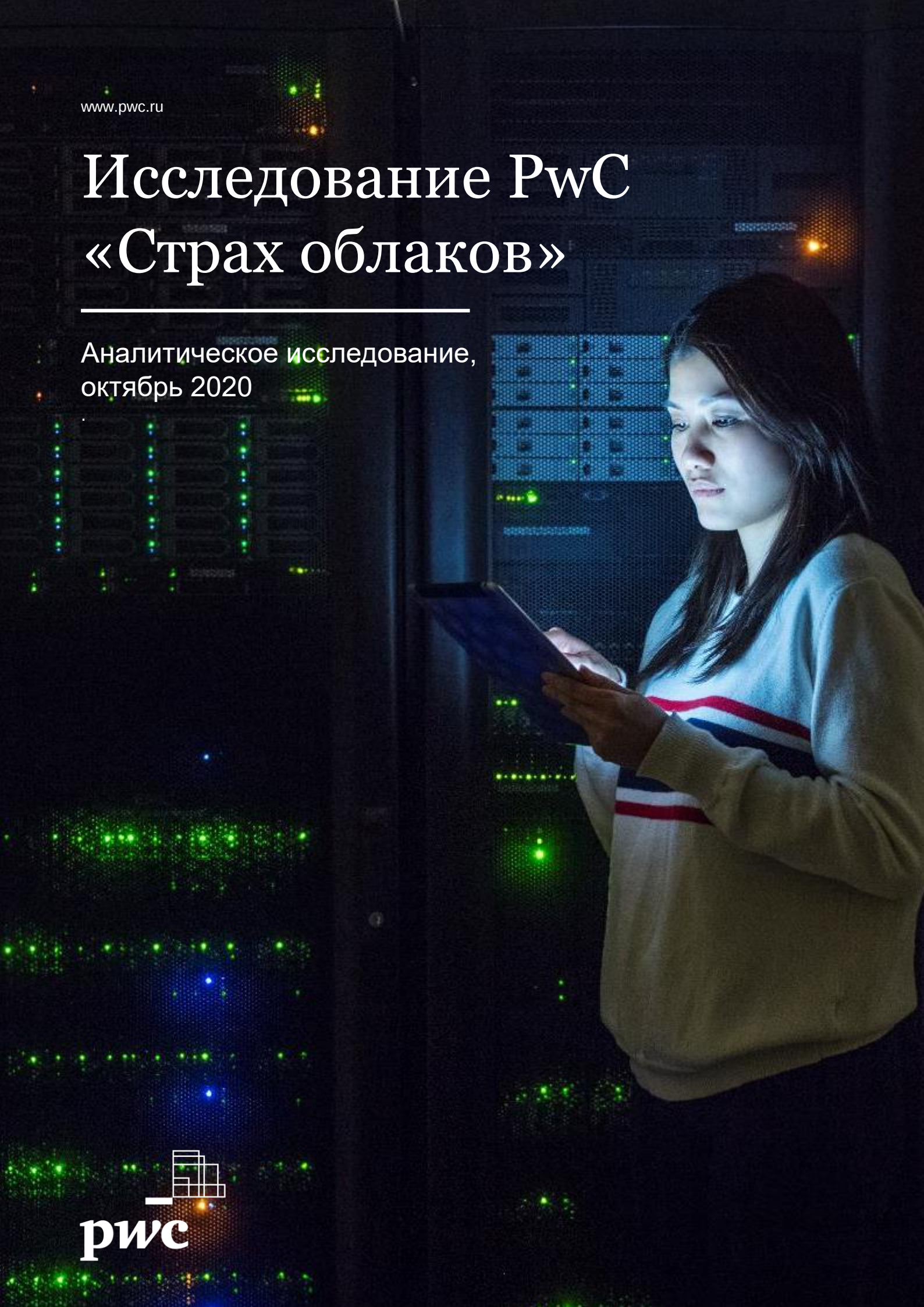
www.pwc.ru

Исследование PwC «Страх облаков»

Аналитическое исследование, октябрь 2020



pwc

Введение

Об исследовании

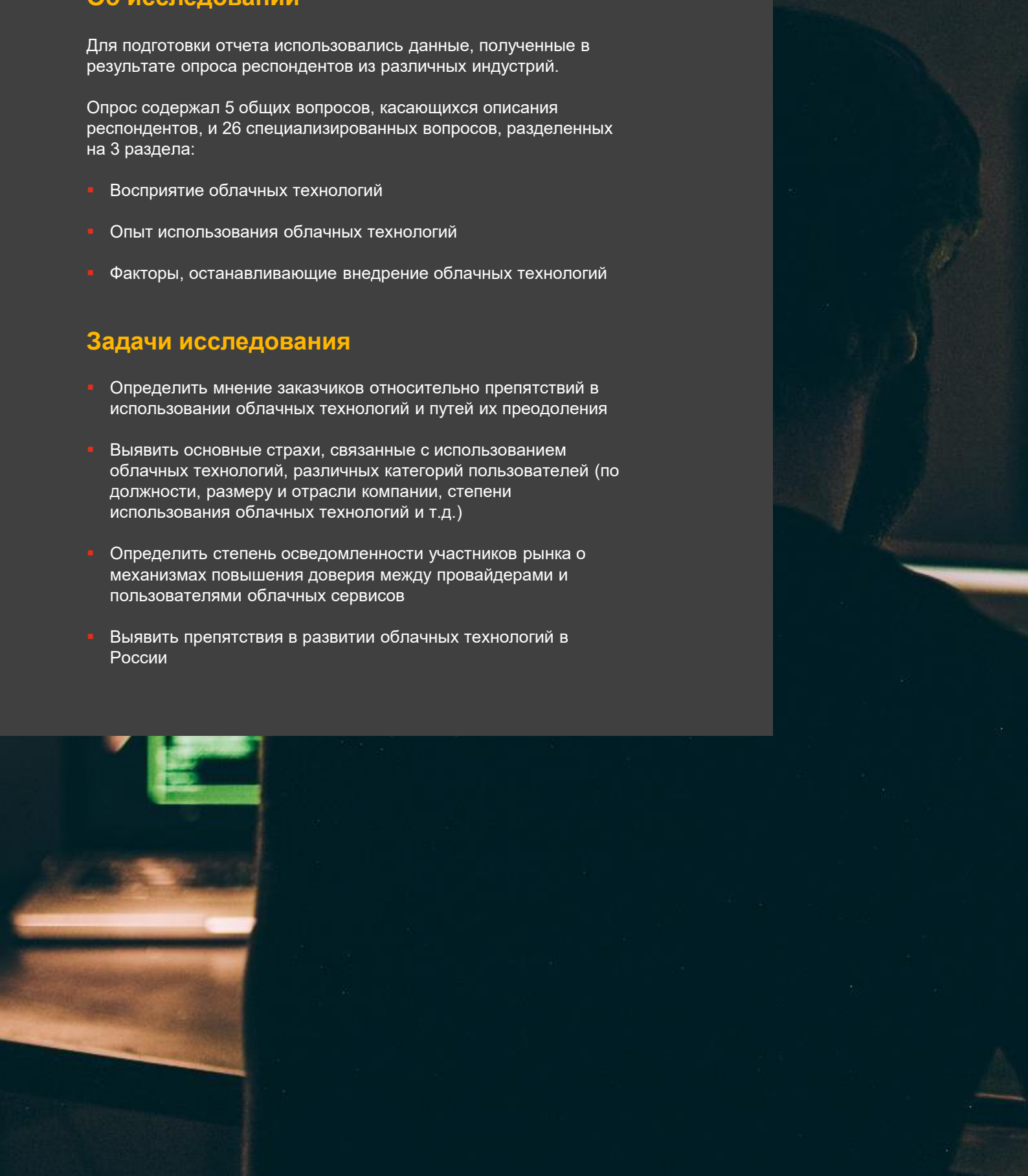
Для подготовки отчета использовались данные, полученные в результате опроса респондентов из различных индустрий.

Опрос содержал 5 общих вопросов, касающихся описания респондентов, и 26 специализированных вопросов, разделенных на 3 раздела:

- Восприятие облачных технологий
- Опыт использования облачных технологий
- Факторы, останавливающие внедрение облачных технологий

Задачи исследования

- Определить мнение заказчиков относительно препятствий в использовании облачных технологий и путей их преодоления
- Выявить основные страхи, связанные с использованием облачных технологий, различных категорий пользователей (по должности, размеру и отрасли компании, степени использования облачных технологий и т.д.)
- Определить степень осведомленности участников рынка о механизмах повышения доверия между провайдерами и пользователями облачных сервисов
- Выявить препятствия в развитии облачных технологий в России



По мере того, как компании переносят инфраструктуру в облако, вопрос облачной безопасности становится приоритетной задачей для все большего числа организаций. Многие компании по-прежнему с осторожностью относятся к облачным технологиям. Они видят на примере других компаний, какие преимущества дают облака, и знают о сильных сторонах данного решения.

Однако все равно боятся делать свой первый шаг. Возможно, они в чем-то и правы, облако не является оптимальным решением для каждого бизнеса. Все зависит от совокупности условий и обстоятельств. Но при правильном внедрении, разумном использовании и соблюдении принципов облачной безопасности, данная технология будет способствовать повышению эффективности бизнеса.

Мы рады представить вашему вниманию наше новое комплексное исследование, в котором рассказываем об отношении компаний в России к облачным технологиями и исследуем основные факторы, препятствующие их внедрению. Наше исследование акцентируется на таком важном явлении, как «страх организаций перед облаками», и причинами его возникновения.

Желаю вам приятного чтения!

Виталий Соколов

Партнер, руководитель практики по кибербезопасности и непрерывности бизнеса PwC в России

Характеристика респондентов

Должностной уровень респондентов

Респонденты в равной степени представляют основные должностные уровни в компаниях - C-level, средний менеджмент и специалисты (соответственно **29%**, **39%** и **32%**)

Менеджмент

39%

Специалист

32%

C - level

29%

В каком направлении вы работаете?

Если говорить о функциональной принадлежности, то здесь преобладает отдел информационных технологий - **около 52%**. Также среди респондентов присутствуют представители подразделений информационной безопасности, продаж и маркетинга, бухгалтерии и финансов.

Другое*

21%

Продажи

9%

Информационные технологии

52%

Информационная безопасность

18%

Другое*

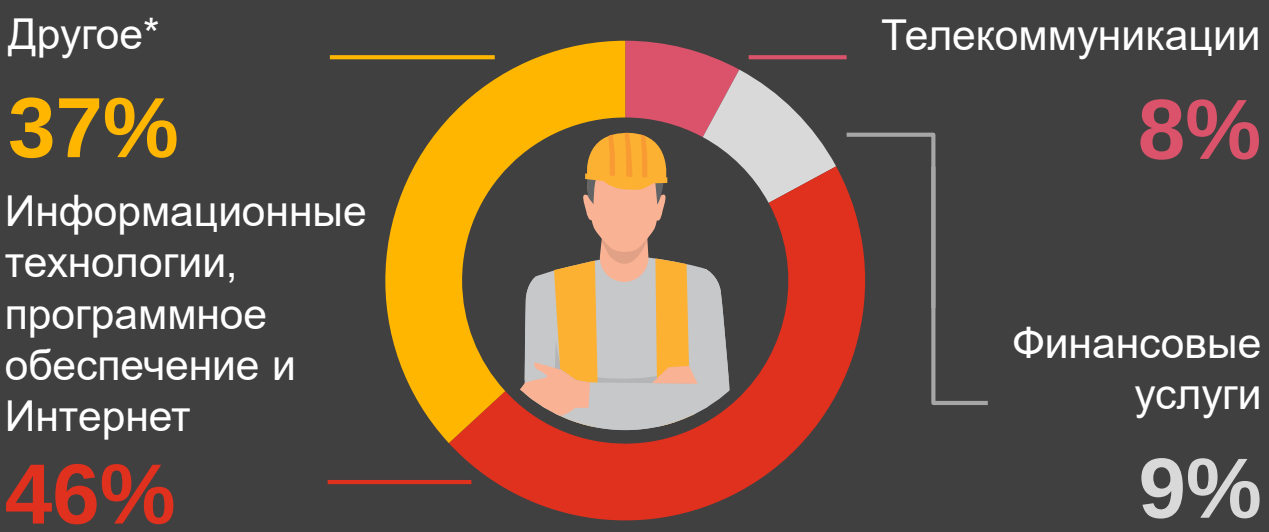
Бухгалтерия и Финансы - 4%; Внутренний аудит - 1%; Инжиниринг - 1%; ИБ + СБ - 2%; Логистика - 1%; Маркетинг - 3%; Управление персоналом - 3%; Управление продуктом - 5%; Юридическая служба - 1%

Численность сотрудников в компаниях респондентах

Основной аудиторией исследования были представители крупных организаций - от 1000 человек (**54%**), но малые и средние организации составляют значительную часть респондентов (**28%** и **18%**)

Основная сфера деятельности вашей компании?

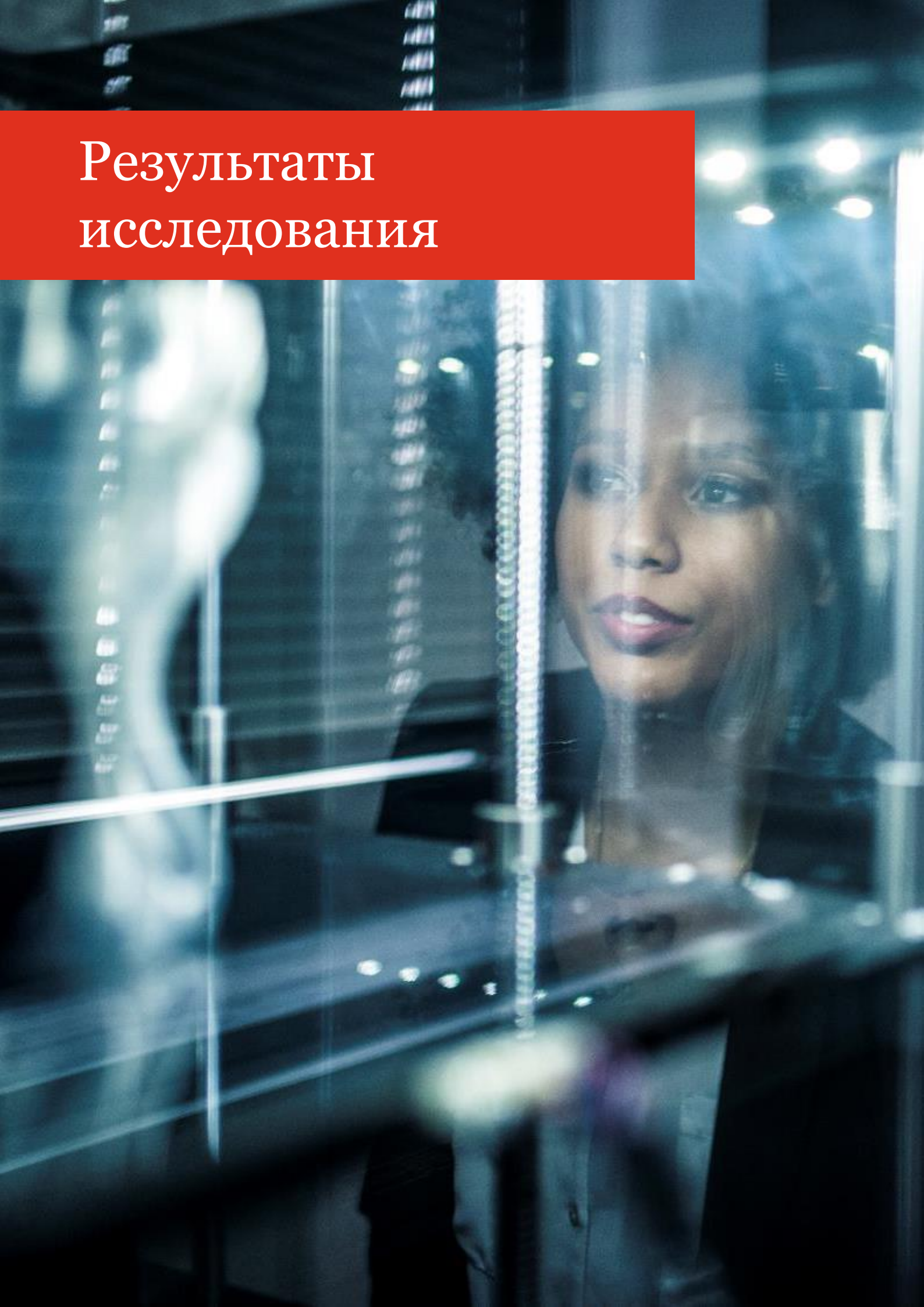
В рамках опроса была получена информация от представителей самых разных отраслей.



Другое*

Автомобильный бизнес - 1%; Государственное и муниципальное управление - 1%; Добыча и транспортировка полезных ископаемых - 5%; Здравоохранение, фармацевтика и биотехнологии - 1%; Медиа и развлечения - 3%; Недвижимость и строительство - 2%; Образование и исследования - 1%; Оптовая торговля и сбыт - 4%; Потребительские услуги - 3%; Производство - 2%; Профессиональные услуги - 3%; Розничная торговля - 5%; Системы безопасности - 1%; Страхование - 1%; Транспортировка и логистика - 4%.

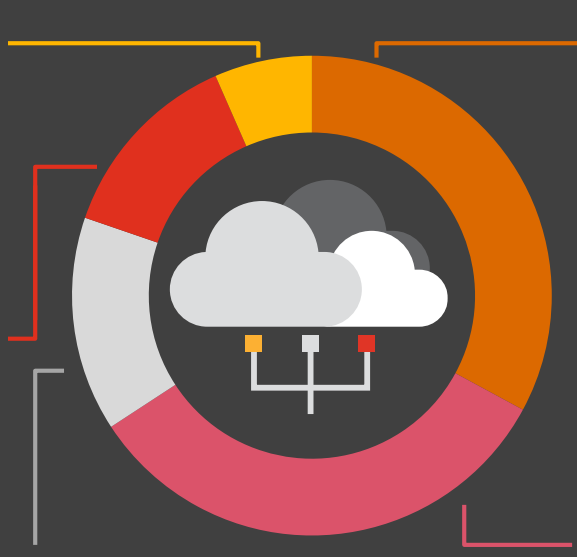
Результаты исследования



Восприятие облачных технологий

Стадии внедрения облачных технологий

Большинство компаний на текущий момент активно используют облачные технологии - 66% находятся на продвинутой или промежуточной стадии внедрения облачных технологий.

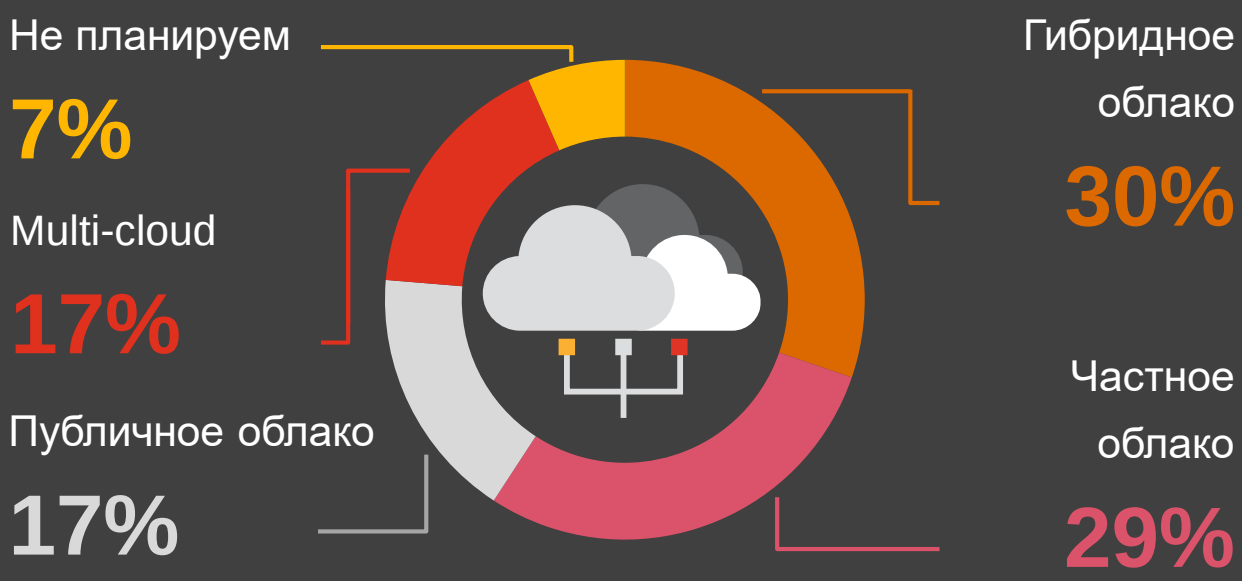


Стадии внедрения:

- **Отстающая** - Облачные технологии не применяются и нет планов по их внедрению
- **Наблюдающая** - Стратегия использования облачных технологий в разработке, сами технологии не применяются
- **Начинающая** - Облачные технологии в процессе внедрения/внедрены и реализованы как минимум для одного проекта
- **Промежуточная** - Облачные технологии используются для поддержания одного или нескольких процессов или систем; в планах расширение области применения облачных технологий
- **Продвинутая** - Облачные технологии задействованы для значительной части ИТ-инфраструктуры или процессов компании

Какой вид облака вы используете/планируете использовать?

При этом большая часть респондентов планирует использовать/использует гибридное (30%) или частное облако (29%). Такое решение соответствует общему уровню зрелости российского рынка облачных технологий и законодательным требованиям (“Закон о персональных данных”)



Типы облаков:

Публичное облако (англ. public cloud) — инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца — поставщика услуг (пример - Azure, Amazon Web Services, Яндекс.Облако).

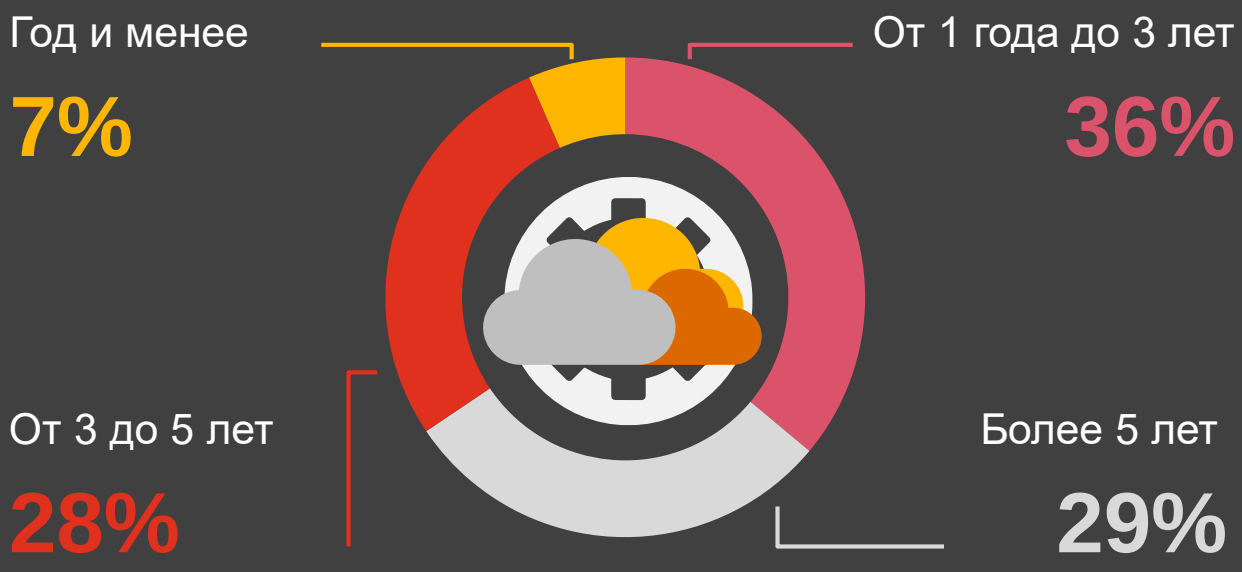
Частное облако - (англ. private cloud) — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Гибридное облако (англ. hybrid cloud) — это комбинация из двух или более различных облачных инфраструктур (частных или публичных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками).

Multi-Cloud стратегия - Использование нескольких облачных провайдеров в единой гетерогенной архитектуре. При типичной многооблачной архитектуре, использующей два или более публичных облака, а также несколько частных облаков, многооблачная среда нацелена на устранение зависимости от одного поставщика облачных услуг.

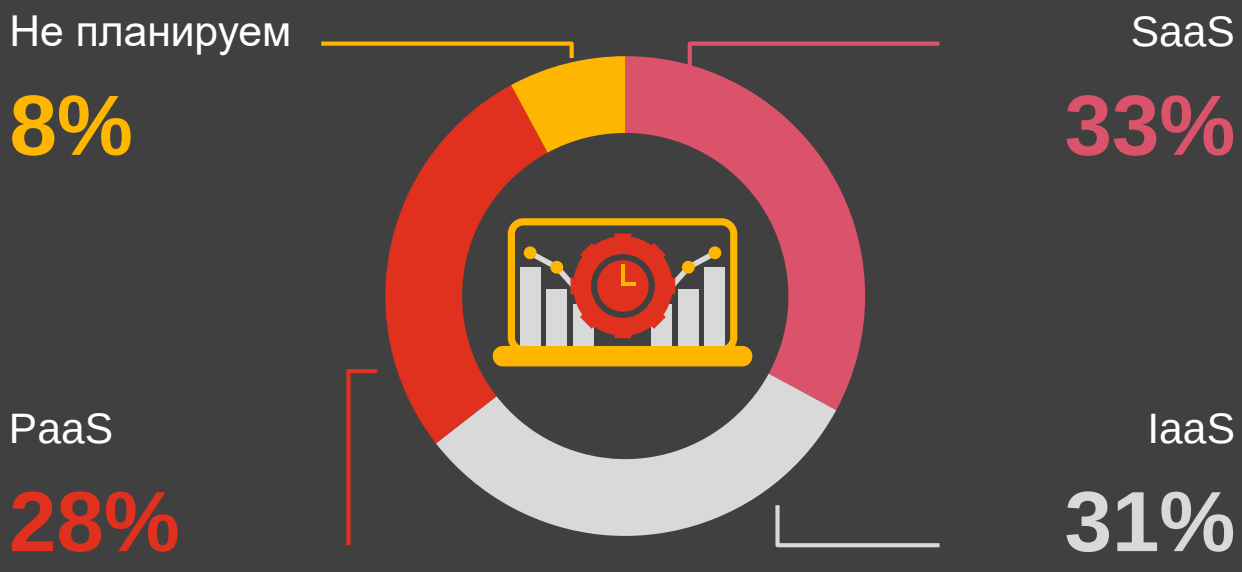
Как давно в компании используются облачные технологии?

Учитывая общий уровень развития ИТ-технологий в России, неудивительно, что облачные технологии в российских компаниях используются практически с момента их появления (30% компаний используют облачные технологии более 5 лет).



Какую модель предоставления сервиса Вы используете/ планируете использовать в большей степени?*

Активнее всего в российских компаниях используются/планируют использоваться облачные технологии в виде программного обеспечения как услуга (SaaS)



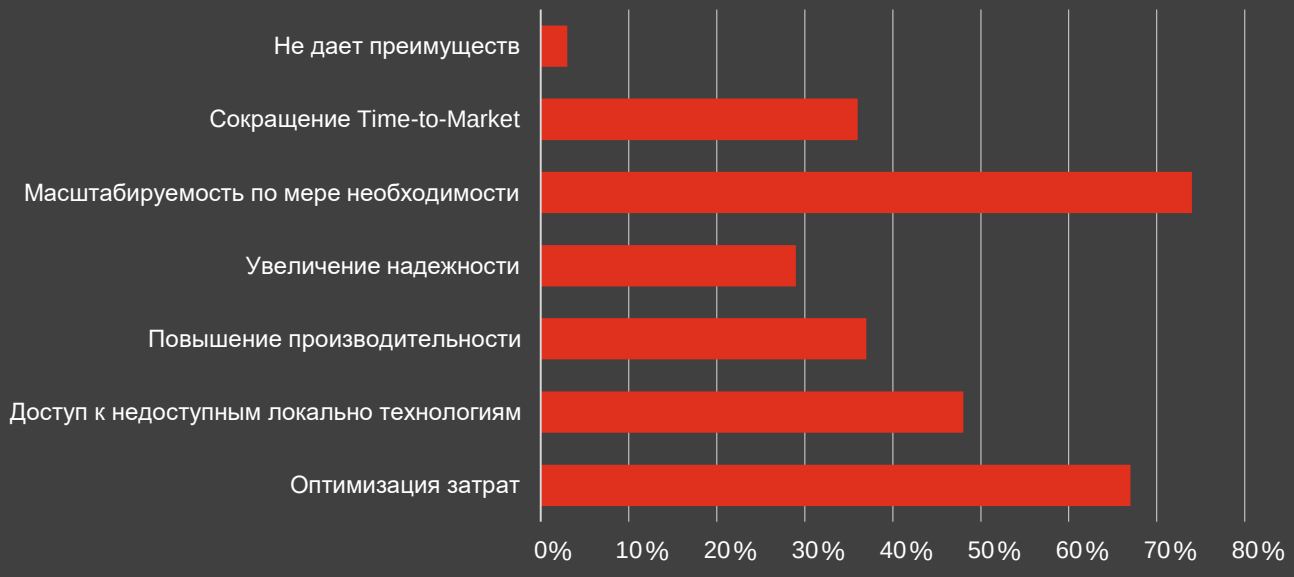
Модели предоставления сервиса*

IaaS - инфраструктура как услуга
PaaS - платформа как услуга
SaaS - программное обеспечение как услуга

Какие преимущества, по Вашему мнению, дает применение облачных технологий?

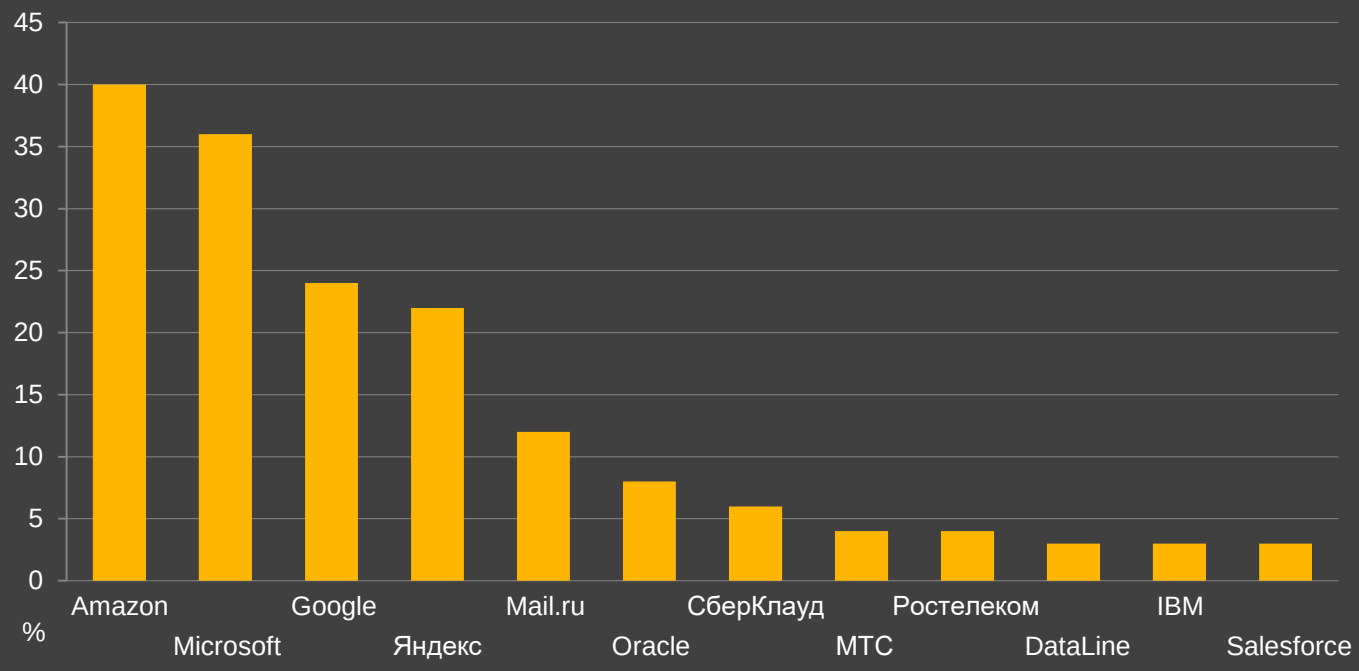
Результаты опроса показывают, что большая часть компаний выделяет такие основные преимущества внедрения облачных технологий, как:

- Масштабируемость по мере необходимости (**74%**)
- Оптимизация затрат (**67%**)
- Доступ к недоступным локально технологиям (**48%**)



Какие поставщики облачных технологий вам известны?

Большинство респондентов знакомы с мировыми лидерами на рынке облачных технологий (Big 3 - **Amazon, Microsoft, Google**), хорошо известны локальные поставщики облачных технологий, предоставляющие услуги публичного облака **(Яндекс.Облако, Mail.ru**)



Укажите, пожалуйста, наиболее важные факторы, влияющие на выбор провайдера облачных технологий

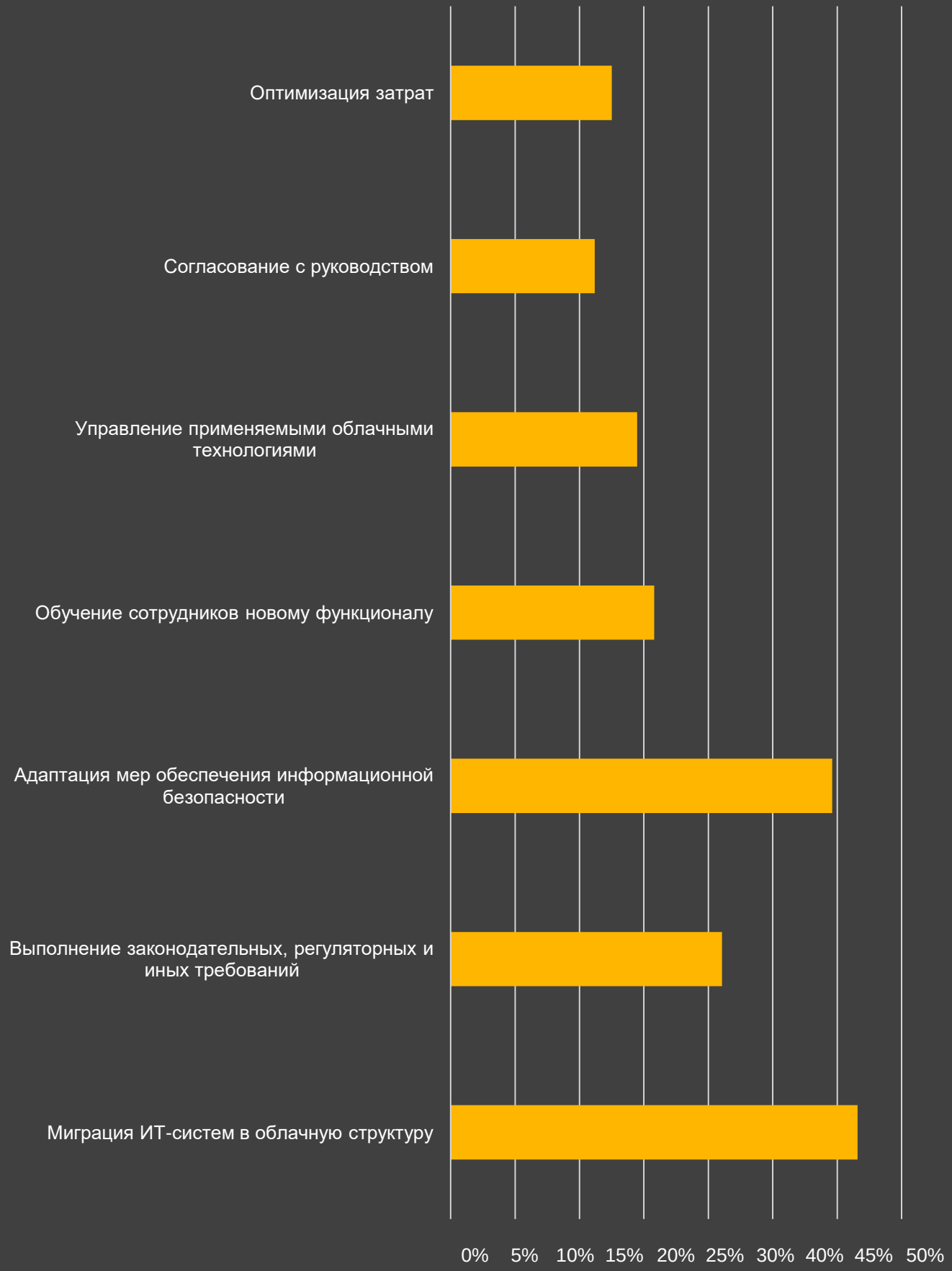
Функциональные и технологические требования являются наиболее важными при выборе облачного провайдера, вопросы безопасности и соответствия нормативным требованиям отходят на второй план:

41% - Наличие надежных каналов связи, современных средств защиты от DDoS-атак
38% - Наличие дата-центров в России
34% - Низкая цена, понятное и гибкое ценообразование

Самые сложные задачи при переходе на облачные технологии:

Вопросы миграции ИТ-систем в облако и адаптации текущих инструментов являются наиболее сложными задачами:

63% - Миграция ИТ-систем в облачную структуру
59% - Адаптация мер обеспечения информационной безопасности
42% - Выполнение законодательных, регуляторных и иных требований

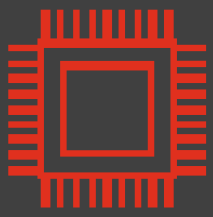


Опыт использования облачных технологий

Какие услуги и рабочие нагрузки развертываются в облаке в Вашей организации?

74%

Хранилище (объектное хранение, архивы, резервное копирование и т.д.)



67%

Виртуальные серверы

51%

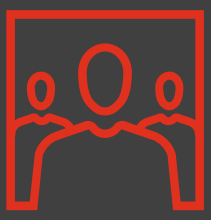
Базы данных (реляционная, NoSQL, кэширование и т.д.)

Контейнеры - 34%; Сетевое взаимодействие и доставка контента (виртуальное частное облако, CDN, DNS и т.д.) - 34%; Безопасность (управление идентификационными данными, контроль доступа, защита данных, обнаружение угроз, мониторинг использования и ресурсов, антивирусная защита и т.д.) - 30%; Разработка / Приложения для тестирования - 46%; Приложения для коммуникации (электронная почта, совместная работа, обмен мгновенными сообщениями и т.д.) - 46%; Бизнес-приложения (CRM, автоматизация маркетинга, ERP, BI, управление проектами и т.д.) - 52%; Виртуальные рабочие места и приложения - 16%; Приложения для ИТ-операций (администрирование, резервное копирование, мониторинг ИТ-инфраструктуры и т.д.) - 30%

Какую информацию Вы храните в облаке?

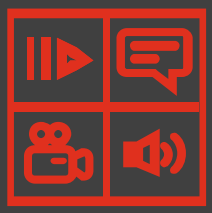
56%

«Электронная» почта



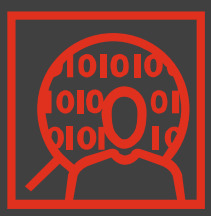
40%

Данные о клиентах



46%

Маркетинговая информация / новости / медиа



33%

Данные о сотрудниках

52% компаний используют больше одного облачного провайдера

Как Вы защищаете данные в «облаке»?

48%

Мы подключаемся к облаку через защищенные каналы связи

41%

Мы используем шифрование или токенизацию

39%

Мы используем службы безопасности, изначально предлагаемые облачным провайдером

В вопросе безопасности облачных технологий важна возможность использовать текущие привычные и хорошо изученные инструменты информационной безопасности:

- **У 34%** компаний все возможности их традиционных инструментов и устройств информационной безопасности работают в облаке
- **У 25%** компаний текущие инструменты информационной безопасности работают в облачной среде с ограниченным функционалом

Останавливающие факторы при переходе на облачные технологии

В рамках исследования респондентам было предложено назвать основные останавливающие факторы, с которыми они сталкиваются при переходе на облачные технологии. Главные возникающие сложности это:

- Сложность / техническая невозможность миграции в облако - **38%**
- Сложно / невозможно выполнять требования законодательства - **34%**
- Высокая стоимость облачных технологий - **33%**

58% - Сомневаются в безопасности облаков

Большинство «Не уверены» или «Больше не уверены, чем уверены» в безопасности общедоступных облаков (Public Cloud).

Основой этих сомнений послужило “**мнение со стороны**”:

61% - Информация об утечках в общедоступных облаках
42% - Мнение внутренних / внешних экспертов

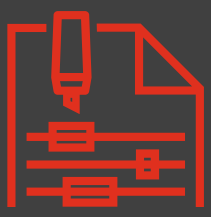
Происходил ли в вашей организации инцидент, связанный с безопасностью в общедоступном "облаке", за последний год?

5% Да

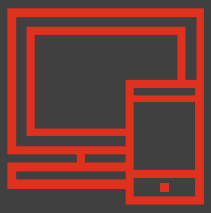
9% Нет, но был с локальной инфраструктурой

20% Не уверен

Основные типы произошедших инцидентов:



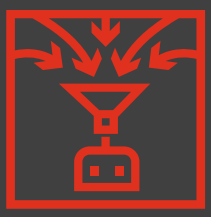
36%
Утечки данных



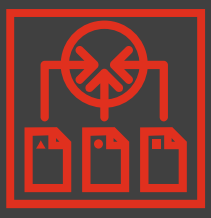
45%
Заражение вредоносным ПО

27%
Взлом учетных записей

Какие самые большие проблемы с безопасностью Вы видите в «облаке»?



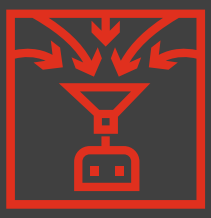
57%
Возможность утечки данных



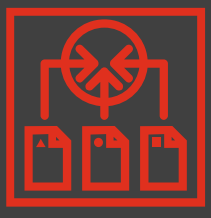
51%
Нецелевое использование конфиденциальных данных провайдером или третьей стороной

45%
Возможность потери / удаления данных

Что Вы считаете самыми большими угрозами безопасности в «облаках»?

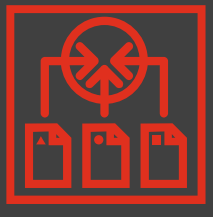


45%
Несанкционированный доступ



38%
Неправильная настройка облачных сервисов

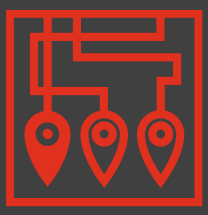
36%
Кража данных



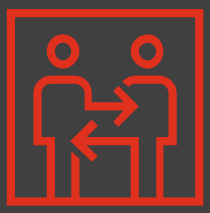
31%
Недостаточность мер защиты со стороны провайдера

По мнению респондентов, риск нарушения безопасности в общедоступной облачной среде **выше** по сравнению с традиционными локальными IT-средами (36% считают, что риск значительно выше, 13% считают, что риск чуть выше). 34% респондентов считают риски нарушения безопасности в “облаке” и в локальной IT-среде одинаковыми. Лишь 10% респондентов считают, что риски в облачной среде ниже чем в локальной IT-среде.

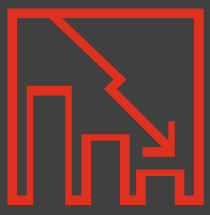
Наиболее значительные риски, связанные с применением облачных технологий:



54%
Наличие доступа к критичным данным у сотрудников облачного провайдера

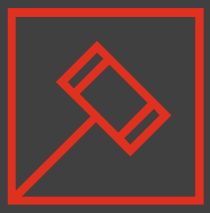


38%
Отсутствие гарантий безболезненной миграции процессов от одного провайдера к другому или от провайдера на внутреннюю площадку



37%
Низкая контролируемость процессов, поддерживаемых облачными технологиями

34%
Нарушение изолированности данных компании, хранимых облачным провайдером, от данных других его клиентов



32%
Нарушение законодательных, регуляторных или иных требований

29%
Небезопасное / неполное / несвоевременное удаление данных облачным провайдером

Трудности обеспечения безопасности облачных технологий

Каковы ваши самые большие ежедневные трудности в работе, связанные с безопасностью в "облаке"?

- Обеспечение соответствия законодательным, регуляторным и иным требованиям - **23%**
- Наглядность в безопасности инфраструктуры - **21%**
- Безопасность не может идти в ногу с темпами изменений в новых / существующих приложениях - **20%**
- Отсутствие интеграции с локальными технологиями безопасности - **20%**
- Отсутствие автоматического обнаружения угроз и контроля безопасности инфраструктуры - **17%**

Какая часть процесса обеспечения соответствия нормативным требованиям для облачных вычислений является наиболее сложной?

- Мониторинг соблюдения политик и процедур - **37%**
- Актуализация новых/изменяющихся нормативных требований и требований к соответствию - **37%**
- Мониторинг новых уязвимостей в облачных службах - **34%**
- Оценка рисков в облачной среде - **33%**

Каковы основные барьеры, сдерживающие внедрение облачных вычислений в Вашей организации?

- Риски потери и утечки данных - **47%**
- Потеря контроля при переходе в облако - **24%**
- Страх перед блокировкой провайдера облачных технологий - **24%**
- Недостаточная прозрачность и информативность облачных ресурсов - **21%**
- Внутреннее сопротивление и инерция - **20%**
- Соответствие законодательству, регуляторным и иным требованиям - **18%**

При этом **значительная часть респондентов готова полагаться на «документы»** - **51%** «Открытая и полноценная документация по используемым технологиям и их безопасности» и «Отчеты внешних аудиторов» - одни из наиболее популярных способов контроля, которые могли бы повысить уверенность респондентов в безопасности облаков

Заключение

Резюме

- Компании активно используют облачные технологии, но не уверены в их безопасности
- Функциональные и технологические требования превалируют над вопросами безопасности при выборе облачного провайдера
- Компании хранят в облаке конфиденциальные и персональные данные
- Риски нарушения безопасности в общедоступной облачной среде оцениваются выше по сравнению с традиционными локальными IT-средами
- Основной “страх” при использовании облачных технологий - возможность несанкционированного доступа, в том числе и сотрудниками облачного провайдера
- Самый сложный вопрос, связанный с облачной безопасностью - обеспечение соответствия законодательным и регуляторным требованиям
- Открытая документация и отчеты внешних аудиторов - наиболее важные способы контроля, которые могли бы повысить уверенность в безопасности облаков

Организации активно перемещают свою инфраструктуру и приложения в облако. Использование облака имеет фундаментальное значение для решения некоторых из проблем, связанных с удаленной работой, ведением критически важных бизнес-процессов и обеспечением доступа к ключевым бизнес-системам. В текущей ситуации компании сталкиваются с проблемой развертывания служб удаленного доступа, защищенных каналов связи и различных сервисов для совместной работы, выстраивают новые процессы взаимодействия с партнерами, создают новые цепочки поставок и обрабатывают огромное количество информации. И эти процессы обязаны быть безопасными. Таким образом, укрепление стандартов безопасности "облачных" вычислений станет приоритетом бизнеса, стандартом и требованием рынка.

При этом отделы Информационной Безопасности предприятий обеспокоены тем, что внедрение облачных технологий часто не согласуется с ними, и хотели бы получить подробную информацию о текущем состоянии безопасности их "облачной" среды.

Текущие вызовы:

- Облачные инициативы часто стимулируются бизнесом, оставляя на второй план безопасность, конфиденциальность, управление рисками и соответствие нормативным требованиям.
- Корпоративные политики, стандарты и инструкции, касающиеся безопасности, часто являются устаревшими или несовместимы с облачными средами, что затрудняет внедрение облачных технологий.
- Соблюдение правовых, нормативных и договорных обязательств затруднено в связи с отраслевыми законами, другими нормативными актами и требованиями.
- Традиционные способы защиты инфраструктуры не могут обеспечить полноценную безопасность облачных технологий.
- Безопасная интеграция облачных технологий с бизнес-процессами и ИТ-инфраструктурой необходима для поддержания комплексного подхода к безопасности (люди/управление, инфраструктура и ее предоставление).
- Консолидированный анализ контроля доступа, прав и ролей пользователей затруднен, особенно среди разных провайдеров облачных технологий.

Ваши следующие шаги:

Вы планируете использовать облачные технологии:

- Интегрировать вопросы безопасности, конфиденциальности и управления рисками в общий бизнес-план и дорожную карту по переходу на облачные технологии.
- Модернизировать корпоративные политики, процедуры, стандарты и внутренние процессы управления для поддержки внедрения облачных технологий.
- Определить и внедрить требования к возможностям IAM в облачной среде, расширить функционал традиционного IAM, где это применимо, и устранить любые выявленные недостатки.
- Оценить безопасность облачной среды перед внедрением и ее соответствие ведущим практикам в облачной безопасности (например стандарты CIS и CSA), провести комплексный анализ безопасности облачного провайдера с рекомендациями по исправлению недостатков.

Вы уже используете облачные технологии:

- Выявить с помощью внешнего аудита пробелы в защите данных и конфиденциальности, юридических, нормативных требованиях и договорных обязательствах, которые могут применяться.
- Встроить меры безопасности облачных технологий в общую систему информационной безопасности для снижения риска угроз и быстрого исправления уязвимостей.
- Определить и внедрить процессы для реагирования на угрозы; подготовить команды и планы реагирования на инциденты в компании; проанализировать реакции клиентов и акционеров на угрозы и принять меры по их устранению.
- Управлять рисками третьих лиц - категоризация и классификация групп пользователей и контроль доступа к ним.
- Обеспечить соответствие "облачной" среды отраслевым нормативам (например, NIST, ISO, HIPAA, PCI) и политикам внутренней безопасности.

Используемые мировые практики и стандарты облачной безопасности:

- **Center for Internet Security -** CIS Controls Cloud Companion Guide
- **ISO -** ISO/IEC 27017:2015
- **Cloud Security Alliance -** CSA Cloud Controls Matrix
- **NIST -** SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing

Контакты

Виталий Соколов
Партнер, руководитель практики по кибербезопасности и непрерывности бизнеса PwC в России
+7 (495) 967 6153
vitaly.l.sokolov@ru.pwc.com

Михаил Курзин
Директор, практика по кибербезопасности и непрерывности бизнеса PwC в России
+7 (495) 223 5040
mikhail.kurzin@ru.pwc.com

Павел Николаев
Старший менеджер, руководитель практики по обеспечению безопасности облачных систем PwC в России
+7 (966) 062 3167
pavel.nikolaev@pwc.com