Garter Briefing 2011: Cloud Computing
ПО как услуга и облачные вычисления: управление рисками

Том Шольтц (Tom Scholtz)

Gartner

О чем следует задуматься компаниям:

- Нестабильность европейской экономики стимулирует тенденцию дальнейшего снижения расходов на ИТ, и одновременно - повышения гибкости/адаптируемости/скорости ИТ;
- Стремительно растет интерес к ПО, предоставляемому в качестве услуги, облачным вычислительным средам и услугам инфраструктур на базе облачных вычислений, и также стремительно растет их распространение;
- Европейские законы, защищающие неприкосновенность частных данных, одни из самых строгих в плане защиты данных потребителей и сотрудников компаний;
- Государственные и коммерческие компании все более обеспокоены вопросами безопасности и соответствия ИТ нормативным требованиям.

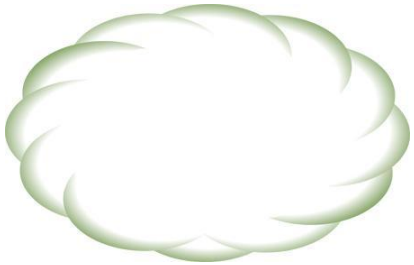
Gartner

Основные вопросы:

1. Какие риски связаны с использованием услуг, предоставляемых на базе облачных вычислений, и что более всего волнует клиентов?
2. Какие существуют способы разрешения вопросов, связанных с возникновением рисков, безопасностью и контрактными обязательствами, для поставщиков данного вида услуг?
3. Каким образом компании могут проводить оценку рисков и преимуществ, связанных с разными видами стратегий использования услуг на облачной основе?

Gartner

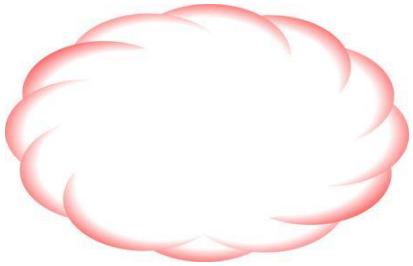
Дилемма «облаков»



Преимущества:

- Удобство, масштабируемость (готовая к использованию услуга «под ключ»);
- Гибкая услуга, с установлением цен на индивидуальных условиях;

Недостатки:



- Отсутствие контроля:
  - полная зависимость от архитектуры, функциональных возможностей и методов работы поставщика услуги;
- Отсутствие ясности в вопросах управления рисками;
  - а также программного обеспечения, местоположения, администрирования, компетенции?

Чем выше степень масштабируемости и удобства, тем сложнее оценивать и контролировать связанные с этим риски.

Gartner

Стратегический прогноз развития ситуации

Вплоть до 2014-го года отсутствие норм сертификации третьих сторон, напрямую касающихся вопросов безопасности, гарантии непрерывности бизнеса и восстановления после сбоев, будет останавливать порядка 30% компаний на пути к использованию платных услуг частных облаков

Факты, говорящие в пользу прогноза:

- Компании не всегда достаточно компетентны в оценке поставщиков.
- Проведение оценки на месте эксплуатации является дорогостоящим, как для поставщиков услуги, так и для клиентов.
- На первый взгляд, очевидное решение проблемы - сертификация третьих сторон, однако, существующие в настоящий момент программы сертификации не могут учесть все специфические риски новой модели вычислений на базе технологии, защищенной правом собственности.

Альтернативный путь развития:

- CAMM - в Великобритании, FedRAMP - в США и другие организации могут разработать специальную систему оценки облачных сред уже в начале 2011-го года.
- Убедившись в отсутствии явных нарушений норм безопасности, клиенты могут и не счесть необходимыми дальнейшие трудоемкие проверки качества облачных услуг.

Gartner

Факторы угрозы безопасности облачной архитектуры

- Ресурсы используются одновременно множеством клиентов (многоарендность):
  - Защита данных в процессе обработки и во время доступа к ним;
  - Защита данных во время хранения.
- Виртуализация действительно упрощает классификацию данных, однако:
  - Безопасность классификации, интеграции и доступности должна обеспечиваться за счет механизма виртуализации;
  - Всем клиентам необходим постоянный доступ к своим данным, вне зависимости от локализации этих данных в облаке, но только не к данным других клиентов.
- Доверие к облачным вычислениям:
  - разрешения и привилегии доступа, как для людей так и для машин, должны быть жестко закреплены за определенным числом виртуальных машин, сетевых узлов, сайтов, организаций и правовых юрисдикций.

Gartner

Проблемы, связанные с обеспечением непрерывности бизнеса и восстановлением после сбоев

- Каким образом осуществляется резервное копирование данных в облачной среде:
  - Данные, платформа, приложение, конфигурации, доступ?
  - Каким образом осуществляется проверка факта обеспечения поставщиком услуги непрерывности бизнеса?
- Полная зависимость от стабильности поставщика:
  - Что если поставщик изменяет предлагаемый им продукт?
    - Есть ли у Вас возможность контролировать внедрение программных исправлений или отслеживать другие события обновлений?
  - Что если облачная среда прекращает свое существование?
    - Каким запасом времени Вы располагаете, чтобы отреагировать на это?
- Каковы расходы в случае окончания срока эксплуатации?
  - Осуществим ли перенос данных?

Gartner

Сложность и подверженность влияниям внешней среды увеличивают вероятность возникновения рисков

Gartner

Разные модели облачных сред связаны с разного вида рисками

- Тогда как Ваш поставщик услуги имеет контроль над Вашими данными, Вы отнюдь не имеете контроля над:
  - Его сотрудниками, кодами, характеристиками, процессами;
  - Управляющей и юридической системой, корпоративной культурой.
- Кто за что отвечает?
  - Инфраструктура как услуга (IaaS): обеспечение безопасности- забота клиента;
  - Платформа как услуга (PaaS): безопасность обеспечивается с обеих сторон;
  - ПО как услуга (SaaS): обеспечение безопасности – забота поставщика услуги.
- Ваш поставщик услуги работает на основании договора субаренды?

Необходимо понимать: кто несет ответственность за какую функцию.

Gartner

Цепочка потребителей и поставщиков

- Кто поставляет услугу Вашему провайдеру?
  - Сервис «платформа как услуга», в первую очередь, используется мелкими компаниями-поставщиками ПО как услуги.
  - Многие сервисы «инфраструктура как услуга»/ «платформа как услуга»/ «ПО как услуга» предоставляются посредством удаленных систем.
- Вы работаете с интегрирующимися данными и смешанными сервисами (mashup)?
  - Из какого именно источника поступают Ваши данные/услуги?
  - Вы можете подтвердить свои права на использование?
- Вы являетесь участником чьей-то еще цепочки данных?
  - Есть ли возможность осуществлять контроль за Вашими данными на должном уровне?
  - Не стоит забывать о вероятности санкционированного гос. органами доступа к Вашим зашифрованным данным.

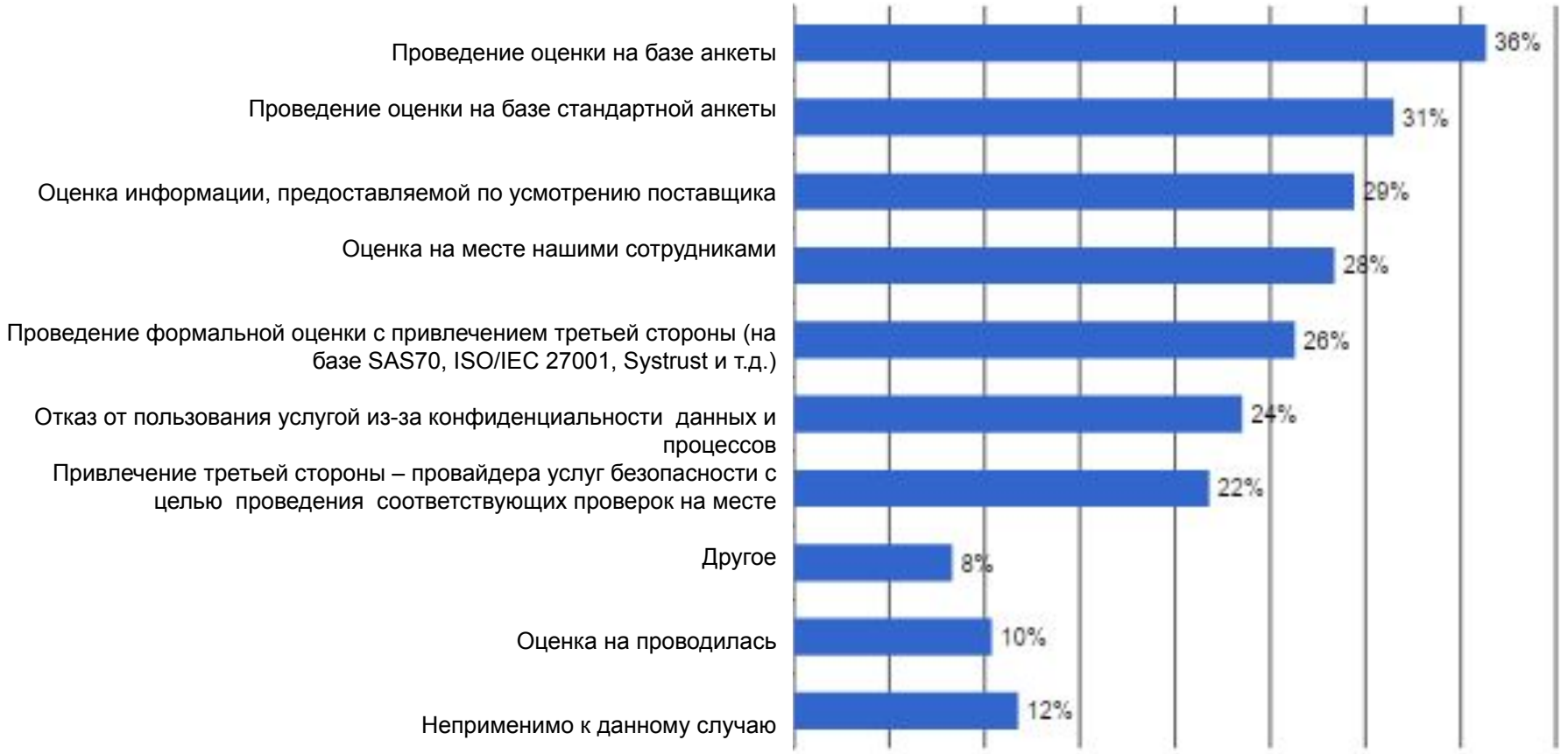
Какие механизмы контроля информационного доступа предоставляются самим поставщиком?

- Механизмы управления информационным доступом (IAM):
  - Интеграция данных, строгие проверки прав доступа к ресурсу, роли.
- Контроль и система оповещений о нарушениях:
  - Системы защиты от утечек данных, системы предотвращения вторжений, системы идентификации подписи, отслеживание активности базы данных.
- Можете ли Вы при необходимости провести аудиторскую проверку или расследование?
  - Каким образом можно проверить принадлежность кому-либо прав доступа к какой-либо информации? А также выяснить, кто совершал те или иные действия?
  - Как при необходимости провести электронное расследование?
  - Как провести криминалистическое расследование?
- Защита конфиденциальности данных:
  - Имеете ли Вы возможность управлять шифровальными ключами?
- Проверка целостности данных:
  - Удаляются ли данные с устройств на время их хранения или ремонта, или при списании?
  - Осуществляется ли резервное копирование данных? И каким образом: в сети либо вне сети?

Если они это не встраивают, Вы не сможете этим пользоваться.

Gartner

Результаты исследования: какие применялись методы оценки рисков использования «ПО как услуги»



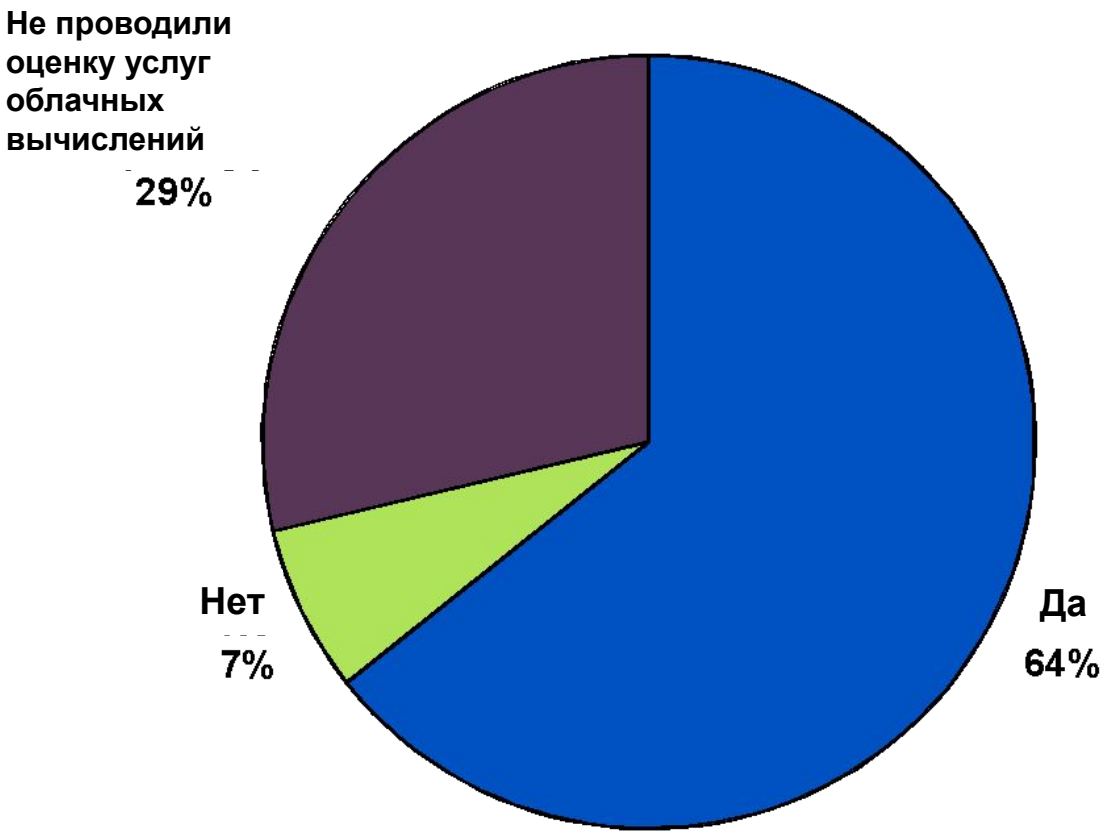
Клиенты и поставщики в равной степени выражают все больше недовольства методом оценки на базе стандартной анкеты.

(n=289, исследования проводилось Дек 10-Янв 11)

Gartner

Неприкосновенность частных данных и облачная среда

n=143



При оценке услуг облачных вычислений опиралась ли Ваша компания на нормы соблюдения неприкосновенности частных данных в качестве критериев отбора?

Gartner

Оценка рисков с учетом эксплуатационных условий

Фаза		Проектное решение	Внедрение	Использование/ операции
Процессы		- Функции систем безопасности - Архитектура - Набор характеристик	- Надежность кодировок	- Конфигурации - Техническое обслуживание
Форма выражения	**Документ**	- Разработка документации - Руководство по использованию	- Методы кодирования по документации - Код с комментариями по применению - Результаты тестов	- Сбор статистических данных за период эксплуатации - Записи о происшествиях
	Обязательство	- Параграфы контракта	- Стандарты кодирования	- Соглашение об уровне предоставляемых услуг (SLA)
	Тестирование	- Оценка архитектуры	- Проверка кодов; - Статичное тестирование - Динамичное тестирование	- Поиск уязвимых мест - Тест систем безопасности - Сертификация процессов
Квалификационные требования: **Сертификации** **Опыт** **Образование**		- Архитекторы	- Программисты	- Операционные менеджеры - Операторы

Достаточно ли вендор продемонстрировал зрелость на всех трех фазах?

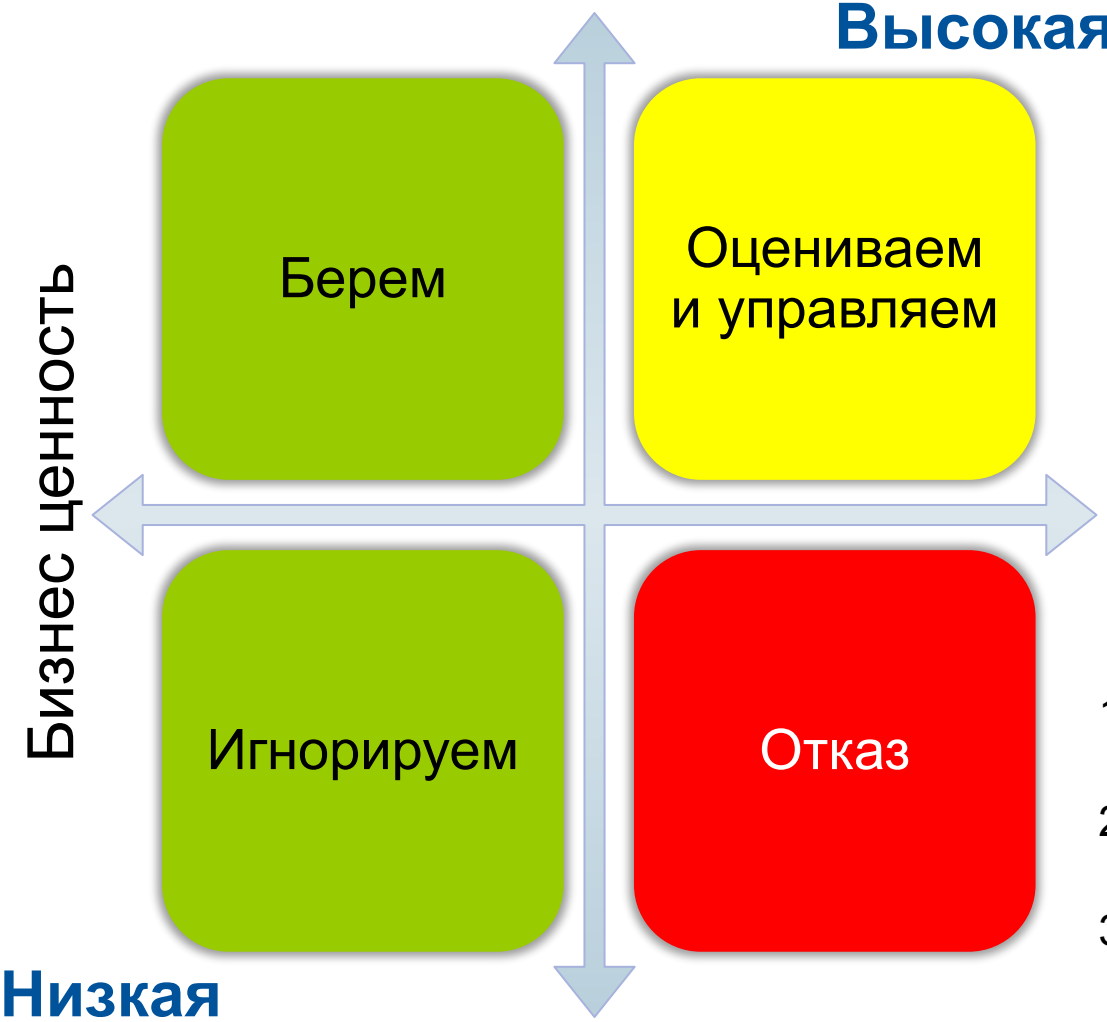
Gartner®

Можем ли мы использовать те же методы оценки рисков, что зарекомендовали себя на протяжении последних 20 лет?

- Адекватно ли оценивается проектное решение?
  - Где свидетельства полноценной и объективной оценки, проведенной опытными архитекторами систем информационной безопасности?
  - Отвечает ли набор функций всем требованиям, связанным с контролем рисков?
- Надежен ли код?
  - Какие языки программирования и среды использовались?
  - Проводилось ли статическое и динамическое тестирование?
  - Как проводилась проверка кода?
- Оценка надежности процессов должна стать последним этапом.
  - Легко применимо в случае с хорошо известными моделями и технологиями.
  - Вы просто не знаете о том, что что-то не знаете о новых ситуациях
- Стандартные подходы (27002, BITS, и т.д.) имеют ограничения.
  - Метод, использующий стандартный вопросник, не может адекватно оценить все факторы риска.
  - Если нам нужен метод, это еще не означает, что сгодится то, что есть.
  - Количественный анализ ничего не докажет.

Gartner

Опорная схема для оценки облачной среды: особое внимание обратите на критичные для Вашего бизнеса ситуации



Порядок проведения оценки

1. Проверка услуги на соответствие установленным стандартам
2. Проверка документации
3. Оценка рисков
4. Посещение предприятия поставщика

Порядок введения ограничений на использование услуги

1. Внедрение на предприятии соответствующей политики
2. Использование модуля доступа в сети (web proxy)
3. Технологии предотвращения утечек конфиденциальной информации (DLP)

Gartner

Рекомендации: разработайте стратегию безопасного использования услуг, предоставляемых внешними поставщиками

- ✔ Определите подходящие Вам сценарии пользования услугой для разных методов предоставления услуги, также оцените уровень риска и сопоставьте вероятность рисков с целями Вашей компании:
  - Вам необходимо понять, как получить максимальную выгоду от использования внешних ресурсов и облачных вычислений?
- ✔ Разработайте компетентные методы составления контрактов и проведения оценки:
  - В том числе и на основании таких критериев как безопасность, соблюдение необходимых норм и обеспечение непрерывности бизнес-процессов.
- ✔ Отберите и апробируйте решения, и перед запуском в эксплуатацию установите необходимые системы контроля.
- ✔ Используйте возможности использования услуги и работу специалистов по безопасности, чтобы полезность услуги для бизнеса стала очевидной.
- ✔ Рассмотрите возможность использования методологии оценки рисков Gartner.

Gartner

Другие исследования Gartner по данной тематике

- **«Результаты опросов: методы оценки рисков, связанных с использованием облачных сред, сервиса «ПО как услуга» и сред партнеров» («Survey Results: Assessment Practices for Cloud, SaaS and Partner Risks»)**
  Джей Хейзер/Jay Heiser (G00175916)
- **«Инструментарий: интерактивный журнал регистрации рисков, связанных с использованием внешних услуг» («Toolkit: Interactive Sourcing Risk Register»)**
  Франчес Кармузис и Фрэнк Риддер /Frances Karmouzis and Frank Ridder (G00174175)
- **«Анализ типов рисков, связанных с использованием облачных вычислительных сред и сервиса «ПО как услуга»» («Analyzing the Risk Dimensions of Cloud and SaaS Computing»)**
  Джей Хейзер/Jay Heiser (G00174873)
- **«Что Вам необходимо знать о безопасности и соблюдении нормативов в облачной среде» («What You Need to Know About Cloud Computing Security and Compliance»)**
  Джей Хейзер/Jay Heiser (G00168345)
- **«Лучшие практики разработки стратегии использования внешних ИТ услуг» («Best-Practice Process for Creating an IT Services Sourcing Strategy»)**
  Клаудио Да Рольд/Claudio Da Rold (G00153560)