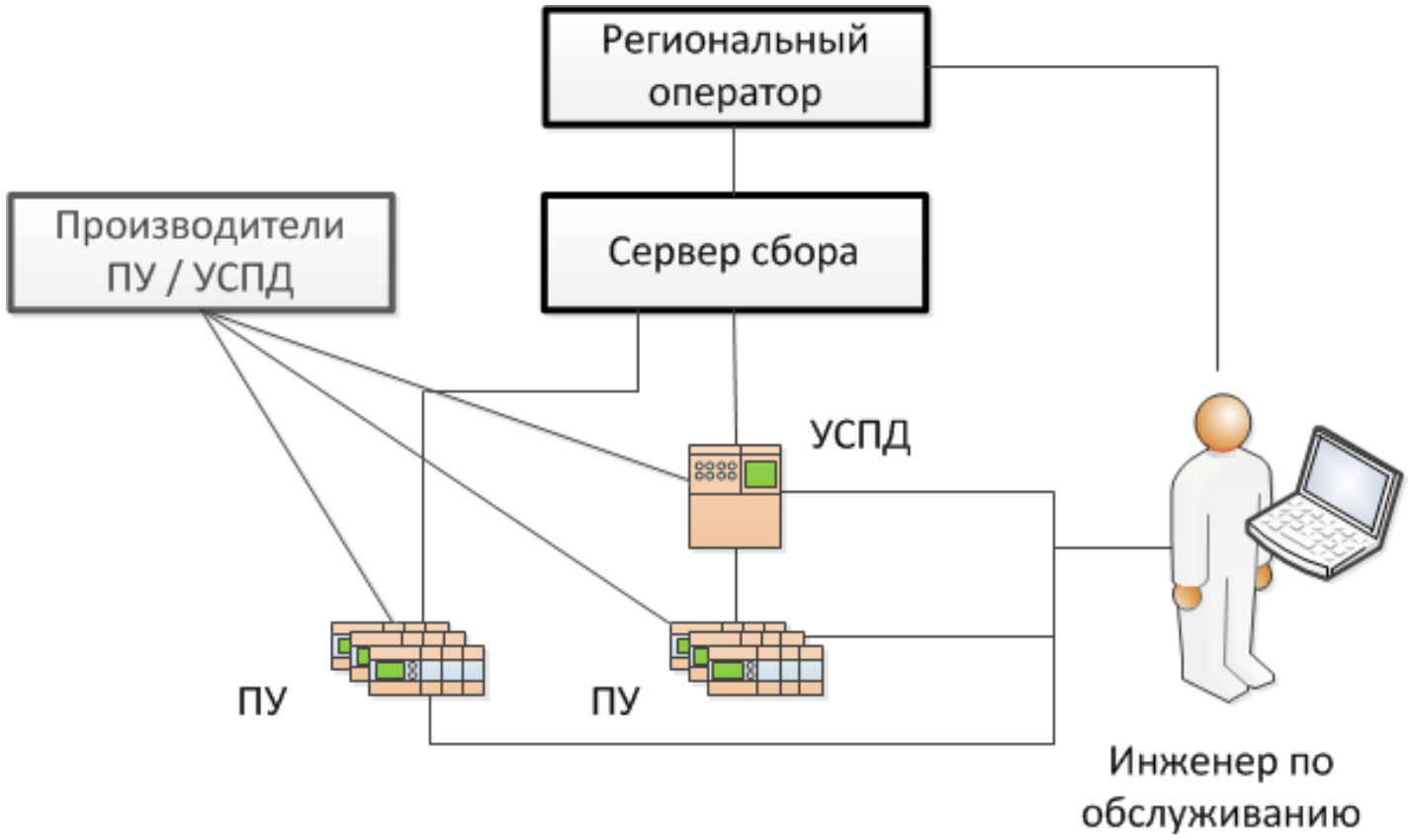
Информационная технология

Криптографическая защита информации

ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ ДЛЯ РЕАЛИЗАЦИИ ОБМЕНА ДАННЫМИ ПО ПРОТОКОЛУ DLMS

Москва 2019

Типовое решение ИСУЭ



Крупные потребители начали пилотирование ИСУЭ, которые рассматриваются как типовые. В частности ИСУЭ внедрено в некоторых региональных подразделениях ПАО Россети.

- Формализованная модель угроз.
- Смешанная схема (с/без УСДП) сбора данных.
- Сертификация серверной компоненты на безопасность ФСТЭК.
- Для совместимости ПУ И УСПД разных производителей данные между ними передаются в открытом виде

Анализ модели угроз типового решения

Все угрозы ИСУЭ в представленной модели угроз сводятся к:

- Мошенническим действиям пользователей.
- Недоступности отчётов серверной компоненты.

Не рассматриваемые угрозы:

- Подмена встроенного ПО через механизм обновления.
- Отказ в предоставлении услуг потребителям (ограничение подачи ЭЭ).
- Утечка персональных данных (детализация энергопотребления) и возможный ущерб потребителям.
- Репутационные риски и косвенные угрозы.

Недостаточная оценка угроз приводит к неправильному проектированию мер защиты, а именно:

- Полное отсутствие защиты уровня ПУ.
- Отсутствие защиты каналов передачи данных.

Позиция по безопасности сетевых организаций и производителей приборов учёта

Было получено принципиальное согласие, что нужно внедрение средств защиты информации в приборы учёта, при выполнении следующих условий:

- Цена решения защиты информации должна быть приемлемой.
- Минимальные требования по лицензированию деятельности по работе с криптографической защитой для производителей ПУ.
- Средство защиты информации должно выполняться на российских микросхемах.
- Взаимозаменяемость ПУ различных производителей.
- Отсутствие необходимости в обслуживании на межповерочном интервале.

Срок обслуживания и жизни ключей

Приказ Росстандарта от 02.07.2019 N 1502 «Об утверждении рекомендуемых предельных значений интервалов между поверками средств измерений» устанавливает межповерочный интервал для счётчиков 16 лет

- более 98% типов средств измерения имеют межповерочный интервал 4 года и меньше
- и только 2 типа (< 0.5%) - более 10 лет

Решение для защищённой ИСУЭ

Структура сети с промежуточными узлами сбора

Взаимозаменяемость ПУ различных производителей

⇨ Асимметричная криптография для установления связи

Минимальные требования по лицензированию производителей ПУ

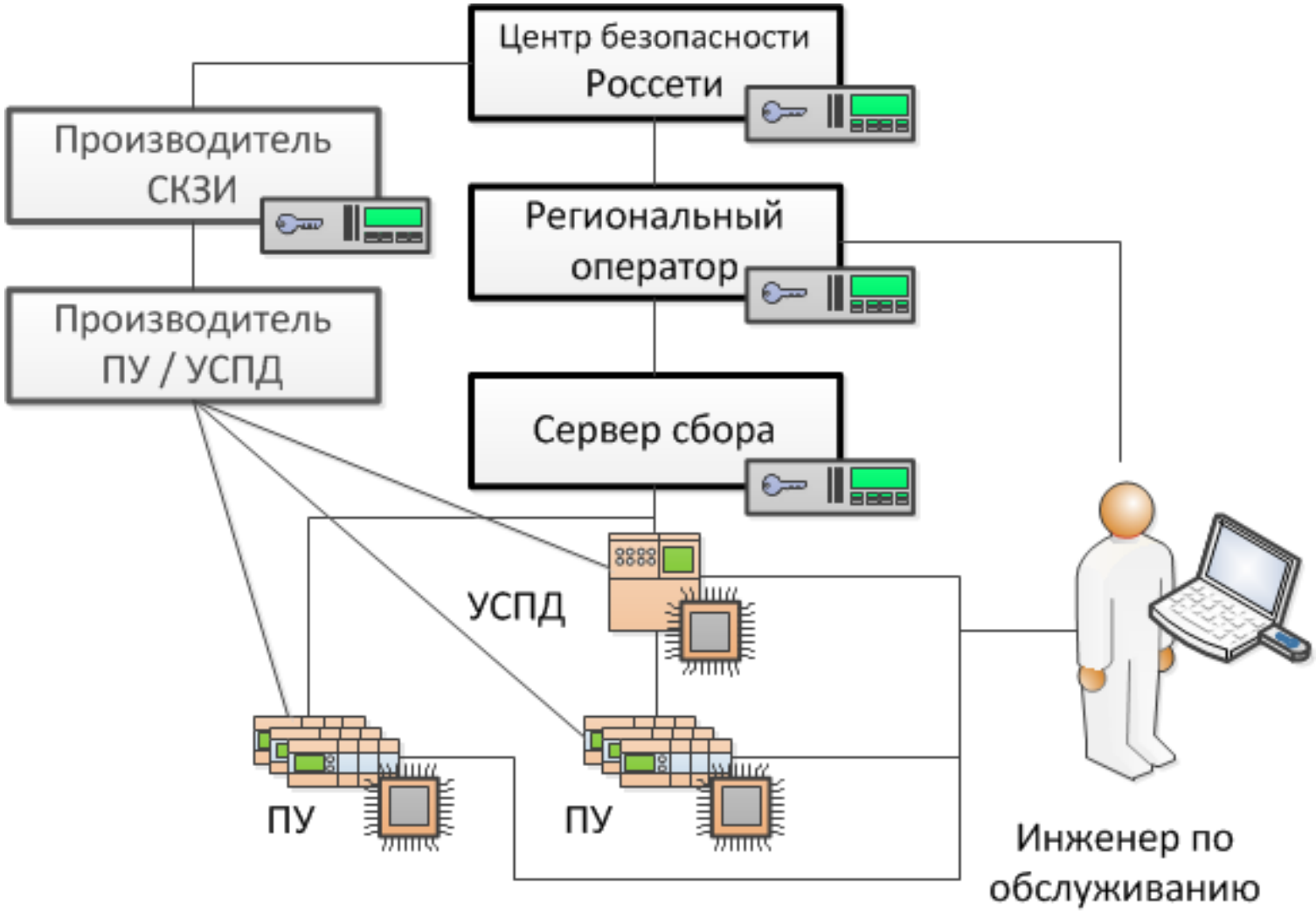
Использование российской ЭКБ

⇨ Безопасность на основе встраиваемых СКЗИ на российских микросхемах

Длительный необслуживаемый период ⇨

- Обоснование возможного ущерба в модели угроз
- Добавление канала ввода ключей в конструктив

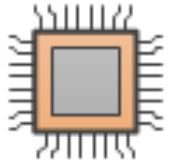
Защищённая сеть ИСУЭ



Средства криптографической защиты информации

- HSM

- встраиваемый СКЗИ



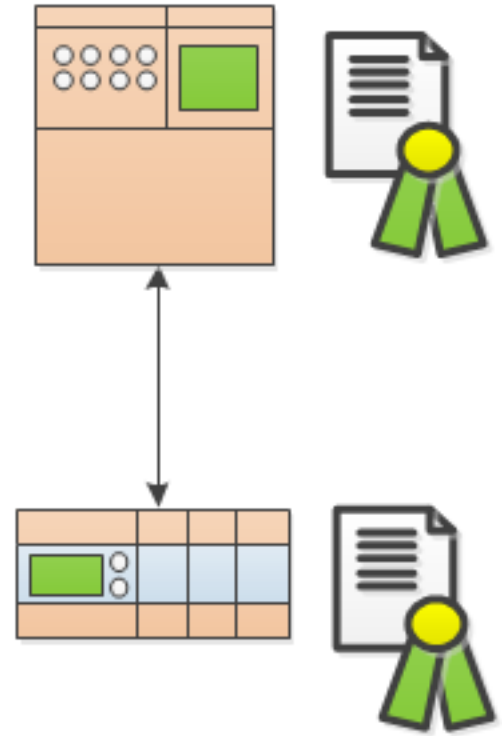
- крипто-токен

Рекомендованная асимметричная криптография

В МР 26.4.003-2019 описаны асимметричные схемы согласования ключа с использованием постоянных и эфемерных ассиметричных ключевых пар.

Проблема со списками отзывов, характерная для ассиметричных схем может быть решена через «белые списки». Фактически они уже реализованы:

- по нисходящему каналу в виде списка опроса
- по восходящему каналу в виде списка поддерживаемых соединений



Лицензирование деятельности

1. Производство HSM

2. Функции УЦ, подготовка HSM для производителей СКЗИ и операторов ИВК

3. Производство СКЗИ, начальная загрузка в них ключей и сертификатов

Лицензия на разработку СКЗИ

4. Производство ПУ и УСПД, встраивание в них СКЗИ

5. Установка и пуско-наладка ПУ и УСПД

6. Сбор данных с сети ПУ и УСПД

Лицензия на эксплуатацию СКЗИ

Использование российских микросхем для СКЗИ

Согласно постановлению правительства РФ от 17 июля 2015 года N 719 в счётчиках электрической энергии должна соблюдаться доля использования российских электронных компонентов:

до 31 декабря 2019 г. - не менее 10 процентов,

с 1 января 2020 г. - не менее 50 процентов,

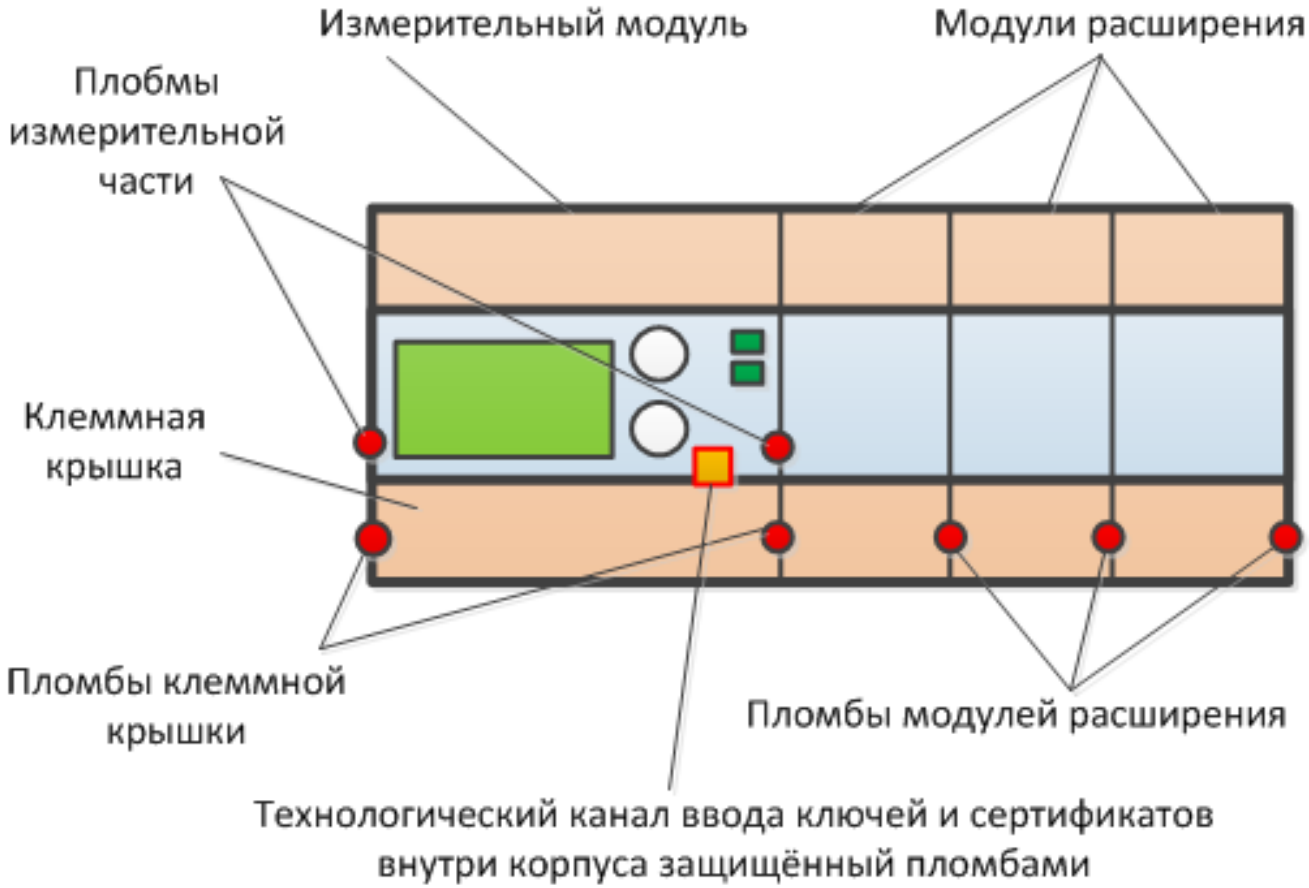
с 1 января 2022 г. - не менее 90 процентов.

Встраиваемые СКЗИ должны быть реализованы только на российских микросхемах, чтобы быть востребованными производителями ПУ.

Российские компании (в частности, ПКК Миландр) производят как микросхемы для создания СКЗИ, так и микросхемы, объединяющие функционал счётчика электроэнергии и СКЗИ.

Смена ключей и сертификатов

В случае необходимости смена ключей и сертификатов выполняется через изолированный и недоступный при нормальной эксплуатации (опломбированный) технологический разъём с физического носителя (криптографического токена)



Достоинства предложенной схемы

- Все ПУ всех производителей взаимозаменяемы пока их корень доверия совпадает.
- Производителям ПУ не требуется получать лицензию на производство СКЗИ, только на эксплуатацию.
- Цена решения:
  - тысячи рублей – при использовании встраиваемого модуля по типу ФН;
  - сотни рублей – при использовании модуля безопасности на базе спец. ИМС / смарт-карт;
  - десятки рублей – при интеграции безопасности в интегральную микросхему счётчика.
- При использовании российских микросхем в СКЗИ не обременяет производителей ПУ по 719 ПП РФ.
- Канал ввода ключей позволяет обновлять ключи и сертификаты без замены устройства.

Открытые вопросы и перспективы

Открытые вопросы:

- Длительный (до 16 лет) срок службы ключей для приборов учёта и рекомендуемой модели угроз.
- Утверждение схемы лицензирование работы с СКЗИ.

Перспективы:

- Умные счётчики в РФ должны оснащаться российской криптографией и российскими микросхемами.
- Общая потребность 80 миллионов штук.
- Массовое внедрение криптографии позволит стимулировать развитие российской радиоэлектроники и криптографии для массового применения.

Вопросы

Контактная информация

Костромин Игорь Сергеевич
Начальник отдела встраиваемых доверенных систем
АО «ПКК Миландр»

Электронная почта:
kostromin.i@milandr.ru
info@milandr.ru

Телефон:
+7 495 981 54 33
+7 916 304 86 26

Сайт:
www.milandr.ru

Адрес:
124498, г. Москва, Зеленоград, Георгиевский проспект, дом 5