Сертификаты физлиц для служебных целей

- Как обеспечить безопасность сотрудников *и физ. лиц при использовании ЭП*?
- Какие носители стоит использовать?

Сергей Груздев
ген. директор
"Аладдин Р.Д."

Как обеспечить безопасность сотрудников при использовании ЭП?

Начнём с матчасти…

- Безопасность сотрудников (физлиц) = **Безопасность технологии применения УКЭП**

Проблема #1

- В РФ нарушен базовый принцип безопасности применения УКЭП
  - УКЭП базируется на технологии PKI - инфраструктуры открытых ключей
  - Базовый принцип PKI (№1) гласит:
    - Закрытый ключ ЭП известен ТОЛЬКО его владельцу, он лично его контролирует и МОЖЕТ обеспечить безопасное хранение и использование
  - Первую редакцию 63-ФЗ "списывали" с Европейского законодательства, но убрали ОБЯЗАТЕЛЬНОЕ требование к УКЭП
    - УКЭП ДОЛЖНА формироваться ТОЛЬКО с использованием специализированного аппаратного средства Secure (Qualified) Signature Creation Device (SSCD/QSCD) с подтверждённой безопасностью (неклонируемость, неизвлекаемость закрытого ключа ЭП)
    - Без этого владелец закрытого ключа ЭП НЕ СМОЖЕТ обеспечить его безопасность и КОНТРОЛИРОВАТЬ его использование, поскольку **ДОПУСКАЕТСЯ наличие дубликатов и клонов**, а значит - "Я не я, и подпись не моя" или еще хуже - "Кто-то подпишет обязывающий документ моей подписью за меня, и я об этом не сразу узнаю…"

✓ **В России такого требования (SSCD/QSCD) нет, отсюда - наши шарахания и фантазии с различными типами подписей. И существенная часть наших бед…**

Как обеспечить безопасность сотрудников при использовании ЭП?

Проблема #2

- Безопасность использования УКЭП
  - В банках (ДБО) мы подписываем платёжку, потом банк её проверяет (Антифрод - выявление подозрительных платежей), может заблокировать и попросить подтверждения
    - Подписанная платёжка без проводки банком - ещё не документ для безоговорочного списания денег
  - В ЭДО всё немного не так (хуже с точки зрения безопасности) - подписанный с помощью УКЭП документ - уже юридически значимый документ, который начинает жить сразу с момента подписания
  - Государство (с текущей регуляторкой) сняло с себя ответственность и переложило все риски на бизнес и физлиц
    - Текущая модель применения УКЭП и квалифицированных сертификатов ЭП несёт в себе большие риски
    - (а) для бизнеса и его владельцев
    - (б) для физлиц (иногда даже больше, чем для бизнеса)

✓ **Это означает, что каждый руководитель, каждая организация (владелец ИС, эл. сервисов) должны определить для себя РИСКИ и ДОПУСТИМЫЕ ПОТЕРИ (и последствия) от использования УКЭП**

Как обеспечить безопасность сотрудников при использовании ЭП?

Риски, связанные с применением УКЭП

- Риск - это вероятность осуществления успешной атаки, приводящей к потерям (убыткам) и последствиям

Факторы риска

- Отработанные технологии атак и сложность их проведения (технические и социальные), например:
  - Атаки на процессы **ПОЛУЧЕНИЯ** УКЭП (незаконное получение сертификата ЭП на другое лицо, последствия - потеря имущества, смена директора компании т.п.)
  - Атаки на процессы **ИСПОЛЬЗОВАНИЯ** УКЭП (незаметная подмена подписываемого документа, "пакетное" подписывание, автоподписывание или подписывание документа за человека, в отсутствии человека и его прямого волеизъявления)
  - Атаки на **СРЕДСТВО ЭП**
    - Терминология "Ключевой носитель (КН)" и его производные - Активные, Пассивные, Интеллектуальные, Функциональные (ФКН) - **некорректные названия** - от заложенной ущербности в наше законодательство и отсутствия требований к SSCD (QSCD) для УКЭП, *мы эту терминологию стараемся не использовать и вам не советуем - только* ***Средство ЭП***
- Оценка рисков: Высокие / Низкие / Средние
  - Где брать данные для оценки рисков? У вендоров, экспертов

Как обеспечить безопасность сотрудников при использовании ЭП?

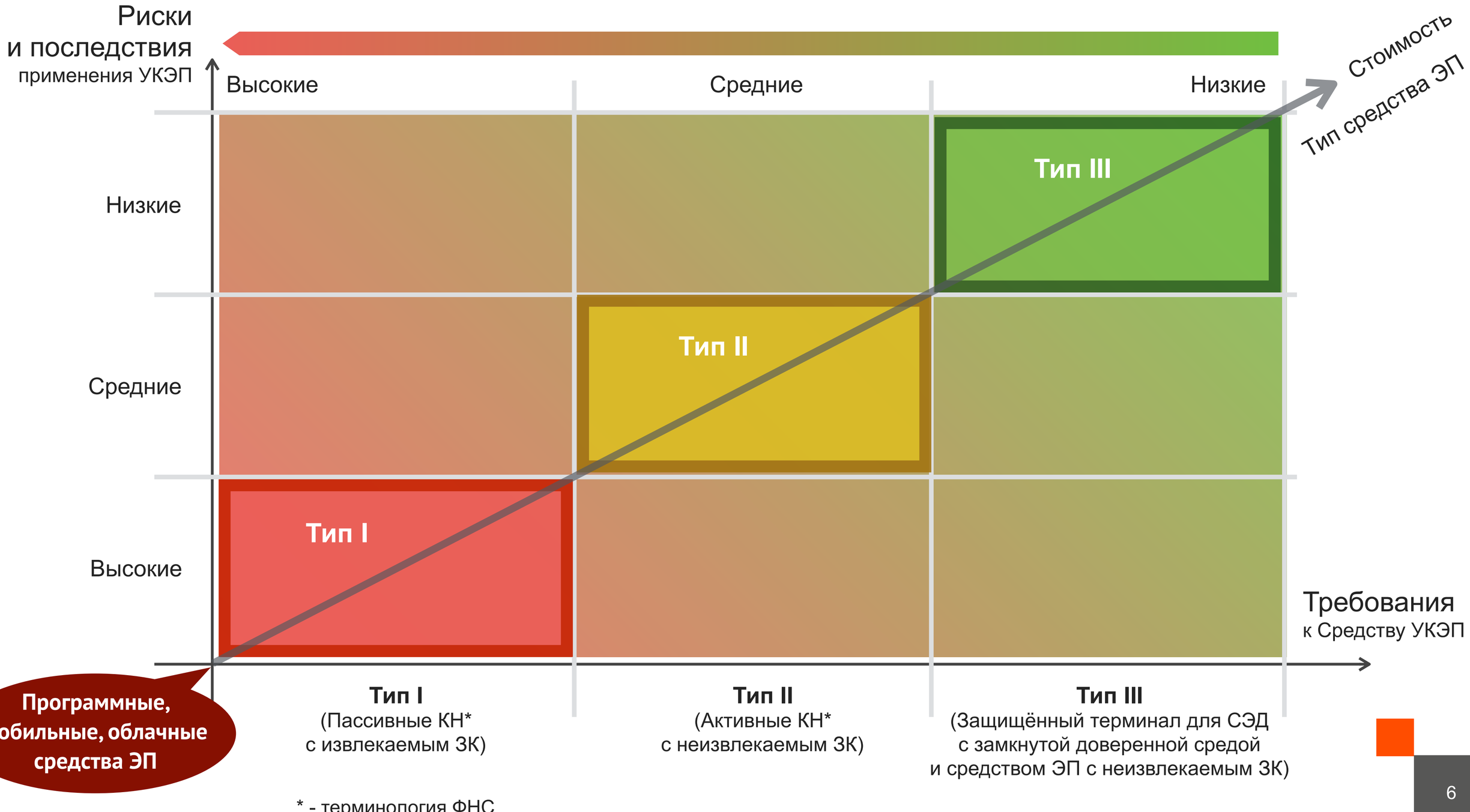
Последствия, связанные с применением УКЭП (для организаций)

- Несущественные
  - Организация "не заметит" последствий атаки
    - Например, внутренние распорядительные, рабочие документы, закупка канцелярки и пр.
- Средние (существенные)
  - Последствия могут быть ощутимы, но не катастрофичны, их можно исправить без существенных финансовых, репутационных и временных затрат
    - Например, документы бухгалтерской отчётности (все деньги - в ФНС!), эл. торги (на средние для компании суммы), закупка оргтехники, мебели и пр.
- Катастрофические
  - Последствия могут привести к остановке, потере бизнеса, банкротству, смене руководства…
    - Например, перерегистрация юр. лица, заключение заведомо невыполнимых сделок с попаданием в чёрный список недобросовестных исполнителей и поставщиков, серьёзные репутационные потери

✓ **Глядя на всё это сотрудники (как физлицу в контексте МЧД) проще отказаться от любой доп. ответственности и последствий использования УКЭП им как физлицом - риски и последствия для него могут быть огромны** - с этим мы ещё столкнемся…

✓ **Каждый руководитель организации должен определить границы применения УКЭП в зависимости от допустимых потерь и выбрать правильные средства ЭП**

Градуирование рисков и выбор соответствующих средств ЭП



* - терминология ФНС

Какие носители и КОГДА стоит использовать?

- Программные, мобильные, облачные средства ЭП
  - **Нарушен базовый принцип PKI** - пользователь не может контролировать и обеспечить безопасность хранения и использования закрытого ключа (ЗК) своей ЭП
  - ✓ **Использовать для УКЭП категорически нельзя, только для собственного внутреннего ЭДО - т.н. КОРПОРАТИВНОЕ использование**

- Пассивные ключевые носители (с извлекаемым ЗК) **- тип I**
  - USB-токены, смарт-карты, используемые как "флешка с PIN-кодом" для хранения криптоконтейнера (крипто?) с ЗК ЭП
    - Неизвлекаемый криптоконтейнер не есть неизвлекаемый ЗК (ключ подписи)
    - Срок действия ЗК (сертификата) - 1 год
  - Основные последствия от типовых атак - **утеря контроля над ЗК ЭП**
    - Кража ЗК ЭП (контейнера ключа)
    - Клонирование ЗК ЭП (создание несанкционированных копий)
    - Несанкционированное использование ЭП
  - ✓ **Риски для организации (ПРИ ПРАВИЛЬНЫХ ОГРАНИЧЕНИЯХ) могут оставаться небольшими**
  - ✓ **Риски для физлиц - могут быть огромны (открытие фирмы-однодневки, подписание дарственной и пр.)**

JaCarta LT

Какие носители и КОГДА стоит использовать?

- Активные ключевые носители (с неизвлекаемым ЗК) - **тип II**

  - USB-токены, смарт-карты с реализуемыми алгоритмами формирования и проверки ЭП с неизвлекаемым ЗК (все вычисления внутри чипа, функций экспорта ключей ЭП нет)

  ✓ **Это ПРАВИЛЬНЫЕ средства ЭП, близкие или соответствующие требованиям к SSCD/QSCD**

  ✓ **На них можно и нужно выпускать УКЭП**

  - При выпуске УКЭП на физ. лицо (в схеме с МЧД) организация может (и должна) брать расходы на средство ЭП и квалифицированный сертификат на себя
    - Срок действия ЗК (сертификата) - 3 года
  - При этом многие сотрудники работают дистанционно (или в смешанном режиме), тогда для организации безопасной дистанционной работы необходимы:
    - Двухфакторная аутентификация (2ФА) удалённых пользователей - ОБЯЗАТЕЛЬНО!
    - VPN - хранение ключей
    - Шифрование служебных данных на дисках и др.

  ✓ **Активный КН должен поддерживать и PKI, и набор ПО для "удалёнки"**

  - Основные последствия от типовых атак
    - **Подмена подписываемого документа** (таргетированная атака, возможна при работе в недоверенной среде - установленный троян, ПО для удалённого администрирования/управления)
    - **Авто-подписывание** навязываемого документа "**вслепую**" - без участия/присутствия/волеизъявления владельца ЭП
  - Риски - СРЕДНИЕ

JaCarta-2 PKI/ГОСТ
JaCarta-2 SE

Какие носители и КОГДА стоит использовать?

Активные ключевые носители (с неизвлекаемым ЗК)

- Как снизить риски от этих атак? (подмена подписываемого документа, навязывание подложного документа)
  - **Разделение сред** функционирования документа и процесса его подписания ЭП (мобильные телефоны)

✓ **Основное преимущество - удобство, все риски не снимает**

- **Специализированный Антифрод-терминал**
  - В него впаян чип смарт-карты, терминал подписывает всё что он отобразил и выполнил, сервер СЭД проверяет эту подпись и разбирает трекинг, что всё ОК

✓ **Снимает практически все риски применения УКЭП**

- **Использование биометрии** (НОВОЕ)
  - **Неотказуемость** и уверенность того, что эту подпись поставил ИМЕННО ЕЁ ВЛАДЕЛЕЦ

Какие носители и КОГДА стоит использовать?

- Защищённый терминал для СЭД с замкнутой доверенной средой и средством ЭП с неизвлекаемым ЗК
  - USB-токен - LiveUSB с предустановленной и настроенной замкнутой доверенной программной средой
  - Можно **безопасно** использовать при дистанционной работе с домашнего (или любого!) **недоверенного** ПК, кишащего тронами и вирусами - внешние агенты, партнёры, удалённые пользователи СЭД и пр.
  - Можно использовать при работе **с гос. органами** и для ЭДО **в ГИС, АСУ ТП, КИИ** до 1-го класса защищённости

✓ **Дороже, но существенно снижает БОЛЬШИНСТВО рисков, можно использовать для организации безопасной дистанционной работы сотрудников, но в разы ДЕШЕВЛЕ, чем использовать выделенный ПК с набором средств защиты (в 7-10 раз)**

✓ **Главное - соответствие Требованиям к средствам безопасной дистанционной работы и наличие сертификата**

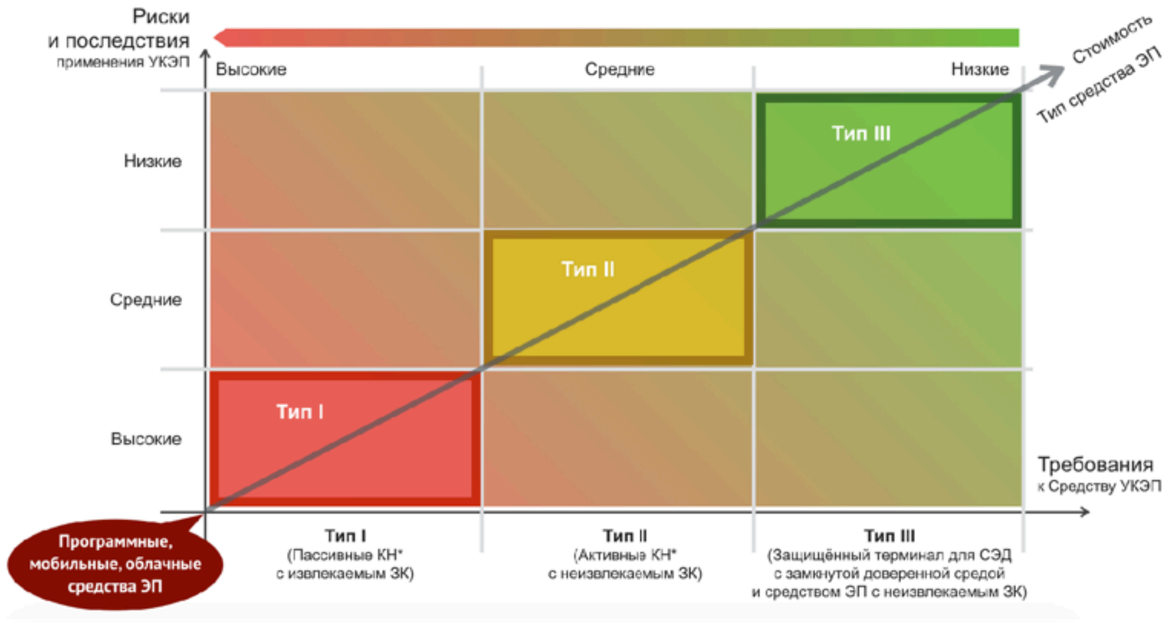
✓ **Продукт - Aladdin LiveOffice**

Как обеспечить безопасность при использовании ЭП - резюме (1)

- Текущая модель применения УКЭП несёт для бизнеса и физлиц (в схеме с МЧД) большие риски
- Каждый руководитель организации должен определить для себя уровни допустимых рисков и допустимых потерь от использования УКЭП
- Выбирая класс и функциональность средств УКЭП надо сразу ориентироваться на корпоративное применение (интеграцию в корпоративную инфраструктуру (2ФА, VPN, дистанционная/смешанная работа офис/дом, централизованное управление)
- Для решения проблемы "привязки" средства ЭП к человеку, возможного отказа от взятых обязательств, разбора инцидентов (наличия доказательств) **рекомендуется использовать биометрию**
  - BIO-кнопку по отпечаткам пальцев для подтверждения транзакции
- Наибольший уровень безопасности при использовании УКЭП обеспечивается **специализированными терминалами**
  - Антифрод-терминал
  - Aladdin LiveOffice - сертифицированное средство для организации дистанционной работы сотрудников с замкнутой доверенной программной средой (можно работать с документами, имеющими гриф **ДСП**)

Как обеспечить безопасность при использовании ЭП - резюме (2)

- ✓ **Различия в цене средств ЭП небольшие, а в возможностях существенно снизить риски и потери от использования УКЭП - огромные**
- ✓ **ИС/СЭД организации САМА ДОЛЖНА реализовывать РАЗДЕЛЕНИЕ сервисов/операций/документов по уровню критичности и ТРЕБОВАТЬ применения соответствующих средств ЭП**
  - Средств ЭП **нужного класса** с набором доп. средств противодействия важным и актуальным для организации и её бизнесу угрозам
  - **Не допускать** использования средств ЭП, не обеспечивающих необходимый уровень безопасности и компенсации существенных угроз или атак
  - Давать возможность устанавливать **границы применения ЭП** (риски) и ПРАВИЛА самим организациям и их руководителям



Спасибо!

Сергей Груздев

ген. директор
АО "Аладдин"

www.aladdin.ru