# Переходите в облако … задайте юристу вопросы

**Георгий Пчелинцев, партнер Dentons,**

**Cloud & Digital Transformation**
**Москва, 28.03.2019**

# Урегулированные облака?

- Законопроект об облачных вычислениях – начали обсуждение в 2014, сделан доступным…
- Были ФТСЭК и ЦБ: ГИС, ПДн, финансовые учреждения…
- Стал общий закон: Закон № 187-ФЗ О безопасности критической информационной инфраструктуры с 1 января 2018
- Ответственность УК РФ 274.1 за несоблюдение требований, повлекшее ущерб КИИ. Вплоть до лишения свободы 6-10 лет.

# Сфера регулирования КИИ

- ОКИИ - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
- Субъекты КИИ – ОГВ и учреждения, российские ЮЛ / ИП предприниматели, которым принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере
  - здравоохранения,
  - науки,
  - транспорта, связи,
  - энергетики, в области атомной энергии, топливно-энергетического комплекса
  - банковской сфере и иных сферах финансового рынка,
  - оборонной, ракетно-космической,
  - горнодобывающей, металлургической и химической промышленности,
  - российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей

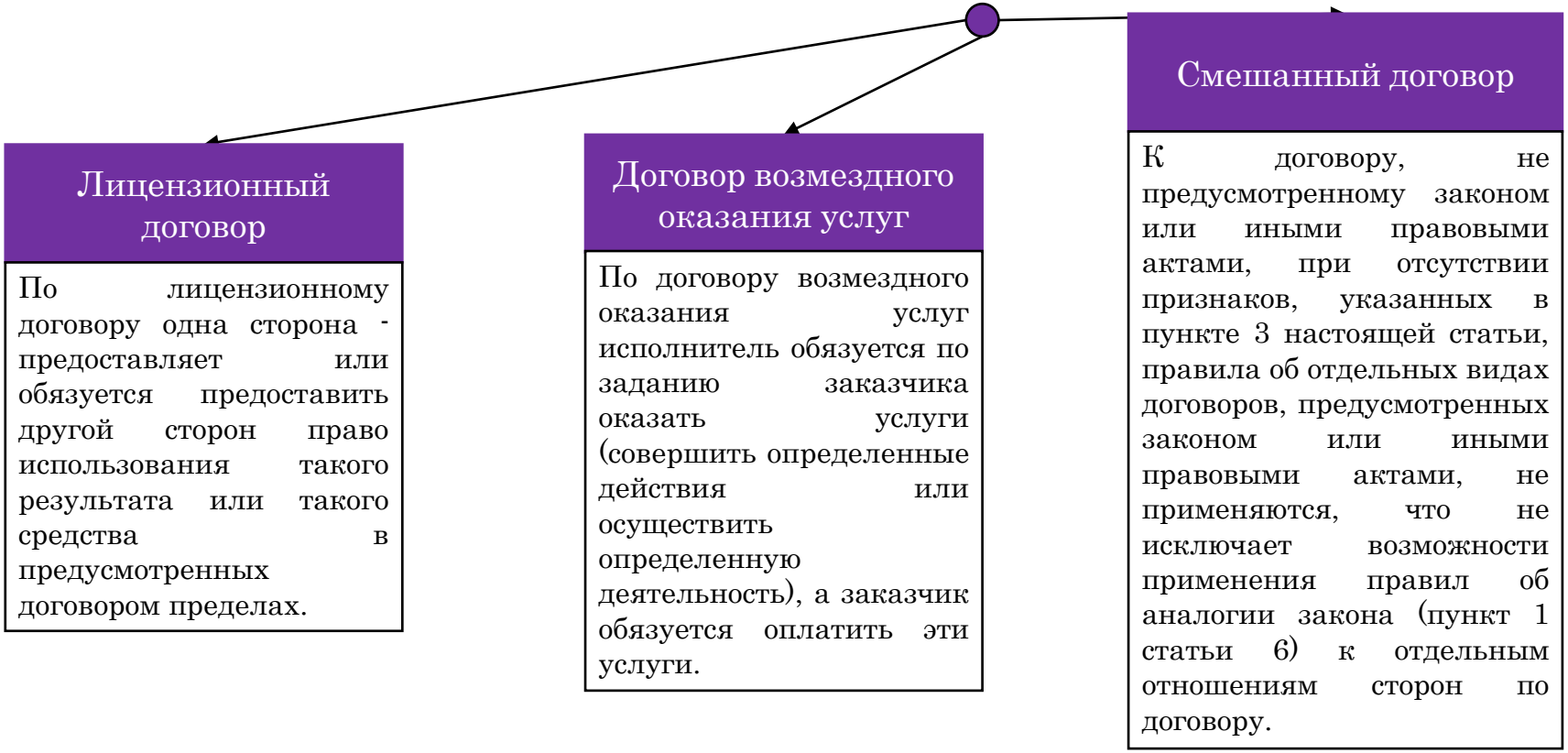
# Основные обязанности субъектов КИИ

- Составление перечня объектов ОКИИ и направление перечня во ФСТЭК
- Категорирование объектов в течение года. Согласование перечня и моделей угроз с ФСТЭК.
  - Постановление Правительства № 127 - Правил категорирования объектов критической информационной инфраструктуры РФ
  - ФСТЭК Приказ № 235 - описывает создание системы защиты, требования к персоналу, регулярности мероприятий по безопасности
  - ФСТЭК  Приказ № 239 - базовый набор мер по защите объектов КИИ
- ФСБ – оператор ГосСОПКА
  - информировать о компьютерных инцидентах ФСБ России – 24 часа;
  - оказывать содействие ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов.

# Облачные технологии- проблема применимого права

- Юрисдикция – в какой стране можете быть подан иск вами или против вас
  - базовое - местонахождение ответчика (деятельности ответчика, местонахождение сервера?)
  - местонахождение имущества ответчика (информации ответчика?)
  - место совершения нарушения (страна регистрации ТЗ)
  - в любом государстве где доступна информация причиняющая вред
  - местонахождение истца при причинении ему вреда
- Отсутствует унифицированный подход, отсутствуют специальные международные соглашения международные договоры

# Договор с провайдером SaaS



# Соглашения сторон

- **Terms of service** – соглашение, содержащее основные условия оказания услуг, включая перечень услуг, порядок расчётов, срок действия и прекращения договора и иные основополагающие условия
  - **End User Agreement** – соглашение о предоставлении права использования тех программ, которые провайдер делает доступными пользователю, есть ли агентская часть программного обеспечения
  - **Acceptable Use Policy** – правила допустимого использования; на самом деле содержат перечень того, что пользователю запрещено (спам, диффамация, нарушение интеллектуальной собственности, иная запрещенная законом или пограничная деятельность)

# Соглашения сторон

- **Service Level Agreement** – соглашение об уровне сервиса, ключевой документ, определяющий обязательства и ответственность провайдера.
- **Privacy Policies** – обязательства провайдера по сохранению конфиденциальности данных пользователя, иные ключевые положения, относящиеся к защите «собственности» на информацию, а также ограничения деятельности оператора по анализу данных и сбору метаданных.

# Ответственность провайдера за недостатки услуг

В лицензионном договоре предметом является "неисключительное право, которое, не являясь вещью, не может быть некачественным. = основания ответственности очень ограниченные

В договоре возмездного оказания услуг – качество услуг, гарантии, возможность требовать возмещения убытков

В смешанном договоре могут предусмотрены вопросы ответственности из аналогичных договоров.

# Некоторые вопросы при переходе в облако

- Проверка политик защиты информации клиентов
- Оценка выполнения провайдером национального законодательства и рисков прекращения деятельности из-за нарушений
  - лицензия на оказание телематических услуг связи (РКН),
  - лицензия на распространение средств, информационных и телекоммуникационных систем, защищенных шифрованием (ФСБ);
  - выполнение работ и услуг в области шифрования информации (ФСБ)
  - деятельность по технической защите информации (ФСТЭК)
- Какую ответственность несет провайдер за недоступность сервиса?
- Предлагается ли SLA? Какая доступность? Ответственность?

# Некоторые вопросы при переходе в облако

- Система нотификации и отслеживания сбоев? Аудит?
- Гарантия сохранности информации? Back-up/восстановление? Цена?
- Страна хранения информации. Есть ли выбор?
- Как часто происходят обновления? Какая политика обновлений?
- Порядок изменения договора? Односторонний?
- Основания расторжения договора? Какие действия могут привести к расторжению договора?
- Оператор связи (телематика) – СОРМ?

# Некоторые вопросы при переходе в облако

- Собственность на информацию
  - Первоначальная информация – «собственность» клиента
  - созданная в облаке информация - **в договор! (м**есто создания РИД)
  - права на информацию при расторжения договора – **в договор!**
  - **процедура возврата** информации при **каждом** виде расторжения договора
  - формат возвращаемых данных, экспорт (non-proprietary format)
  - срок возврата после предъявления требования
  - срок и обязанность удаления информации провайдером
  - права на информацию **при нарушении** договора (неоплате) **– в договор!**
  - **удержание** информации (как способ обеспечения) – **в договор!**
  - **метаданные и data mining**

# SLA - предмет и содержание

- Определение уровня и состава собственного сервиса
  - Понятия, используемые в SLA
  - Четкий перечень видов услуг, регламентируемых SLA
- Определение измеримых метрик для выбранных сервисов
  - Перечень измеримых критериев качества по каждому сервису
  - Целевой  и минимальный уровень по каждой метрике
  - Uptime/Downtime 99,99%= 52.56 мин.в год, TAT - время реагирования
  - Mean-Time-Between-Failure (MTBF): время работы до ошибки  .
  - Mean-Time-To-Repair (MTTR): время на устранение ошибки
- Исключения из сферы ответственности провайдера
  - Форс-мажор, сети связи и доступность Интернета
  - Разумные усилия

# SLA - предмет и содержание

- Время предоставления услуг и исключения
  - Регулярное обслуживание, выходные
- Разграничение зон ответственности провайдера и клиента (инф. безопасность)
- Порядок уведомления о происшествиях и разрешения разногласий
  - Заявки и Trouble ticket
  - Эскалация
- Последствия нарушения service levels
  - Service credits, штрафы, и их пределы
  - Дополнительные возмещения
- Расторжение договора
- Пересмотр договора
- Отчетность и мониторинг