ИНСТИТУТ
ЭКОНОМИЧЕСКОЙ
ПОЛИТИКИ
имени Е.Т. ГАЙДАРА

Апрель 2022

# Исследование использования облачных сервисов в проектах «ГосОблако» и «ГосТех»

# Содержание

Данное исследование направлено на анализ процесса перехода государственных информационных систем на облачные технологии, в частности, в рамках проектов «ГосОблако», «ГосТех».

Целями исследования являются изучение международных стандартов и практик зарубежных стран (США, ЕС, Италии, Германии) по переводу государственных информационных систем на облачные технологии, изучение процессов создания государственных облаков в России, а также возникающих в связи с таким переходом правовых проблем, включая вопросы прохождения аттестации ФСТЭК, проблемы осуществления государственных закупок и пр.

Например, одной из проблем использования облачных технологий в проектах «ГосОблако» и «ГосТех» является необходимость реализации подхода мультиоблачности (multicloud). Такой подход позволяет создавать коммунальное облако (а не частные облака под каждую геоинформационную систему (далее – ГИС), которая переносится в облако), чтобы существовала возможность при необходимости переходить из одного облака в другое, гарантируя обеспечение безопасности данных, эластичность, масштабируемость, совместимость.

Также существует необходимость развития законодательства о закупках для возможности использовать гибкую систему закупок для оплаты услуг в зависимости от их использования (принцип «pay-as-you-go»).

Данное исследование предназначено для государственных органов в части возможности изучения международного опыта, который может быть применим при развитии проектов «ГосОблако», «ГосТех»; изучения основных проблем, связанных с переходом государственных органов на облачные технологии; изучения ситуации на российском рынке поставщиков услуг.

Также исследование может быть полезным для поставщиков облачных услуг и других заинтересованных лиц в части понимания того, как развивается использование облачных услуг государством.

# Введение.
# Что такое облачные вычисления?

Государственные облачные системы сегодня развиваются в ряде стран, например в США, странах ЕС (Германии, Италии), Великобритании, Австралии, Сингапуре и ряде других стран. Поэтому международные организации активно разрабатывают стандарты использования облачных технологий, например, Международная организация по стандартизации (ИСО) разрабатывает стандарты использования облачных технологий, Организация экономического сотрудничества и развития (далее – ОЭСР) исследует политики стран в области защиты данных и вопросов закупок облачных технологий, Международный союз электросвязи (МСЭ) создает технические стандарты использования облачных технологий.

Сегодня отсутствует единый подход к определению понятия «облачных вычислений». ОЭСР как международная организация, которая объединяет опыт зарубежных стран, в публикации «Измерение цифровой трансформации: дорожная карта для будущего» 2019 г. дает широкое определение **облачным вычислениям** – это ИКТ-услуги, доступ к которым осуществляется через Интернет, включая серверы, хранилища, сетевые компоненты и программное обеспечение[1].

В международной практике выделяются **3 модели** облачных вычислений[2]:

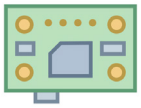
### 1. инфраструктура как услуга (infrastructure as a service, IaaS)

При оказании услуг IaaS пользователям облаков предоставляются **вычислительные ресурсы**, включая ресурсы для и зучения, обработки, хранения и сети, которые пользователи могут использовать для виртуализации. Например, пользователи могут получать доступ к серверам, сервисам для хранения, службам резервного копирования, запускать операционные системы и программное обеспечение на вычислительных ресурсах.

Примеры поставщиков: AWS, Microsoft Azure, Google Cloud, VMware, OpenStack.

### 2. платформа как услуга (platform as a service, PaaS)

При оказании услуг PaaS пользователям предоставляется платформа для **развертывания собственных приложений и сервисов**, включая языки программирования и дополнительные инструменты. При этом пользователи не имеют доступа к управлению и контролю за базовой инфраструктурой (сетям или операционным системам). Поставщики PaaS используют специальные интерфейсы прикладного программирования (API).



Примеры поставщиков: AWS Elastic Beanstalk, Heroku, Red Hat OpenShift, Cloud Foundry, Github, Kubernetes, Docker.

1 OECD (2019), Measuring the Digital Transformation: A Roadmap for the Future, OECD Publishing, Paris. https://doi.org/10.1787/9789264311992-en

2 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2011)19/FINAL&docLanguage=En

### 3. программное обеспечение как услуга (software as a service, SaaS)

В модели SaaS пользователи получают **доступ к приложениям поставщика** облачных услуг, например, к приложениям электронной почты, бизнес-приложениям, программным решениям для управления (инструменты управления взаимоотношениями с клиентами, управления документами или бухгалтерского учета) и пр.

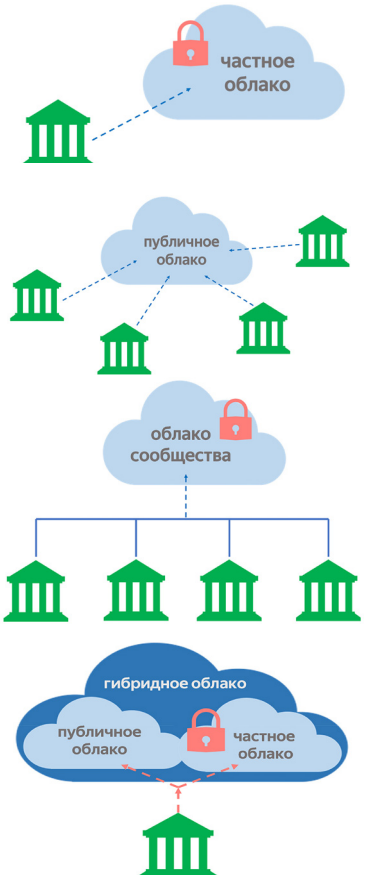
Примеры поставщиков: Dropbox, Salesforce, Google Apps, Red Hat Insights, Slack, Trello, Office 365.

Три уровня услуг представлены на рис. 1.


**Рис. 1. Модели облачных услуг**

**Существуют 4 типа облаков**[1]:

1. **частное облако (private cloud)** – модель, при которой одна компания имеет в собственности или арендует центры обработки данных. Базовое оборудование, программное обеспечение и сетевая инфраструктура не доступны для совместного использования с другими компаниями. То есть облаком **управляет сама компания** или провайдер, облако может быть размещено как внутри компании, так и за ее пределами.
2. **публичные облака (public clouds)** – модель, при которой поставщик предоставляет вычислительные ресурсы и инфраструктуру, а центр обработки данных становится **общедоступным** для широкого круга пользователей.
3. **облака сообщества (community clouds)** – модель, при которой облака могут быть как частные (**используются сообществом** с общими целями, например, небольшими организациями или исследовательскими институтами), так и публичные (используются реселлерами облачных сервисов, которые объединяют услуги различных облачных провайдеров и перепродают их).
4. **гибридные облака (hybrid clouds)** – модель, при которой используют **частную и общедоступную инфраструктуру**, то есть часть центра обработки данных зарезервирована для одного арендатора (как в частном облаке), а остальная часть доступна для общественности (как в публичном облаке).




1 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2011)19/FINAL&docLanguage=En

Использование облачных технологий несет ряд выгод для государства.

### 1. снижение издержек для государства

Государству как пользователю облачных технологий, не нужно дополнительно инвестировать в создание и поддержку собственной ИКТ-инфраструктуры или программного обеспечения, так как государство может **закупать облачные вычислительные** ресурсы у сторонних поставщиков.

**NB!** По данным VMware, при применении подхода мультиоблачности на **38%** сокращаются операционные расходы на ИТ.

Исследование перехода Государственного департамента США, города Лос-Анджелеса, штатов Калифорнии, Вашингтона, Майами, округа Колумбии, и пр. на облачные технологии выявило **потенциал экономии** средств при переходе на облачные технологии для правительств от **25%** до **50%**. Например, Федеральное управление по трудовым отношениям США перевело свою систему управления делами на облачное решение в рамках SaaS и снизило общий размер затрат **на 88 % за 5 лет**. Управление наземного транспорта Сингапура выявило **60% экономию средств** при переходе на облачные технологии.

### 2. использование облачных услуг с учетом потребностей

Услуги облачных вычислений возможно использовать с учетом потребностей, то есть государственные органы могут получить доступ к стольким ресурсам, сколько необходимо для выполнения функций и по мере необходимости могут увеличивать или уменьшать количество ресурсов, при этом оплата будет происходить за каждое использование или количество данных, которые хранятся в облаках (по модели **«оплата по мере использования»** (pay-as-you-go).
Это снижает риски избыточности, например, если государственный орган чрезмерно закупил вычислительные ресурсы, которые простаивают, а также риски нехватки ресурсов в пиковые моменты.

### 3. ускорение и оптимизация процессов

Облачные технологии позволяют государственным органам ускорять и оптимизировать процессы, например, за счет возможностей удаленного обмена информацией. Например, Департамент информационных и коммуникационных технологий Филиппин в 2017 г. использовал облачные технологии для автоматизации системы выдачи разрешений на ведение бизнеса и лицензирования, что позволило местным органам власти обрабатывать заявки на получение и продление разрешений на ведение бизнеса онлайн, сократив продолжительность процесса с 2–3 дней до нескольких часов..

Стоит отметить, что зарубежные страны внедряют облачные технологии по принципу **мультиоблачности (мультиклаудного облака)**.

**NB!** Экономия средств при переходе на облачные технологии для государственных органов – от **25%** до **50%.**

То есть осуществляют закупку услуг от разных поставщиков, которые лучше всего подходят для требуемой услуги, в том числе закупку одной и той же услуги у нескольких поставщиков.

Применение подхода мультиоблачности обеспечивает более высокое качество сервисов за счет их предоставления специализированными поставщиками вместо множества сервисов от одного «универсального» поставщика.

Мультиоблачность облегчает внедрение инноваций (можно закупить отдельные более инновационные услуги, которые нет у текущих поставщиков услуг), позволяет распределить нагрузку между поставщиками (особенно во время пиковой нагрузки на работу сервиса), дает возможность перенести данные (например, если один поставщик остановит работу, или произойдет инцидент, связанный с безопасностью) и пр.

# I. Проекты государственных облаков в России

## Проект «Гособлако»

### Что такое «ГосОблако»?

На данный момент правовое закрепление **понятия «государственного облака»** предложено в проекте федерального закона о внесении изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ID проекта 01/05/11-21/00122604), разработанном Минцифры России.

Под данным термином понимается *«совокупность унифицированных облачных услуг, оказываемых независимыми поставщиками с применением предоставляемой ими собственной или арендуемой информационно-коммуникационной инфраструктуры, объединяемая и управляемая государственной информационной системой управления распределенной информационно-коммуникационной инфраструктурой, предназначенной для размещения и функционирования информационных систем и ресурсов органов государственной власти, органов местного самоуправления и государственных внебюджетных фондов».*

В Облачной стратегии **Великобритании** принят другой подход к термину «государственное облако» – *постоянная и повторяющаяся рабочая программа, которая позволяет использовать ряд облачных услуг и менять способы приобретения и эксплуатации ИКТ во всем государственном секторе.*

Таким образом, в стратегическом документе Великобритании определение дано через возможности государственного облака как комплекса мероприятий по внедрению технологий в работу органов власти.

В **Сингапуре** термин «Центральное государственное облако» (Central G-Cloud) определяется как *инфраструктура, представляющая собой частное облако государственного сектора и обеспечивающая ресурсы облачных вычислений для нужд государства.*

Стоит отметить, что в зарубежных странах термин «государственное облако» обычно **не закрепляется нормативно**. Вместо этого для определения используемых для целей государственного управления, государственной службы, предоставления государственных услуг и т.д. облачных технологий адаптируется термин «облачные вычисления».

В Стратегии развития облачных технологий **ЕС** (Cloud Strategy) термин «облачные вычисления» раскрывается как *IT-парадигма, обеспечивающая повсеместный доступ к общим пулам настраиваемых системных ресурсов и IT-услугам более высокого уровня, которые могут предоставляться с минимальными усилиями по управлению, обычно через Интернет*[1].

1 https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf

В **США** Национальным институтом по стандартам и технологиям (NIST) «облачные вычисления» определены как *модель предоставления сетевого доступа по запросу к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ, приложений и служб), которые можно быстро выделить и освободить с минимальными усилиями по управлению или взаимодействием с поставщиком облачных услуг.*

В **России** указанным выше законопроектом термин «облачные вычисления» определен как *«способ организации вычислений, выполняемых с применением технологий распределенной обработки данных».*

Следует обратить внимание, что российское определение «облачных вычислений» не указывает на тот факт, что данная технология минимизирует технические и управленческие усилия, связанные с предоставлением вычислительных ресурсов. Таким образом, не обозначены решаемые внедрением облачных вычислений проблемы, например: затрудненность получения доступа к данным, сложности при предоставлении услуг государственного сектора, обусловленные хранением данных в разных инфраструктурах и т.д. Такие проблемы существуют, если у разных органов власти есть собственные отдельные вычислительные инфраструктуры.

Следует отметить, что Законопроектом о Государственной единой облачной платформе (далее – ГЕОП) не предусмотрены базовые принципы работы ГосОблака, на основе которых развивалось бы дальнейшее специальное регулирование использования облачных вычислений для размещения и функционирования ГИС. Установление таких принципов необходимо для определения ключевых правил и ценностей, в соответствии с которыми будет развиваться указанное специальное регулирование.

В числе таких принципов может быть указан **принцип мультиоблачности (мультиклаудного облака)**, предполагающий учет целесообразности диверсификации поставщиков услуг облачных вычислений для нужд государства, в том числе с целью снижения издержек на их закупку, что позволяет создавать коммунальное облако (а не частные облака под каждую ГИС, которая переносится в облако) с возможностью при необходимости переходить из одного облака в другое, гарантируя обеспечение безопасности данных, эластичность, масштабируемость, совместимость.

### История создания проекта «ГосОблако»

**2013**

Проект ГосОблако в России начался еще в 2013 г., когда по заказу Минкомсвязи ЗАО «Крок инкорпорейтед» составило Концептуальную модель создания инженерной инфраструктуры в части обработки и хранения данных федеральных государственных органов РФ, в которой определялись в том числе базовые **принципы формирования состава облачной инфраструктуры** и подходы к **структуре и организации государственного облака**[1].

**2015**

7 октября 2015 г. Распоряжением правительства РФ № 1995-р была утверждена «Концепция перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных».

Планировался перевод государственных органов, государственных корпораций и открытых акционерных обществ с государственным участием в систему центров обработки данных, используемую для нужд органов государственной власти, до декабря 2021 г.[2], включая меры по осуществлению **контроля качества деятельности оператора** системы центров обработки данных, **аккредитации поставщиков** облачных услуг, установления требований в части **обеспечения безопасности данных** и пр.

1 https://filearchive.cnews.ru/doc/2012/06/pc.docx

2 http://static.government.ru/media/files/EOFotaHdQ8qcbm139O6mluwU302H4GDy.pdf

**NB!** В Концепции впервые была заложена идея отказа от **инвестиций в собственную государственную ИКТ-инфраструктуру** (проектирование и строительство ЦОД, закупку и монтаж оборудования) за счет перехода на **закупку облачных технологий**, для снижения нагрузки на бюджеты государственных органов до 10% в год с учетом объема потребляемых вычислительных ресурсов.

**2016**

В ноябре 2016 г. произошла первая попытка на уровне закона ввести **регулирование облачных вычислений**.

Минкомсвязью России опубликован законопроект по внесению изменений в Федеральные законы «Об информации, информационных технологиях и о защите информации», «Об организации предоставления государственных и муниципальных услуг» и «Об электронной подписи».

Законопроект предлагал закрепить **понятие облачных вычислений**, понятие **поставщика услуг** инфраструктуры, включая установление обязанностей поставщика, изменения в части использования единой цифровой инфраструктуры при оказании государственных и муниципальных услуг и пр. [1]

**2017**

В 2017 г. был утвержден План мероприятий по направлению «Информационная инфраструктура» программы «Цифровая экономика Российской Федерации», согласно которому ввод ГЕОП в эксплуатацию был намечен на конец 2019 г.

К 2024 г. доля государственных систем, перенесенных на платформу, должна составить **90%**.[2]

**2019**

Постановлением Правительства РФ от 28 августа 2019 г. № 1114 начат эксперимент по вводу в эксплуатацию ГЕОП[3]. В 2019 г. единственными исполнителями, ответственными за внедрение ГЕОП, были назначены ПАО «Ростелеком» и НИИ «Восход»[4] в рамках так называемой первой очереди ФГИС «Управление государственной единой облачной платформой»[5][6].

Согласно данному Постановлению, методологическое и техническое обеспечение эксперимента осуществляется Минцифры России совместно с НИИ «Восход».

Постановление заложило **цели по формированию и апробации условий для создания ГЕОП**, апробации функционала первой очереди данной системы, новых подходов к обеспечению органов власти автоматизированными рабочими местами и программным обеспечением с использованием ГЕОП, а также по формированию модели бесперебойного функционирования государственных информационных систем с использованием ГЕОП.

Распоряжением Правительства РФ от 28 августа 2019 г. № 1911-р утверждена действующая в настоящее время **Концепция создания ГЕОП** (далее – Концепция), которая содержит уже перечень конкретных шагов по развитию ГЕОП.

1 http://regulation.gov.ru/p/59054
2 http://static.government.ru/media/files/DAMotdOImu8U89bhM7IZ8Fs23msHtcim.pdf
3 http://publication.pravo.gov.ru/Document/View/0001201908300019?index=10&rangeSize=1
4 http://publication.pravo.gov.ru/Document/View/0001201911180029?index=0&rangeSize=1
5 http://publication.pravo.gov.ru/Document/View/0001201908300019?index=10&rangeSize=1
6 https://www.voskhod.ru/projects/scsmev/

В соответствии с Концепцией *«ГЕОП – это экосистема аккредитованных сервисов и поставщиков информационно-телекоммуникационной инфраструктуры, обеспечивающая информационно-технологическое взаимодействие информационных систем органов государственной власти, органов местного самоуправления и государственных внебюджетных фондов, размещаемых на указанной платформе, федеральной государственной информационной системы, обеспечивающей комплексный мониторинг функционирования инфраструктуры государственной единой облачной платформы и ее взаимодействия с иными подключенными к ней информационными системами, а также системы обеспечения информационной безопасности»*[1].

Концепцией предусмотрено определение **норм технического регулирования и требований к инфраструктуре ГЕОП**, ее составу, компонентам и архитектурно-техническим решениям, механизмам государственного регулирования услуг по использованию ГЕОП, стоимости такого использования.

Отмечается необходимость нормативного регулирования требований к элементам ГЕОП и порядку их использования; случаев перехода информационных систем на использование ГЕОП, случаев и порядка подключения инфраструктур к ГЕОП, требований к взаимодействию с такими ИТ-структурами. Планируется разработать требования к ИТ-сети органов власти, перечень услуг связи, оказываемых с использованием сетей связи, порядок формирования и ведения реестра поставщиков программных услуг и облачных вычислений, требования к уровню предоставления услуг ГЕОП, к инфраструктуре ЦОД ГЕОП, модели классификации ЦОД, требования к использованию услуг сертифицированных ЦОД и пр.

**2021**

В ноябре 2021 г. разработан проект федерального закона о внесении изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ID проекта 01/05/11-21/00122604).

Данным законопроектом определяется термин «ГосОблако», «облачные услуги» (см. выше), а также «облачные вычисления» и «пользователи облачных услуг», определены элементы ГосОблака, полномочия Правительства РФ и ответственных ФОИВ в отношении ГосОблака[2].

### Проект «ГосОблако»: текущее состояние

На данный момент, согласно пояснительной записке к проекту федерального закона о внесении изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ, подготовленному Минцифры России, уже разработаны и **прошли апробацию механизмы миграции государственных информационных систем в ГосОблако**, накоплен опыт по подготовке государственных информационных систем к миграции, развертыванию вычислительной инфраструктуры для ГосОблака[3].

В ноябре 2021 г. появились сообщения о том, что в Минцифры России трансформировали концепцию Государственной единой облачной платформы, приняв решение о создании новой инфраструктуры **«Гособлако 2»**. Данная инфраструктура предполагается к формированию параллельно с существующей ГЕОП и по принципу community cloud (облаков сообщества, коммунальных облаков).

ОЭСР определяет community cloud как *частные или публичные облачные платформы, совместно использующиеся определенным сообществом, которое имеет общие интересы (например, не-*

1 http://static.government.ru/media/files/3pP2jAu58rAlWXyCmVZAMzJiX0Liw5Dg.pdf

2 https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122604

3 https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122604

*большие организации или исследовательские институты), или предоставляемые реселлерами облачных услуг, которые объединяют услуги разных поставщиков облачных услуг и перепродают их*[1].

В набор базовых сервисов, которые предоставляются в рамках платформы «ГосОблако» (ГЕОП), входят сервисы, которые могут быть охарактеризованы как инфраструктурные (**IaaS**, например, инфраструктуры по обработке и хранению данных в соответствии с разделом II Концепции[2], услуги облачных вычислений в соответствии с Разделом III Концепции)[3].

В настоящее время ГосОблако содержит в себе **более 100 сервисов**.

**NB!** На данный момент проект ГЕОП будет формироваться за счет внедрения облаков сообщества **(коммунальных облаков)**. Отличие новой инфраструктуры состоит в том, что ранее под каждую ГИС создавалось отдельное частное облако.

В настоящее время планируется, что **ГосОблако станет одним из сервисов экосистемы ГосТех**[4]. В соответствии с подготовленной Сбербанком концепцией «технологической платформы государства ГосТех» (см. ниже) ГЕОП обеспечивает инфраструктуру для платформы ГосТех, а именно, управление вычислительной инфраструктурой в облаке, то есть, услуги Iaas[5].

Стоит отметить, что на данный момент SberCloud разрабатываются решения для обеспечения функционирования платформы ГосТех на базе технологической платформы Platform V наряду с ГЕОП. Минцифры планирует **расширение перечня поставщиков облачных услуг**, в том числе услуг PaaS, Saas для функционирования платформы ГосТех.

### Основные участники проекта «ГосОблако»

- **Закупка у Ростелекома**

В ноябре 2019 года Правительство (Распоряжением от 11 ноября 2019 г. № 2667-р) определило «Ростелеком» **единственным исполнителем закупок** товаров и услуг Минцифры в 2019–2020 гг., связанных с переводом в ГЕОП информационных систем Минтруда, Минюста, Ростехнадзора, Росимущества, ГФС России, Росархива и Фонда социального страхования, а также с арендой вычислительной инфраструктуры и организацией связи, которые необходимы для проведения эксперимента[6].

Таким образом, Ростелеком стал единственным поставщиком услуг в части перевода в ГЕОП информационных систем этих ведомств.

- **Закупка у ООО «Мэйл.Ру»**

В декабре 2019 г. НИИ «Восход» провел **закупку у единственного поставщика** (ООО «Мэйл.Ру») на предоставление услуг по проектированию и разработке информационных технологий для сетей и систем (создание первой очереди ФГИС «Управление ГЕОП»).

Договор на сумму 238,5 млн рублей действовал до конца 2020 г., фиксированные выплаты совершались поэтапно. Согласно техническому заданию, работы включали в себя поставку оборудова-

1 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2011)19/FINAL&docLanguage=En

2 http://static.government.ru/media/files/3pP2jAu58rAIWXyCmVZAMzJiX0Liw5Dg.pdf

3 http://static.government.ru/media/files/3pP2jAu58rAIWXyCmVZAMzJiX0Liw5Dg.pdf

4 https://www.interfax.ru/russia/803966

5 https://www.tadviser.ru/images/7/72/%D0%A1%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA_-

6 http://publication.pravo.gov.ru/Document/View/0001201911180029?index=0&rangeSize=1

ния, технических средств и специального программного обеспечения, актуализацию проектных решений, разработку рабочей документации системы «Управление ГЕОП», адаптацию специального программного обеспечения, сопровождение и поддержку опытной эксплуатации очереди системы[1].

- **Закупка у ООО «Центр хранения данных»**

В декабре 2020 г. Минцифры России заключило договор по закупке на сумму 2,98 млрд руб. с поставщиком ООО «Центр хранения данных» (дочерней компанией Ростелекома). Закупка проводилась в форме **электронного аукциона**, вторым участником было ЗАО «КРОК Инкорпорейтед»[2].

Предметом закупки являлось **оказание услуг по предоставлению вычислительных ресурсов** для государственной единой облачной платформы в целях размещения и обеспечения функционирования информационных ресурсов и систем федеральных органов исполнительной власти РФ. В соответствии с техническим заданием, в рамках закупки предоставляются такие услуги вычислительных ресурсов и ресурсов хранения данных для информационных систем, пространства для хранения резервных копий, машин баз данных, каналов связи, публичных IPv4-адресов, а также услуги по обеспечению информационно-технологической инфраструктуры[3].

ООО «Центр хранения данных» в рамках данной закупки установило ценовое предложение в 1,17 млн рублей, цена контракта составила почти 2,98 млрд рублей. Услуги предоставляются в 2 этапа, по 1 году каждый, цена контракта определяется по окончании этапа как сумма стоимостей всех заказов (количественных требований к предоставлению услуг и их характеристик), которые должны быть исполнены в течение срока этапа[4].

При этом заказ на предоставление услуг формируется на каждый отдельный орган власти, использующий услуги, ресурсы и сервисы инфраструктуры (в соответствии с Постановлением Правительства от 28 августа 2019 г. № 1114. Таким образом, в закупке **определен верхний порог** суммы закупки, **конечная сумма определяется по окончании этапа** (года). Цены на услуги определены заранее в контракте[5].

Таким образом, в настоящее время в России разработка, обслуживание ГосОблака и работы по миграции ведомственных ГИС осуществляются Ростелекомом и его дочерней организацией.

При этом рассматривается возможность **вовлечения множества поставщиков услуг IaaS** с возможностью для государственных органов выбрать поставщика, который лучше всего подходит для необходимой государственному органу услуг.

**NB!** Практика зарубежных стран (США, Великобритания, Германия и пр.) показывает эффективность закупки услуг по такому принципу. Согласно опросу MeriTalk, сегодня **81%** федеральных агентств США используют более одного поставщика облачных услуг.

Например, с учетом того, какие данные планируются к хранению или использованию (в зависимости от уровня чувствительности данных могут применяться разные стандарты безопасности), какая архитектура облачного решения больше всего подходит, будет ли использоваться инфраструктура частного или публичного облака и пр. Иными словами, **планируется внедрение принципа мультиоблачности (multicloud, мультиклаудного облака)**.

Следует отметить, что применение концепции multicloud позволит Минцифры России оптимизировать затраты за счет диверсификации **поставщиков с наиболее выгодными ценами** за отдельные типы услуг. Например, в закупке с ООО «Центр хранения данных» цена 1 ГБ дискового

1 https://zakupki.gov.ru/223/purchase/public/download/download.html?id=58192680
2 https://zakupki.gov.ru/epz/order/notice/ea44/view/documents.html?regNumber=0173100007520000033
3 https://zakupki.gov.ru/44fz/filestore/public/1.0/download/priz/file.html?uid=B4D3F90FCFA61DC1E0530F548D0AF432
4 https://zakupki.gov.ru/44fz/filestore/public/1.0/download/rpec/file.html?uid=B6F8476A65AC97C5E0530F548D0A4B5F
5 https://zakupki.gov.ru/44fz/filestore/public/1.0/download/rpec/file.html?uid=B6F8476A65AC97C5E0530F548D0A4B5F

пространства SSD установлена в размере 0,49 руб. за день использования. Согласно Калькулятору услуг компании Яндекс, аналогичная услуга стоила бы около 0,25 руб. за день использования[1].

Стоит отметить, что сегодня в России на рынке облачных технологий действует множество компаний, которые поставляют различные услуги:

Yandex Cloud

ООО«Яндекс.Облако» предоставляет сервис Yandex Cloud, в рамках которого поставляются услуги IaaS[2], PaaS, SaaS[3].

BeeCLOUD

ПАО «Вымпелком» в рамках инфраструктуры BeeCloud предоставляет услуги IaaS, PaaS для разработки сайтов, сервисов и приложений[4], а также SaaS .

CROC CLOUD SERVICES

Компания КРОК предоставляет услуги IaaS (Публичное облако КРОК[5]), PaaS (Платформа SAP HANA), SaaS (корпоративный файлообменник, почта, управление логистикой и др. [6]).

SBER CLOUD

ООО «Облачные технологии» (SberCloud) предоставляет услуги IaaS (виртуальные машины, ЦОД и др.) и PaaS (например, Cloud Performance Test Service[7]).

Selectel

ООО «Селектел» предоставляет услуги IaaS (например, облачную инфраструктуру 1С[8]), PaaS (например, платформа Managed Kubernetes[9]), SaaS (например, продукты МойОфис по модели SaaS https://selectel.ru/about/newsroom/news/selectel-predostavit-produkty-moiofis-po-modeli-saas/).

#CloudMTS

ПАО «МТС» предоставляет услуги IaaS (например, Azure Stack[10]), PaaS (хостинг 1С), SaaS (например, Naumen Contact Center).

VK Cloud Solutions

VK Cloud Solutions предоставляет услуги IaaS (облачные серверы, хранилища, базы данных и др.[11]) и PaaS (например, платформа Managed Kubernetes [12]).

1 https://cloud.yandex.ru/prices#calculator

2 https://beecloud.beeline.ru/iaas/

3 https://beecloud.beeline.ru/saas/

4 https://moskva.beeline.ru/business/products-and-solutions/developers-section/beecloud-for-developers/

5 https://cloud.croc.ru/services/iaas/

6 https://cloud.croc.ru/services/saas/

7 https://sbercloud.ru/ru/advanced

8 https://selectel.ru/services/1c-leasing/1c-cloud/

9 https://kb.selectel.ru/docs/selectel-cloud-platform/kubernetes/

10 https://cloud.mts.ru/services/microsoft-azure-iaas/

11 https://mcs.mail.ru/easy-k8s/?utm_source=google.ads.DB&utm_medium=cpc&utm_campaign=g_umnaya_k8s_docker_rf_%7Bcampaign_id%7D&utm_content=%7Bad_id%7D&utm_term=%7Bkeyword%7D&gclid=Cj0KCQiArt6PBhCoARIsAMF5wajyV9NEER2GOIiZZgPVyc0GVOPmX9B8DpEuxDJM6xcaQb0ifnWr2MYaAlsaEALw_wcB

12 https://mcs.mail.ru/easy-k8s/?utm_source=google.ads.DB&utm_medium=cpc&utm_campaign=g_umnaya_k8s_docker_rf_%7Bcampaign_id%7D&utm_content=%7Bad_id%7D&utm_term=%7Bkeyword%7D&gclid=Cj0KCQiArt6PBhCoARIsAMF5wajyV9NEER2GOIiZZgPVyc0GVOPmX9B8DpEuxDJM6xcaQb0ifnWr2MYaAlsaEALw_wcB

# Проект «ГосТех»

## Что такое «ГосТех»?

В соответствии с п.2 Постановления Правительства РФ от 12 октября 2020 г. № 1674, платформа «ГосТех» представляет собой экосистему создания, развития и эксплуатации государственных информационных систем, включающую в себя единую программно-аппаратную среду и методологию, поддерживающую взаимоотношения граждан, государственных органов и коммерческих организаций на базе современных информационных технологий с целью повышения доступности государственных услуг и функций, а также направленную на снижение расходов участников на использование государственных услуг.

Таким образом, «**ГосТех» состоит из двух компонентов**:

1. платформа разработки, на которой создается, развивается и эксплуатируется прикладное программное обеспечение государственных информационных систем и их компонентов;

2. методология функционирования экосистемы.

## История создания проекта «ГосТех»

**апрель 2021**

В апреле 2020 г. Сбербанком была разработана концепция «технологической платформы государства ГосТех». В соответствии с данной Концепцией инфраструктура для работы с платформой (**IaaS**) должна обеспечиваться ГЕОП и SberCloud: компонент IaaS в данной Концепции включает в себя **инфраструктуру ГЕОП** и «**фабрику данных**» (сервисы по хранению и аналитике данных).

Сервисы **PaaS** (например, единый профиль клиента, аудит, журналирование и т.д.), согласно данной концепции, должны предоставляться Сбербанком. Сервисы **SaaS** предоставляются участниками (разработчиками), в качестве единого технологического заказчика определен Главный Научно-Исследовательский Вычислительный Центр ФНС России[1].

**октябрь 2021**

Постановлением Правительства РФ от 12 октября 2020 г. № 1674 **запущен эксперимент по созданию**, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех»[2].

**ноябрь 2021**

Уже в ноябре 2020 г. Минцифры России объявило о закупке в форме **электронного аукциона** на 900 млн руб. в целях проведения эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех».

Единственная заявка была подана ПАО «Сбербанк». Техническим заданием предусмотрено 14 этапов оказания услуг до 31 мая 2022 г.

В рамках контракта Сбербанк предоставляет следующие виды услуг: по передаче неисключительных прав на программное обеспечение, входящее в состав Платформы; по организации функционирования программного обеспечения DEV-, TEST-стендов

1 https://www.tadviser.ru/images/7/72/%D0%A1%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA_-_%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D1%8B_%D0%93%D0%BE%D1%81%D0%A2%D0%B5%D1%85.pdf

2 http://publication.pravo.gov.ru/Document/View/0001202010150045

Платформы; по установке среды виртуализациии Платформы; по обеспечению работы программного обеспечения Платформы на PROD-, ПСИ-, НТ-стендах для трех Ведомств и пр.[1]

Цена контракта является твердой, при этом в части предоставления услуг по обеспечению функционирования, администрирования и бесперебойной работы программного обеспечения ГосТеха на DEV-, TEST-стендах и по обеспечению функционирования, администрирования и бесперебойной работы программного обеспечения ГосТеха оплачиваются по стоимости фактически оказанных услуг, прочие – **в фиксированной сумме**. Стоимость фактически оказанных услуг рассчитывается **за единицу времени** (1 рабочий день или 1 час).

## Проект «ГосТех»: текущее состояние

На данный момент сопровождением процессов создания, перевода, развития и эксплуатации ГИС и их компонентов на базе платформы «ГосТех»[2], а также ее развитием и эксплуатацией занимается ФКУ «ГосТех»[3]. При этом ООО «Облачные технологии» (бренд SberCloud) предоставляет платформу разработки и обеспечивает технологическое функционирование и развитие платформы разработки.

В соответствии с общим описанием, **платформа ГосТех состоит из следующих основных сегментов[4]**:

- **облачная инфраструктура** Платформы, включая среду виртуализации – «Облачная платформа Сбербанка» по модели обслуживания IaaS;
- **инструменты управления контейнерами** – свободно распространяемое программное обеспечение (Open Source Software), отвечающее за автоматизацию и управление жизненным циклом контейнеров и сервисов, включая планирование ресурсов, управление масштабируемостью, правила балансировки нагрузки и контроль доступности, а также организация виртуальных сетей;
- **инструменты управления производственным процессом** – инструменты «SberWorks», обеспечивающие организацию единой среды разработки для инженеров и разработчиков;
- **компоненты управления данными** – компоненты работы с данными для решения таких задач как: работа со структурированными и слабоструктурированными данными, хранение данных в оперативной памяти, сбор данных из разных источников и др.;
- **компоненты аналитики данных** – платформенные компоненты, предназначенные для обработки больших массивов структурированных и неструктурированных данных;
- **компоненты интеграции** – платформенные компоненты, обеспечивающие реализацию интеграционной логики приложений в сервис-ориентированной архитектуре (SOA);

1 https://zakupki.gov.ru/44fz/filestore/public/1.0/download/priz/file.html?uid=B49EC2A66ECB26A6E0530F548D0A7668

2 https://digitalcc.ru/

3 https://platform.digital.gov.ru/docs/files/%D0%9E%D0%B1%D1%89%D0%B5%D0%B5%20%D0%BE%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%9F%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D1%8B.pdf

4 https://platform.digital.gov.ru/docs/files/%D0%9E%D0%B1%D1%89%D0%B5%D0%B5%20%D0%BE%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%9F%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D1%8B.pdf

- **инструменты и компоненты безопасности** – инструмент, функциональные компоненты которого обеспечивают идентификацию, аутентификацию, авторизацию пользователей;

- **интерфейсные компоненты** – набор инструментов, реализующих функциональность пользовательского взаимодействия с системой, моделирования бизнес-процессов, интеграциями с сервисами регистрации/авторизации пользователей через системы ЕСИА, СМЭВ, ОТТ.

В структуру платформы ГосТех входит «**производственный конвейер**», позволяющий пользователям создавать из существующих компонентов на технологических платформах готовые приложения, сложные ГИС и настраиваемые компоненты (например, автоматизированные рабочие места).

**NB!** Планируется, что компоненты IaaS будут поставляться разными поставщиками наряду со SberCloud (Ростелеком, Яндекс и др.) в рамках ГЕОП.

Платформа ГосТех также включает в себя сегменты, предполагающие предоставление **услуг по модели PaaS** (например, инструменты управления производственным процессом, обеспечивающие организацию единой среды разработки для инженеров и разработчиков) и **SaaS** (например, сервисы защиты от утечек данных).

Что касается требований к провайдерам сервисов PaaS, для них установлен **Минимальный набор требований, которым должно соответствовать платформенное программное обеспечение**, а именно:

- поддержка ключевых технологий: управление контейнерами, объектное хранилище, реляционная база данных, база данных NoSQL, обработка больших данных.

- наличие открытых систем оркестрации контейнеров для развертывания компонента приложений и микро-сервисов;

- предоставление сервисов Ansible (системы управления конфигурациями) и Terraform providers со слоем управления инфраструктурными сервисами для их развертывания и конфигурирования, а также управления по REST API;

- обеспечение развертывания в различных конфигурациях резервирования, шардирования и резервного копирования, поддержанные в управляемых системах управления базами данных (СУБД);

- предоставление скриптов развертывания PaaS сервисов в Единый репозиторий;

- поддержка ПО со стороны производителя на территории РФ;

- обеспечение технической возможности предоставления и сопровождения сервиса в соответствии с заключенным договором на протяжении минимум трех лет;

- обеспечение возможности установки расширений поддерживаемых СУБД (например, установка расширения PostGIS в Postgres).

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС, в том числе ГосТех, определены Постановлением Правительства РФ от 6 июля 2015 г. № 676. Данное Постановление не является уникальным для облачных сервисов – вместе с тем, Минцифры России планирует в 2022 г. внесение изменений в данное Постановление в части установления **порядка доступа и включения продуктов и сервисов в ГосТех**, а также разработки нового порядка создания ГИС для запуска итеративного жизненного цикла создания ГИС и ускорения запуска новых сервисов[1].

1 https://www.youtube.com/watch?v=bitzhLqnjts&ab_channel=%D0%93%D0%BE%D1%81%D0%A2%D0%B5%D1%85

Кроме того, ФКУ «ГосТех» разработан **Стандарт по управлению динамической инфраструктурой платформы ГосТех**, который описывает требования к модулям проводников Terraform (инструмента для управления инфраструктурой через машиночитаемые файлы, разработанного компанией HashiCorp). Этот стандарт позволяет установить единые требования для провайдеров IaaS ГосТех, что, в свою очередь, позволит таким провайдерам участвовать в размещении ГИС на мощностях, находящихся под их управлением.

В марте 2022 г. Минцифры России опубликовало первую версию **Методических рекомендаций по включению сервисов в единую цифровую платформу «ГосТех».** Устанавливаются требования к программному обеспечению, предоставляемому поставщиками, для включения их в состав платформы ГосТех с целью развития ее функциональности в соответствии с потребностями клиентов – получателей государственных услуг, государственных функций и пр.[1]

Методическими рекомендациями установлен ряд требований: к поставщику (например, соответствие требованиям в части средств защиты конфиденциальной информации), к поставке (дистрибутиву, скриптам развертывания, документации, манифесту сервиса), к сервисам (к надежности, доступности, диагностируемости, управлению пользователями, API), к юридическому оформлению (передача права использования по лицензионному договору, приоритет применения российского ПО). Также установлены дополнительные требования к сервисам, созданным в рамках госконтрактов, к публикуемым сервисам SaaS и пр.).

**Методическими рекомендациями охватываются следующие виды сервисов**:

- **сервисы ГК**, являющиеся частью или модулем какой-либо информационной системы, разрабатываемой в рамках государственного контракта, которые можно переиспользовать при создании новых ГИС. Сервисы данного типа поставляются в виде исходного кода с использованием Национального фонда алгоритмов и программ;

- **сервисы поставщиков**, поставляемые в виде дистрибутивов без передачи исключительных прав (например, Postgres Pro, Tarantool, AntiDDOS и т.д.). Сервисы размещаются у облачного провайдера «ГосТех» и предоставляются пользователю в виде заказа сервиса из каталога сервисов ЕЦП «ГосТех» через портал самообслуживания;

- **публикуемые SaaS – сервисы**, которые поставщик предоставляет конечным пользователям в виде готовых облачных SaaS-решений через простые web-интерфейсы, при этом поставщик обеспечивает работоспособность сервиса (например, «Дневник.ру», «Мой Спорт» и т.д.).

В целом, документ содержит формальные и технические требования, как универсальные для всех Сервисов, так и специальные для сервисов ГК и SaaS. В частности, что готовые облачные сервисы должны обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. При разработке сервисов рекомендуется руководствоваться Методическими рекомендациями по совершенствованию пользовательских интерфейсов и Методическими рекомендациями по информированию граждан о преимуществах получения государственных и муниципальных услуг в электронной форме.

Сервис должен предоставлять государственным органам возможность бесплатного предварительного ознакомления с функциональностью сервиса в объеме достаточном для осуществления обоснованного выбора сервиса и его закупки, а также позволять осуществлять идентификацию и аутентификацию конечных пользователей через ЕСИА.

1 https://d-russia.ru/wp-content/uploads/2022/03/proekt_metodicheskie_rekomendatsii_po_vklyucheniyu_servisov_na_platformu_gostekh.pdf

## Основные участники проекта «ГосТех»

Поставщиком услуг по организации функционирования и обслуживанию платформы ГосТех является **ПАО «Сбербанк**[1]. Сопровождением процессов создания, перевода, развития и эксплуатации ГИС и их компонентов на базе платформы «ГосТех», а также ее развитием и эксплуатацией занимается **ФКУ «ГосТех»**[2].

Наряду с ООО «Облачные технологии» в предоставлении утвержденных сервисов PaaS будут участвовать и другие провайдеры (**Яндекс, Ростелеком и др.**). Таким образом, в настоящее время в рамках проекта ГосТех планируется реализовать **принцип мультиоблачности (мультиклауда)**, при котором сервисы как разных «слоев», так и в рамках одного слоя (PaaS) будут предоставляться разными поставщиками.

Так, например, компания Яндекс может обеспечить предоставление и функционирование компонентов управления данными, таких, как Yandex Database, вместо действующего на ГосТех компонента «СУБД Platform V Pangolin»[3], сервис Yandex Identity and Access Management[4] может заменить действующий компонент «Авторизация ЕФС Platform V».

## «ГосОблако» и «ГосТех»: в чем разница?

На данный момент проект **«ГосОблако»** представляет собой платформу, на которой по модели **IaaS** предоставляются инфраструктурные сервисы для ГИС органов власти, МСУ, государственных внебюджетных фондов, а также для платформы «ГосТех».

**Платформа «ГосТех»** представляет собой систему, на которой предоставляются сервисы по моделям PaaS и SaaS для создания среды для разработки новых сервисов, использующих данные государственного сектора, и для работы с физическими и юридическими лицами. Соотношение проектов «ГЕОП» и «ГосОблако» представлено на рис. 2.

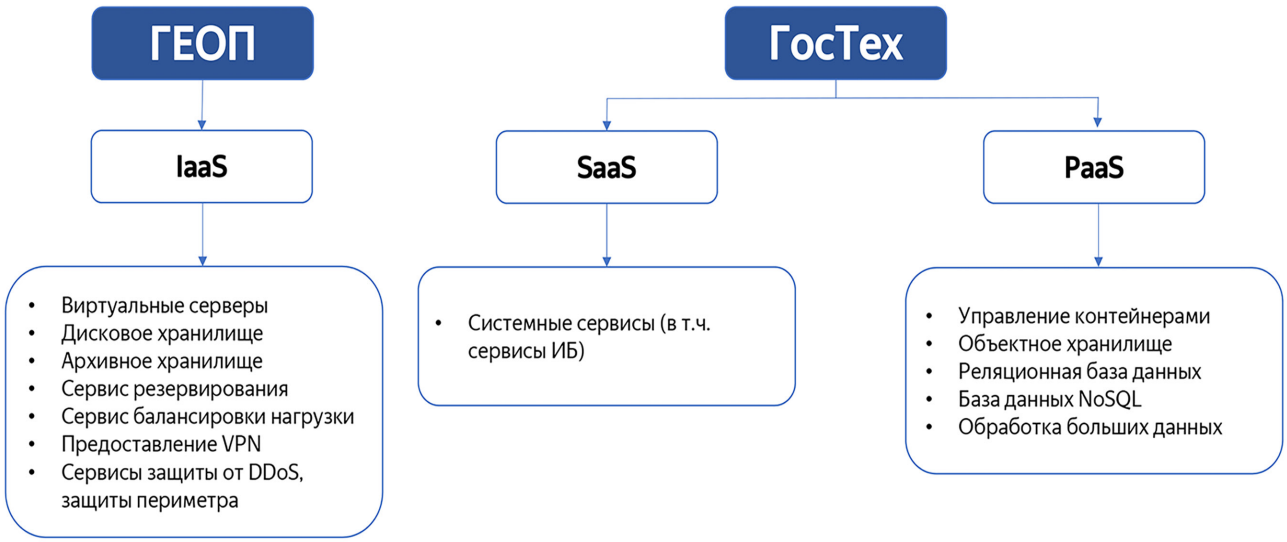



**Рис. 2. Структура сервисов «ГЕОП» и «ГосТех»**

1 https://zakupki.gov.ru/epz/order/notice/ea44/view/supplier-results.html?regNumber=0173100007520000032

2 https://digitalcc.ru/

3 https://cloud.yandex.ru/services/ydb

4 https://cloud.yandex.ru/services/iam

# II. Прохождение аттестации на соответствие требованиям по защите информации облачных платформ

В соответствии с Приказом **ФСТЭК от 11 февраля 2013 г.** № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», субъектами положений приказа являются:

- **обладатель информации** (заказчик, заключивший контракт на создание государственной информационной системы).

На практике заказчиком выступает государственный орган, владелец информационной системы. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (п. 3 ст. 2), информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (далее – ГИС).

- **оператор информационной системы** – лицо, организующее и осуществляющее обработку данных, составляющих информацию в информационной системе.

В соответствии с ФЗ-149 «Об информации» (п. 12 ст. 2), оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. На практике, оператором может выступать также и сам государственный орган – тогда происходит совпадение субъектов для целей Приказа ФСТЭК.

- **уполномоченное лицо** – лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора.

Таким образом, облачный провайдер в терминологии ФСТЭК пользуется статусом «уполномоченного лица». В соответствии с п. 4 раздела I Приказа ФСТЭК № 17 именно облачный провайдер (уполномоченное лицо) обеспечивает защиту информации, что указывается в договоре.

В соответствии с п. 17.6 Приказа ФСТЭК от 11 февраля 2013 г. № 17, если информационная система создается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных (далее – ЦОД) уполномоченного лица, такая инфраструктура должна быть аттестована на соответствие требованиям Приказа. Таким образом, Приказ ФСТЭК направлен на вопросы обеспечения безопасности ГИС, при этом если для создания и работы ГИС используются центры обработки данных (инфраструктура облачных провайдеров), то такие ЦОД также подлежат аттестации в соответствии с требованиями Приказа ФСТЭК от 11 февраля 2013 г. № 17.

Таким образом, **облачные провайдеры (владельцы ЦОД) должны проводить аттестацию своих центров обработки данных** при предоставлении вычислительных ресурсов (мощностей) для обработки информации для ГИС на соответствие требованиям безопасности ФСТЭК в порядке, установленном Приказом № 17.

Однако положения Приказа изначально разрабатывались для автономных технологических систем. Поэтому установленный порядок не учитывает особенностей предоставления облачных услуг различного типа, в том числе с использованием подхода мультиоблачности (мультиклаудного облака), для которого, в частности, важна интероперабельность серверов и форматов данных в сочетании с безопасностью оборота данных для беспроблемной переносимости данных. В связи с этим облачные провайдеры несут существенные временные и организационные издержки, обусловленные отсутствием практики ФСТЭК в оценке необходимых требований безопасности.

### Процесс прохождения аттестации ФСТЭК

Аттестация информационной системы проводится по требованиям защиты информации (абз. 4 п. 13 Приказа ФСТЭК № 17)[1] через комплекс аттестационных испытаний. По итогам испытаний **подтверждается соответствие системы защиты информации информационной системы** требованиям законодательства в области информации и информационных технологий (п. 17).

Для проведения аттестации информационной системы применяются национальные стандарты (например, ГОСТ Р ИСО/МЭК 27000-2021. «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»), а также методические документы, разработанные и утвержденные ФСТЭК России (п. 17.2), например, Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных[2].

При проведении испытаний применяются такие **методы**, как:

- **экспертно-документальный метод** (проверка соответствия на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы);
- **анализ уязвимостей** информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;
- испытания системы защиты информации путем осуществления **попыток несанкционированного доступа** (воздействия) к информационной системе в обход ее системы защиты информации.

Испытания могут проводиться в отношении только части информационной системы – сегментов, реализующих весь процесс обработки информации (п. 17.3 Приказа № 17): *«при испытании части информационной системы аттестация распространяется на остальные сегменты системы при условии их соответствия аттестованным сегментам»*. Поэтому облачный провайдер может аттестовать серверы самостоятельно независимо от аттестации иных видов ИКТ-инфраструктуры, на которую заказчик (владелец ГИС) планирует размещать саму ГИС.

Соответствие подтверждается в процессе приемочных испытаний. По результатам испытаний оформляются (п. 17.2):

1 https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17

2 https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

- **протоколы** аттестационных испытаний;
- **заключение о соответствии** информационной системы требованиям о защите информации;
- **аттестат соответствия** в случае положительных результатов аттестационных испытаний.

Аттестат соответствия выдается на весь срок эксплуатации информационной системы (п. 17.4). Оператор (обладатель информации) в ходе эксплуатации информационной системы должен обеспечивать поддержку соответствия системы защиты информации аттестату соответствия.

Ввод в действие информационной системы осуществляется в соответствии с законодательством об информации, информационных технологиях и о защите информации, и с учетом ГОСТ 34.601[1] и при наличии аттестата соответствия (п. 17.5 Приказа № 17).

Для государственных информационных систем с **использованием персональных данных** необходимо регулировать выявленные актуальные угрозы организационными и техническими мерами, установленными Приказом ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[2].

Приказ предусматривает **меры в 15 категориях**:

1. идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
2. управление доступом субъектов доступа к объектам доступа (УПД)
3. ограничение программной среды (ОПС)
4. защита машинных носителей персональных данных (ЗНИ)
5. регистрация событий безопасности (РСБ)
6. антивирусная защита (АВЗ)
7. обнаружение вторжений (СОВ)
8. контроль (анализ) защищенности персональных данных (АНЗ)
9. обеспечение целостности информационной системы и персональных данных (ОЦЛ)
10. обеспечение доступности персональных данных (ОДТ)
11. защита среды виртуализации (ЗСВ)
12. защита технических средств (ЗТС)
13. защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
14. выявление инцидентов и реагирование на них (ИНЦ)
15. управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)

1 ГОСТ 34.601-90 «Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» https://docs.cntd.ru/document/1200006921

2 https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21

Меры, принимаемые по защите информации, определяются в соответствии **с классом защищенности** и **уровнем защищенности персональных данных**, как определено Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[1].

Положения Приказа № 21 адресованы конкретно операторам персональных данных (в соответствии с ч. 4 ст. 19 ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). В постановлении Правительства определяются **три типа актуальных угроз** для информационной системы, где ключевым фактором является наличие недокументированных возможностей информационной системы. Сертификация ФСТЭК должна подтвердить **отсутствие недокументированных возможностей**.

В отношении персональных данных конкретные актуальные угрозы определяет именно оператор персональных данных. И, соответственно, оператор персональных данных, исходя из уровня защищенности данных и конкретных актуальных угроз, определяет необходимые меры и средства защиты от них. Чаще всего информационные системы с персональными данными имеют 1 и 2 уровень защищенности. **Облачный провайдер аттестует свои серверы для размещения в них данных конкретных уровней защищенности**[2].

Согласно абз. 2 п. 2 Приказа ФСТЭК № 21, *«для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации».* Облачные провайдеры могут получить такую лицензию в соответствии с положениями Постановления Правительства РФ № 313 от 16 апреля 2012 г.[3]

**NB!** Например, лицензию на деятельность по технической защите конфиденциальной информации получил владелец **ЦОД Oxygen.**

Такая лицензия позволяет компании контролировать защиту информации **высокого уровня значимости** (УЗ1) в информационных системах **первого класса защищенности** (К1) от несанкционированного доступа.

Что касается системы защиты персональных данных, в ФЗ-152 нет препятствий для хранения и обработки данных в облачных системах. Согласно требованию локализации персональных данных, действующему с 2015 г. в России, операторы персональных данных должны использовать центры обработки данных, серверы которых физически находятся на территории России. Это значит, что операторы данных смогут пользоваться облачными сервисами при условии, что центр обработки данных облачного провайдера находится в России.

**NB!** В отношении обеспечения безопасности данных следует учитывать **разграничение ответственности** между оператором персональных данных и провайдером облачных систем: **облачный провайдер** обеспечивает облачную инфраструктуру и несет ответственность только за обеспечение **инфраструктуры соответствующего класса безопасности** на основании соглашения о предоставлении облачных услуг для данных определенного уровня защищенности (уровень защищенности данных определяется владельцем информации).

Например, при предоставлении облачных услуг IaaS облачный провайдер не имеет доступа к размещаемым в облаке данным, что может быть дополнительно зафиксировано в соглашении об ока-

1 http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/

2 https://www.croc.ru/news_posts/chto_oblachnye_provajdery_ne_dogovarivayut_o_personalnyh_dannyh/

3 http://www.consultant.ru/document/cons_doc_LAW_128739/

зании облачных услуг[1]. Облачный провайдер выполняет обязательства по безопасности облака в соответствии с соглашением с оператором данных, но в отношении информационных систем облачный провайдер не принимает решений.

Облачный провайдер может создавать технические инструменты безопасности для информационных систем в облаке, решения об использовании которых принимает оператор данных. Это значит, что **облачный провайдер не несет ответственности за риски для безопасности данных, связанные с обработкой данных**. Обработка данных (включая хранение, изменение, управление и т.п.) полностью находится в зоне ответственности оператора данных согласно положениям ФЗ-152.

Для предоставления облачных услуг по хранению и обработке персональных данных в облаке облачный провайдер должен иметь *аттестат соответствия требованиям безопасности информации, предъявляемым к информационным системам персональных данных (ИСПДн) при обеспечении соответствующего уровня защищенности персональных данных.*

**4 уровня защищенности и 3 типа угроз** безопасности персональных данных установлены Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[2]:

- **4-й уровень** обеспечивает защиту общедоступных и иных сведений с 3-м типом угроз (угрозы, связанные с неоформленными функциональными возможностями ПО без рисков доступа к данным третьих лиц)[3].

- **3-й уровень** защищает не только общедоступную информацию, но и специальные и биометрические данные, работает при 2-м и 3-м уровне угроз (угрозы 2-го типа связанны с неоформленными функциональными возможностями ПО в прикладных программах).

- **2-й уровень** защищает данные любого типа. Для некоторой информации допускает 1-й тип угроз (угрозы 1-го типа представляют собой комплексы факторов, связанных с недокументированными функциональными возможностями, на системном и прикладном уровне, которые могут привести к блокировке, изменению, удалению, к несанкционированному открытию доступа к данным).

- **1-й уровень** защищает данные специального и биометрического типа.

Таким образом, облачный провайдер должен иметь **аттестат соответствия** тому уровню защищенности, который зависит от того, какой тип данных будет храниться и обрабатываться в облаке[4].

### Проблемы прохождения аттестации ФСТЭК

В соответствии с Приказом № 17 следует, что требования (пп. 14–16) к безопасности ГИС устанавливает заказчик (государство). При этом, если поставщик облачных технологий хочет участвовать в проекте по созданию ГИС, он должен проходить аттестацию ФСТЭК по Приказу № 17 для ГИС. На практике ГИС переносится в существующую облачную систему, объекты которой уже должны быть аттестованы по требованиям Приказа № 17 ФСТЭК.

Аттестация ФСТЭК на основании положений Приказа №17 проходит с использованием **средств защиты информации, которые уже получили сертификацию ФСТЭК** (по Приказу ФСТЭК России от 03.04.2018 N 55 «Об утверждении Положения о системе сертификации средств защиты

1 https://www.it-lite.ru/blog/it-autsorsing/oblachnye-kontrakty-i-soglasheniya-ob-urovne-uslug/

2 http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/

3 https://data-sec.ru/personal-data/threats-types/

4 https://nubes.ru/blog-item/personal-data

информации»). Но проблема в том, что в отличие от процесса аттестации ЦОД, который проходит по большей части понятным и конкретным требованиям, процесс сертификации платформы для государственного облака сопряжен с проблемой недостатка практики и неопределенности требований безопасности для обслуживания государственных мультиоблачных систем (мультиклаудных облаков).

В частности, **подвержены изменениям требования к операционным системам**, которые, например, должны в обязательном порядке соответствовать минимальным системным требованиям операционной системы Astra Linux. Такая операционная система включена в Единый реестр российских программ Минкомсвязи России. Особенность системы заключается в обеспечении высокого уровня защиты обрабатываемой информации, поэтому такая система сертифицирована для информационных систем Минобороны, ФСТЭК, ФСБ[1].

Таким образом, для обслуживания государственных мультиоблачных систем процесс подтверждения соответствия облачной инфраструктуры требованиям ФСТЭК осложняется совмещением процесса сертификации и процесса разработки регулирующим органом требований для облачных провайдеров таких облачных сервисов. Это обуславливается тем, что сертификация средств защиты облачной платформы по типу «community cloud» проводится впервые.

Такая организационная проблема может приводить к ситуации, когда владелец информационной системы регулярно отдает предпочтение тому поставщику облачных услуг, с которым в первый раз было заключено соглашение об оказании облачных услуг, поскольку к повторным закупкам облачных сервисов иные поставщики либо не успевают пройти все процедуры аттестации, либо предпочитают экономить административные ресурсы и не участвовать в закупках на оказание облачных услуг.

Поэтому процедуры подтверждения соответствия облачной инфраструктуры требованиям ФСТЭК (сертификацию и аттестацию) нужно оптимизировать (**упрощать и ускорять**), обращаясь к существующим практикам и стандартам.

Проблема соблюдения требований безопасности для облаков и мультиоблачных систем на ЦОД может быть решена путем **упрощения процедур сертификации и аттестации** за счет зачета сертификации средств защиты и аттестации центров обработки данных **по международным стандартам**.

Следовательно, до того, как будут выработаны ясные требования ФСТЭК для сертификации мультиоблачных платформ, облачным провайдерам может быть обеспечена возможность подтверждать качество и безопасность своей облачной инфраструктуры на основе полученных сертификатов по международным стандартам.

В зарубежных странах регулирующие органы включают в нормативные акты ссылки на рекомендованные стандарты. Поставщики самостоятельно проходят сертификацию.

В **Италии** Агентство по цифровизации (AgID) согласно циркуляру по квалификации поставщиков IaaS, PaaS квалифицирует облачные сервисы на основании соответствия требованиям международных отраслевых стандартов (например, UNI, ISO/IEC и т. д.), а также в некоторых случаях применяются конкретные сертификаты (например, ISO/IEC 27001)[2].

Эталонными стандартами для этого набора требований являются стандарты, принадлежащие к семейству **ISO/IEC 20000**, в частности, стандарты ISO/IEC 20000-1 и ISO/IEC TR 20000 – для управления и обслуживания IT-сервисов.

1 http://bourabai.ru/os/AstraLinux.htm

2 https://cloud-italia.readthedocs.io/projects/cloud-italia-circolari/it/latest/

Для обеспечения **безопасности, конфиденциальности и защиты данных поставщики SaaS** сертифицируются по стандарту ISO / IEC 27001 «Системы обеспечения информационной безопасности», дополненным элементами управления стандартами ISO / IEC 27017 «Свод правил по управлению информационной безопасностью» (включающий стандарты аудита информационных систем и облачных служб) и ISO / IEC 27018 «Свод правил по защите персональных данных в облаке».

Для обеспечения **производительности и масштабируемости** поставщики оцениваются по стандарту ISO / IEC 19086-1: 2016 «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции», ISO / IEC 22313 «Менеджмент непрерывности бизнеса. Руководство по внедрению».

Засчитываться могут сертификаты и по частным системам сертификации. В частности, российские ЦОД часто проходят сертификацию по американским стандартам **Tier 3**, **Tier 4**. Хотя система разработана американским институтом Uptime Institute, система очень популярна в мире – по стандартам Tier сертифицировано более 1700 ЦОД в 98 странах мира, в том числе в России (ЦОДы Ростелеком, МТС, и др.)[1].

**ФСТЭК** может определить **рекомендованные международные стандарты** для облачных провайдеров, соответствие которым могут **декларировать сами облачные провайдеры**. То есть, ФСТЭК может принимать (признавать) сертификаты провайдеров облачных услуг, которые добровольно сертифицировались по международным стандартам.

Также ФСТЭК может использовать зарубежные стандарты сертификации при выработке требований безопасности для мультиоблачных систем.

В **Сингапуре** Комитет по стандартам в области информационных технологий разработал стандарт 584 (Multi-Tier Cloud Security (MTCS)/ Standard 584)[2] на основе комплекса стандартов **ISO 27000** по обеспечению информационной безопасности.

Наравне со стандартом MTCS была создана **Схема сертификации MTCS** с целью поощрения внедрения надежных методов управления рисками и безопасности поставщиками услуг связи посредством сертификации MTCS.

Стандарт включает более **20 направлений**: управление информационной безопасностью, рисками, инцидентами, данными; правовой комплаенс; аудит и мониторинг; конфигурация безопасности; шифрование; управление изменениями; аварийное восстановление; администрирование облачных систем; виртуализация и защита сети и пр., включая особенности функционирования мультиоблачных систем[3].

Следует отметить, что при введении альтернативных решений по установлению соответствия требованиям информационной безопасности **ФСТЭК** для средств информационной защиты и для центров обработки данных может сформировать **рекомендации по проведению аудита мер безопасности облачного провайдера** для государственных облачных систем. В регулирующих актах ФСТЭК нет общих требований к проведению аудита информационной безопасности систем.

ФСТЭК может разработать **руководство по аудиту информационной безопасности** специально для государственных информационных систем на основе облачных технологий. Тем более, что в российском праве уже осуществляется практика введения обязательного внутреннего аудита для информационных систем в отдельных отраслях. Например, в соответствии с Положениями

1 https://ru.uptimeinstitute.com/tier-certification/tier-certification-list

2 https://www.site24x7.com/learn/datacenter/data-center-security-and-privacy-for-singapore.html

3 https://www.singaporestandardseshop.sg/Product/SSPdtDetail/b5430dc1-27f3-4203-bd8e-00345da6bed5

Банка России № 672-П, № 683-П и № 684-П с 1 января 2021 года проведение финансовыми организациями оценки соответствия требованиям ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций» стало обязательной процедурой.

Стоит отметить, что первая версия Методических рекомендаций по включению сервисов в платформу «ГосТех» 2022 г. включает вопрос подтверждения соответствия требованиям информационной безопасности облачного сервиса. Облачный провайдер, заинтересованный в участии в «ГосТех», должен представлять **манифест о характеристиках своего облачного сервиса**, где указываются данные сертификата в области информационной безопасности (п. 5.4.5), полученного от ФСТЭК1.

В данном случае в качестве альтернативы возможно было бы признавать **сертификаты соответствия** требованиям по информационной безопасности, **полученные по международным и зарубежным системам стандартов**, что упростит доступ поставщика к участию в «ГосТех». Поэтому возможно внести изменения в Положения о системе сертификации средств защиты информации, утвержденные Приказом ФСТЭК №55 от 3 апреля 2018 г., в части введения возможности учета международных и зарубежных сертификатов облачного провайдера (как минимум, частично в отдельных аспектах сертификации мультиоблачных платформ)[2].

### Планируемые изменения в регулировании в сфере требований к защите информации

В августе 2021 г. ФСТЭК представила законопроект, направленный на установление **требований о защите информации**, обладателями которой являются государственные органы, вне зависимости от места ее хранения или обработки (ID проекта 01/05/08-21/00118865)[3].

ФСТЭК считает, что создание информационных систем и государственных сервисов на единой цифровой платформе «ГосТех» происходит без учета требований о защите информации, установленных ч. 5 ст. 16 ФЗ «Об информации, информационных технологиях и о защите информации». В результате снижается уровень защиты информации как государственного информационного ресурса[4].

Поэтому законопроект предлагает внести в ФЗ положение о том, что ФСТЭК и ФСБ будут совместно разрабатывать требования защиты информации, которой обладают государственные органы.

В соответствии с законопроектом предполагается, что требования защиты информации, которой обладают государственные органы, будут обязательными к соблюдению операторами информационных систем, в которых обрабатывается государственная информация (оператором может выступать как государственный орган, так и третье лицо по смыслу п. 12 ст. 1 ФЗ-149).

В соответствии с такими требованиями операторы информационных систем должны создавать системы **организации** и **управления защиты информации**. Система организации и управления защиты информации состоит из лиц, ответственных за защиту информации и контроль ее эффективности, и средств защиты информации.

### Выводы и рекомендации по вопросам совершенствования процесса аттестации облачных сервисов

Для оптимального регулирования вопросов сертификации средств защиты информации облачных систем и аттестации ЦОД возможно принятие ряда мер:

1 https://d-russia.ru/wp-content/uploads/2022/03/proekt_metodicheskie_rekomendatsii_po_vklyucheniyu_servisov_na_platformu_gostekh.pdf

2 https://docs.cntd.ru/document/542622316?marker=64U0IK

3 https://regulation.gov.ru/projects#npa=118865

4 Пояснительная записка к проекту 01/05/08-21/00118865

### 1. Ускорение процедур аттестации и сертификации ФСТЭК за счет признания международных стандартов

Могут быть введены механизмы зачета сертификации по международным стандартам по отдельным требованиям безопасности для мультиоблачных технологий (в том числе в рамках Методических рекомендаций по включению сервисов в платформу «ГосТех» 2022 г.).

ФСТЭК может определить перечень рекомендованных международных стандартов, сертификация по которым может квалифицироваться как соответствие требованиям ФСТЭК, например стандарты ISO 27000.

### 2. Разработка требований о защите информации с учетом международного опыта

ФСБ и ФСТЭК намерены совместно разрабатывать требования о защите информации, обладателями которой являются государственные органы, вне зависимости от места ее хранения или обработки в соответствии с проектом поправок в ФЗ-152 «Об информации» (ID проекта 01/05/08-21/00118865)1.

Поэтому с учетом международного опыта (США, стран ЕС) целесообразно, чтобы такие требования учитывали вопросы, стандарты, разработанные ФСТЭК в отношении облачных технологий, могут учитывать задачи по:

- обеспечению **интероперабельности** систем;
- обеспечению **переносимости данных** в мультиоблачных системах;
- внедрению системы **оценки производительности** и **качества** поставляемых услуг;
- внедрению требований к постоянному **аудиту** систем (на данный момент, например сроки проведения аудита могут устанавливаться поставщиками самостоятельно, например, раз в год или раз в 3 месяца, что создает риски безопасности);
- внедрению требований к прозрачности и предоставлению информации заказчику или оператору о работе облачных систем и пр.

Например, в **Италии** требуется, чтобы для обеспечения интероперабельности и переносимости поставщики IaaS и PaaS использовали открытые стандарты (например, Open Virtualization Format) и соответствующий программный интерфейс приложения (API).

1 https://regulation.gov.ru/projects#npa=118865

# III. Анализ 44-ФЗ «О государственных закупках» на предмет административных барьеров для использования публичных облачных сервисов в проектах «ГосОблако» и «ГосТех»

По опыту зарубежных стран одним из важных направлений для перехода государственных органов на облачные услуги является создание **инструментов для закупки таких технологий**.

В 2016 г. ОЭСР был принят **Инструментарий цифрового правительства**, в рамках которого Принцип 11 рекомендовал странам при закупке таких технологий, как облачные услуги, адаптировать закупочное законодательство, в частности, необходимо учитывать, что сами услуги могут оплачиваться в зависимости от времени использования, количества пользователей, количества занимаемого для хранения данных места и пр., поэтому установление твердых цен или каких-либо пороговых значений для контрактов может ограничивать закупки облачных услуг[1].

Например, **цены на услуги IaaS** варьируются в зависимости от используемой операционной системы, количества центральных процессоров, памяти и доступных хранилищ файлов и других факторов, при этом стоимость услуг может взиматься, например, за гигабайты данных, хранящихся в месяц, за секунду/ минуту использования и пр.

Плата **за услуги PaaS** может взиматься в зависимости от используемой вычислительной мощности и требований к хранению данных, как и в случае IaaS. Плата **за услуги SaaS** чаще всего взимается в виде абонентской платы за каждого пользователя в месяц, в том числе может учитываться период обслуживания.

Ввиду этого, в России важно **адаптировать систему государственных закупок** с учетом того, что облачные услуги чаще всего предоставляются по запросу, поэтому оплата таких услуг должна происходить с учетом объема потребленных услуг (**принцип «pay-as-you-go»**). В целом по сравнению с опытом зарубежных стран в России можно выделить ряд отличий в сфере закупок облачных услуг.

### Возможности внедрения принципа «pay-as-you-go» при осуществлении государственных закупок облачных услуг

В России в соответствии со статьей 34 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – 44-ФЗ), стоимость контракта может указываться:

1. **в твердой цене на весь срок контракта**

Стоимость является **фиксированной** за все товары, услуги, работы, предоставляемые по контракту.

1 https://www.oecd.org/governance/digital-government/toolkit/principle11/

**ПРИМЕР:** в ноябре 2020 г. Минцифры заключило контракт на проведение эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе «ГосТех» с ПАО «Сбербанк», при этом цена контракта являлась **твердой**.

Фактически закупка осуществляется по принципу «платы на экземпляр»» (pay-by-instances), когда государство платит за каждый используемый сервер или экземпляр виртуальной машины, который запускает поставщик в рамках услуг IaaS и PaaS.

**МИНУСЫ:** такой способ не удобен для поставки облачных услуг, так как государственным органам может быть **трудно рассчитать точное количество** облачных услуг, которые потребуются для ГИС. Например, может быть трудно рассчитать количество пользователей облачных услуг, количество места для хранения данных (в том числе точное количество данных, которые будут храниться) и пр.

2. **по цене за единицу товара, работы, услуги и максимальное значение цены контракта**

Данный способ применяется, если количество поставляемых товаров, объем подлежащих выполнению работ, оказанию услуг невозможно определить.

**ПРИМЕР:** такой способ уже используется для закупок в рамках проекта «ГосОблако». Например, в декабре 2020 г. Минцифры заключило контакт на сумму 2,98 млрд руб. с поставщиком ООО «Центр хранения данных» (дочерняя компания Ростелекома)[1]. Стоимость формировалась исходя из **цены за единицу услуги в сутки** пропорционально **количеству дней фактического оказания** с учетом коэффициента качества оказанных услуг.

В рамках контракта установлены цены за каждый вид услуги в рублях в день. Однако в рамках контракта все равно установлено максимальное значение цены контракта, что создает неудобство для закупки облачных услуг, так как превысить такую цену нельзя.

При этом в контракте обслуживание устанавливается исходя из цены за день, независимо от того, какое количество услуг потреблялось, тогда как **поставщики предлагают варианты цен за минуту или секунду, что позволяет экономить**, оплачивая услуги по количеству использованного времени, а не по дневной ставке использования. Либо же возможна оплата по количеству места, занимаемого для хранения данных, а не полная аренда всего сервера.

**МИНУСЫ:** если устанавливать цену за минуту или секунду, либо за гигабайт памяти, то возникают проблемы. Например, если фактическое количество потребленных услуг за все время оказалось меньше стоимости, заложенной в рамках контракта, то государство фактически **переплачивает за неиспользованные мощности**.

А если количество потребленных услуг значительно выросло в пиковый период обслуживания, то поставщик не может взимать цену за услуги выше максимального значения цены контракта. В таком случае заказчик и поставщик могут изменить цену контракта, но не более чем на 10%, либо расторгнуть контракт по обоюдному согласию (согласно ст. 95 44-ФЗ).

3. **ориентировочное значение цены контракта либо формула цены и максимальное значение цены контракта**

Такой способ используется для отдельных видов контрактов в соответствии с постановлением Правительства РФ от 13 января 2014 г. № 19 «Об установлении случаев, в которых при заключении контракта указываются формула цены и максимальное значение цены контракта».

К таким контрактам относится контракт на предоставление услуг обязательного страхования, агентских услуг, услуг по оценке недвижимого имущества, на выполнение работ по проектирова-

1 https://zakupki.gov.ru/epz/contract/contractCard/document-info.html?reestrNumber=1771047437520000074

нию, строительству и вводу в эксплуатацию объектов капитального строительства и пр. Данный перечень услуг является закрытым, что не дает возможности осуществлять закупки облачных услуг.

Стоит отметить, что максимальное значение цены контракта формируется из начальной (максимальной) цены контракта. При этом в России существует **проблема применения начальной (максимальной) цены контракта**, которая не может быть скорректирована, например, если заказчиком была неверно рассчитана цена контракта, затраты превысили плановые расчеты и пр.

Таким образом, для закупки устанавливаются **максимальные суммы контракта**, что больше подходит для капитальных затрат и создает сложности для закупки облачных услуг, которые могут быть также и операционными.

При этом облачные услуги можно закупать по запросу (on-demand) или по количеству используемых услуг (pay-per-use), по количеству пользователей, то есть **оплачивать услуги по мере использования (в минутах, в секундах)**, а не по обязательной ежедневной ставке в рамках максимального значения цены контракта.

В **США** возможно сочетать 2 метода ценообразования: часть закупать по модели «**твердой фиксированной цены**» (цены, рассчитанной на весь контракт), а еще часть по модели «**времени и материалов**» (цена формируется исходя из количества потребленных услуг, например, если было потреблено больше услуг, чем это изначально рассчитывалось)[1].

При этом для государственных органов **установлены максимальные затраты**, которые госорган может понести в отношении конкретной услуги или группы значение цены контракта; если стоимость фактически поставленных услуг меньше, чем величина максимальных затрат, то заказчик все равно оплачивает только стоимость фактически поставленных услуг.

В **Италии** и **Германии** в рамках контрактов реализуется **принцип «pay per use»**, то есть, оплата услуг происходит в зависимости от количества потребляемых ресурсов в конце определенного периода.

При этом, например, в странах **ЕС** действует возможность **не устанавливать цену контракта** в отношении контрактов, **срок** которых **не превышает 48 месяцев**.

Стоит отметить, что в марте 2022 г. Минцифры представило первую версию Методических рекомендаций по включению сервисов в Единую цифровую платформу «ГосТех», которые устанавливают **«принцип оплаты фактического объема потребления»** – оплата потребления Сервисов, входящих в состав ЕЦП ГосТех, должна осуществляться преимущественно по факту их потребления.

**NB!** В России планируется реализовать принцип «pay-as-you-go» в рамках закупок по ГосТех.

Таким образом, в России возможно внедрение различных дополнительных способов формирования цены и видов контрактов. Например, по принципу «времени и материалов» либо по оплате по количеству потребленных товаров/услуг/работ (pay-per-use; pay-as-you-go) без установления конкретной цены в контракте и пр.

Для закупок облачных услуг необходимо, чтобы такой контракт включал:

- **возможность оплачивать товары/услуги/работы по стоимости фактически оказанных услуг**, реализуя принцип «pay-as-you-go», например, оплачивать услуги за терабайт/гигабайт памяти, минуту/секунду использования и пр.

1 https://cic.gsa.gov/acquisitions/pricing

При этом для такого контракта возможно формировать **начальную (максимальную) цену за единицу** товара/услуги путем обращения к участникам закупки.

- **возможность поставщиков оценивать объем/количество** поставленных товаров/услуг/работ за отчетный период с предоставлением заказчику механизмов для проверки и контроля объема.

Стоит отметить, что при внедрении таких форм контракта по принципу «pay-as-you-go», необходимо будет менять нормы действующего закупочного законодательства. Например, при проведении электронного аукциона (по ст. 49), необходимо будет определить возможность подачи предложений по снижению не только начальных (максимальных) цен контракта или суммы цен единиц товара/работы/услуги, но и начальных (максимальных) цен за единицу товара/услуги.

### Возможности внедрения системы рамочных контрактов, а также использования соглашений об уровне обслуживания при осуществлении государственных закупок облачных услуг

В странах ЕС, США и других странах распространены рамочные контракты для закупки облачных услуг, то есть контракты с одним или несколькими заказчиками и одним или несколькими поставщиками. Такие рамочные контракты обладают рядом особенностей (в соответствии с **Типовым законом ЮНСИТРАЛ о публичных закупках 2011 г**.)[1].

Рамочные контракты используются, если необходимость в объекте закупок будет, как ожидается, возникать на неопределенной или многократной основе в течение какого-либо конкретного периода времени или на безотлагательной основе. То есть, рамочные контракты подходят для товаров/услуг/работ, которые **закупаются неоднократно, регулярно, в разном количестве.**

**Процедура рамочного соглашения** проходит в два этапа:

- **ПЕРВЫЙ ЭТАП** – отбор поставщиков: заключается общее рамочное соглашение, к которому могут присоединиться все поставщики, подходящие под требования закупки.

При этом существуют закрытые соглашения – определяется конкретный перечень подходящих поставщиков, новые поставщики не могут присоединяться; и открытые соглашения – могут присоединяться новые поставщики.

- **ВТОРОЙ ЭТАП** – заключение индивидуального договора о закупке согласно рамочному соглашению с поставщиками, которые стали стороной рамочного соглашения. На втором этапе заказчик размещает заказ на закупку по мере возникновения потребности в конкретной услуге/работе/товаре. На данном этапе может проводиться закупка без конкуренции у одного или нескольких поставщиков, либо проводиться конкурс на поставку.

В России на данный момент в 44-ФЗ не содержится подобного вида контракта, когда существует возможность заключить рамочное соглашение с несколькими поставщиками (согласно ст. 26, возможны централизованные закупки для нескольких заказчиков), так как в соответствии со ст. 24 выбирается один участник закупки, который признается победителем конкурса.

Между тем, в странах ЕС (например, Франция, Италия, Швейцария) с поставщиками облачных услуг активно заключаются рамочные соглашения, особенно для поставки услуг IaaS, PaaS. Это позволяет обеспечить реализацию принципа мультиоблачности (мультиклаудного облака), когда **к закупке привлекаются**, например**, несколько поставщиков** услуг ЦОД **на равных условиях** при определении индивидуальных условий в отдельных контрактах (уточнение отдельных услуг, сроков (могут быть меньше срока самого рамочного соглашения), цен). Рамочное соглашение позволяет **добавлять новых поставщиков**, например, если необходимо увеличение поставки услуг.

1 https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ru/2011-model-law-on-public-procurement-r.pdf

В **России возможно развитие рамочных соглашений**, которые дадут возможность участия в закупке сразу нескольких «со-победителей», что может упрощать реализацию принципа мульти-облачности (мультиклаудного облака), так как рамочное соглашение позволяет проводить не отдельную закупку с каждым поставщиком, а привлечь сразу несколько поставщиков на единых условиях.

Внедрение рамочного соглашения должно основываться на следующих особенностях:

1. **закупка должна проходить в два этапа**:

- первый этап – **отбор поставщиков** (со-победителей), которые соответствуют критериям закупки, и заключение с ними общего рамочного соглашения.

- второй этап – **заключение договора** о закупках согласно рамочному соглашению с поставщиками, которые стали стороной рамочного соглашения (то, есть заключение контракта с индивидуальными условиями, определяющего объем поставки, стоимость услуг и пр., а также соглашения об уровне обслуживания).

В рамках второго этапа может проводиться конкурс на определение одного или нескольких поставщиков наиболее подходящих для оказания услуг;

2. **соглашение дает возможность присоединяться новым поставщикам**

Это позволит присоединять поставщиков с новыми видами услуг, либо предлагающих инновации существующих облачных слуг.

При внедрении рамочных соглашений необходимо будет вносить ряд изменений, например, ввести **понятие «со-победителей»**, изменить ст. 24 44-ФЗ, установив возможность выбора нескольких участников закупки, которые будут признаваться победителями конкурса.

По опыту зарубежных стран в России могут быть **разработаны минимальные требования к соглашению об уровне обслуживания (SLA)** либо типовые соглашения, которые:

- могут включать вопросы **безопасности данных** и вопросы **распределения ответственности за безопасность**. Например, поставщики услуг IaaS не имеют доступа к данным, тогда как в рамках услуг SaaS поставщик может получить доступ к данным и осуществлять шифрование неактивных данных;

- учитывать вопросы **управления данными**, например, интероперабельность, переносимость при расторжении контракта или возникновении аварийной ситуации; вопросы **оценки качества** поставляемых услуг и проведения аудита и пр.

Важно также учитывать, что **соглашение об уровне обслуживания должно признаваться частью закупочной документации**. Кроме того, необходимо создать правовые нормы, позволяющие вносить изменения в соглашение, которые должны согласовываться сторонами, например, если поставщик вводит обновления, например, повышает производительность, водит дополнительные полезные функции, инструменты предотвращения рисков и пр.

### Возможности внедрения системы маркетплейсов и каталога аккредитованных поставщиков облачных услуг

По опыту зарубежных стран (США, стран ЕС) для закупок облачных технологий внедряются **системы маркетплейсов** и **каталога аккредитованных поставщиков облачных услуг**. На данный момент в России обсуждается идея выделения в рамках проекта «ГосТех» части SaaS, которая может быть выделена в отдельный маркетплейс.

Кроме того, в России запущены частные маркетплейсы облачных услуг. Например, собственный маркетплейс запустила компания Яндекс[1], объединив поставщиков облачных услуг в том числе в разных отраслях. Аналогично запущен Cloud Marketplace от VK Cloud Solutions, маркетплейс Market.CNews и пр.

При внедрении маркетплейса и каталога поставщиков облачных услуг в России возможно использовать опыт зарубежных стран:

1. **привлечение поставщиков, аккредитованных/ квалифицированных государственными органами**

На зарубежные маркетплейсы для поставщиков облачных услуг для государственных органов могут попадать поставщики, аккредитованные/ квалифицированные специальными государственными органами.

Аккредитация/квалификация подтверждает **соответствие поставщика необходимым требованиям безопасности**, интероперабельности, наличия системы управлением качеством услуг, наличия процедур управления инцидентами и пр.

Аккредитация/квалификация поставщиков действует в среднем 2–3 года. Чаще всего разрабатываются отдельные требования для аккредитации/ квалификации поставщиков в зависимости от поставляемых услуг: IaaS, PaaS или SaaS, которые чаще всего базируются на общепринятых международных стандартах, например, **стандартах ISO** (группы ISO 20000 для управления и обслуживания ИТ-сервисами, ISO / IEC 27017 по обеспечению безопасности для поставщиков и пользователей облачных услуг и пр.).

2. **создание общедоступного каталога поставщиков**

На зарубежных маркетплейсах формируется общедоступный каталог поставщиков, из которых государственные органы могут выбрать поставщиков и их услуги.

Указывается **информация о поставщике**, а также его **услугах**, включая технические характеристики, модель затрат и уровни обслуживания, контактную информацию, **базовая цена** на услуги (которая не влияет на закупочный процесс, а носит исключительно информационный характер для понимания порядка ценообразования).

То есть госорганы могут сравнивать аналогичные услуги и выбирать наиболее подходящие решения, исходя из своих потребностей.

3. **маркетплейс должен действовать отдельно от государственных облаков**

Зарубежные маркетплейсы позволяют выбирать все виды услуг IaaS, PaaS, SaaS, при этом маркетплейсы действуют отдельно от государственных облаков и служат **для формирования государственными органами закупочной документации**, процесса планирования закупок, установления цен закупки и пр.

Таким образом, в России маркетплейс может представлять собой вспомогательный инструмент для осуществления государственных закупок, позволяющий заранее ознакомиться с предложениями поставщиков, сформировать требования к закупке, при этом государственные органы могут быть уверены, что поставщики прошли предварительную квалификацию/аттестацию по требованиям безопасности, интероперабельности, управления рисками, инцидентами и пр. по международным и внутренним стандартам.

1 https://cloud.yandex.ru/marketplace

## Выводы и рекомендации по формированию позиции компании Яндекс по вопросам совершенствования процесса закупок облачных сервисов

Учитывая выявленные проблемы, облачный провайдер может предложить собственное видение развития закупочного законодательства. Позиция компании Яндекс может включать следующие пункты:

1. **внедрение принципа оплаты услуг по мере их использования (принцип «pay-as-you-go»)**

В России возможно внедрение такого принципа для оплаты облачных товаров/услуг/работ по стоимости фактически оказанных услуг, то есть оплачивать услуги за терабайт/гигабайт памяти, минуту/секунду использования и пр., формируя начальную (максимальную) цену за единицу товара/услуги путем обращения к участникам закупки. В данном случае важно внедрять отчетность поставщиков об объеме потребленных товаров/услуг/работ.

2. **внедрение рамочных соглашений**

В России необходимо внедрение рамочных соглашений, которые дадут возможность участия в закупке сразу нескольких «со-победителей» на единых условиях.

Закупка должна начинаться с отбора поставщиков (со-победителей) и заключения с ними общего рамочного соглашения, далее должны заключаться индивидуальные договоры с каждым поставщиком, ставшим стороной рамочного соглашения (то, есть заключение контракта с индивидуальными условиями, определяющего объем поставки, стоимость услуг и пр., а также соглашения об уровне обслуживания). Такие соглашения должны давать возможность присоединяться новым поставщикам.

3. **внедрение требований к SLAs**

Необходимо определить минимальные требования к соглашению об уровне обслуживания (SLA) либо ввести типовые соглашения, которые могут включать вопросы безопасности данных, распределения ответственности за безопасность, интероперабельности, переносимости данных, оценки качества поставляемых услуг и проведения аудита и пр.

4. **создание маркетплейса аккредитованных поставщиков облачных услуг**

В России возможно создание маркетплейса аккредитованных поставщиков облачных услуг, который представляет вспомогательный инструмент перед осуществлением государственных закупок. Маркетплейс может содержать каталог поставщиков услуг, предоставлять возможность ознакомиться с предложениями поставщиков, сформировать требования к закупке и пр.

# Рекомендации: как дальше развивать «ГосОблако» и «ГосТех» в России?

### Развитие принципа мультиоблачности (мультиклаудного облака)

Принцип мультиоблачности уже планируется внедрить в рамках проектов «ГосОблако-2» и «ГосТех», однако рекомендуется его полноценная реализация **в течение ближайших 3–6 месяцев** с учетом планов по внедрению в 2022 г. проекта «ГосТех».

Необходимо принять **стандарт для мультиоблачного (мультиклаудного) государственного облака,** включая требования к сервисам и провайдерам в части информационной безопасности, совместимости, переносимости данных, реагирования на инциденты и пр.

Данный принцип позволит создать единое коммунальное облако вместо множества частных облаков для ГИС. Это создаст возможность при необходимости переходить из одного облака в другое, обеспечив безопасность данных, эластичность, масштабируемость, совместимость сервисов. Мультиклаудное облако также позволит Минцифры России оптимизировать затраты за счет диверсификации поставщиков с наиболее выгодными ценами за отдельные типы услуг (по исследованию VMware, мультиоблачность позволяет на 38% сократить операционные расходы на ИТ[1]).

### Упрощение процесса сертификации и аттестации ФСТЭК

Для участия на платформе «ГосТех» облачным провайдерам необходимо проходить сертификацию средств защиты и аттестацию центров обработки данных в соответствии с требованиями ФСТЭК. Однако на данный момент процесс прохождения сертификации вынужденно совмещен с процессом разработки самих требований для облачных платформ по типу «community cloud», что создает трудности для участия новых поставщиков.

Для реализации принципа мультиклауда на платформе «ГосТех» должно участвовать множество облачных поставщиков, поэтому важно **ускорить процесс прохождения сертификации и аттестации облачных провайдеров** к запуску платформы «ГосТех», запланированному до конца 2022 г.

Опыт зарубежных стран (Италии, Германии, Сингапура) показывает, что процесс квалификации поставщиков может быть упрощен за счет **признания сертификации по международным стандартам** (например, стандартам ISO).

Поэтому в ближайшие **3–6 месяцев** возможно внести изменения в Приказ ФСТЭК №55 и Приказ ФСТЭК №17 в части введения положений **о механизмах зачета сертификатов, полученных по зарубежным или международным стандартам** в области облачной информационной безопасности. С учетом зарубежной практики квалификации облачных провайдеров для публичных облачных систем, такие механизмы могут упростить и ускорить получение доступа поставщиков облачных услуг к участию в «ГосТех».

1 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-multi-cloud-management-overview.pdf

## Закупки облачных услуг

### 1. Реализация принципа «pay-as-you-go»

Согласно первой версии Методических рекомендаций по включению сервисов в Единую цифровую платформу «ГосТех», устанавливается **«принцип оплаты фактического объема потребления»**, то есть, планируется реализовать принцип «pay-as-you-go».

На данный момент 44-ФЗ (о государственных закупках) в части регулирования правил определения стоимости контракта (ст. 34) не дает возможности оплачивать услуги по факту их потребления независимо от общей цены контракта, так как устанавливается либо **твердая цена**, либо **максимальное значение цены** контракта.

С учетом того, что проект «ГосТех» планируется запустить уже в 2022 году, **в ближайшие 3 месяца** рекомендуется внесение поправок в 44-ФЗ в части реализации принципа «pay-as-you-go», устанавливая, что при формировании стоимости контракта может устанавливаться **принцип оплаты услуг по факту их потребления**, например, оплачивать услуги за терабайт/гигабайт памяти, минуту/секунду использования и пр. При этом для такого контракта возможно формировать начальную (максимальную) цену за единицу услуги путем обращения к участникам закупки.

### 2. Внедрение рамочных контрактов

Опыт зарубежных стран (США, Италии, Германии) показывает, что при закупке облачных услуг используются рамочные соглашения. Закупка проводится в два этапа: сначала заключается рамочное соглашение с множеством поставщиков, соответствующих требованиям оказания облачных услуг, далее по мере возникновения потребности с поставщиками заключаются индивидуальные контракты.

Внедрение в России рамочных контрактов для закупки облачных услуг **в ближайшие 3–6 месяцев упростит процедуру закупок**, так как снизит временные и административные издержки на отбор поставщиков для каждой отдельной закупки с выбором одного победителя, так как будет определен **пул квалифицированных поставщиков**.

Это удобно при реализации принципа мультиоблачности, так как в закупках может участвовать несколько поставщиков, каждый из которых является «со-победителем» и может оказывать услуги в рамках «ГосОблака» и «ГосТеха» одновременно с другими поставщиками.

### 3. Внедрение маркетплейса и каталога поставщиков облачных услуг

В России существует множество компаний – поставщиков облачных услуг, включая ООО «Яндекс.Облако», ПАО «Вымпелком», компания КРОК, ООО «Облачные технологии», ООО «Селектел», ПАО «МТС», VK Cloud Solutions, которые могут поставлять услуги SaaS, PaaS, IaaS для государственного облака.

Поэтому важно ускорить **создание маркетплейса с каталогом поставщиков облачных услуг**, среди которых государственные органы могут выбрать поставщиков, сравнивая их услуги (технические характеристики, модель затрат и уровни обслуживания, цены) для выбора наиболее оптимальных поставщиков.

Это упростит процесс формирования государственными органами закупочной документации, процесс планирования закупок, установления цен закупки и пр.

## Таблица 1. Внедрение облачных технологий государственными органами в зарубежных странах и в России

| | Критерий | ЕС | США | Италия | Германия | Россия |
|---|---|---|---|---|---|---|
| 1. | наличие стратегии по развитию облачных технологий | ДА | ДА | ДА | ДА (только в части стандартов безопасности) | НЕТ, только отдельные концепции ГЕОП и ГосТех |
| 2. | система единого облака / каждый государственный орган переходит на облако отдельно | - | каждый государственный органа переходит на облако отдельно | единое облако | единое облако для чувствительных данных; каждый государственный орган может перейти на облако отдельно | единое облако: ГЕОП (IaaS) + ГосТех (PaaS, SaaS) |
| 3. | внедрение принципа мультиоблачности | ДА | ДА | ДА | ДА | в процессе внедрения |
| 4. | создание частных облаков для данных, имеющих особую чувствительность, важность для государственной безопасности | - | ДА, каждый государственный орган сам определяет тот уровень безопасности, который ему необходим, и облако развертывается, исходя из нужд госоргана | ДА, в рамках национальных стратегических хабов для хранения стратегических данных | ДА | НЕТ |
| 5. | разработка руководств для государственных органов по миграции/ использованию облачных технологий | - | ДА | ДА | ДА | в процессе разработки |
| 6. | разработка собственных стандартов для сертификации / аккредитации поставщиков | ДА, в проекте European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) | ДА | ДА | ДА | аккредитация ФСТЭК для ЦОД |
| 7. | использование международных стандартов при разработке собственных стандартов для сертификации / аккредитации | ДА, в т.ч. ISO | НЕТ, используют собственные стандарты:<br>– NIST[1];<br>– FIPS PUB[2];<br>– Tier Standards (Uptime Institute) | ДА<br>– ISO/IEC 20000 (в т.ч. ISO/IEC 20000-1[3] и ISO/IEC TR 20000-9[4])<br>– ISO / IEC 27017[5], ISO / IEC 27018[6] для SaaS<br>– ISO / IEC 19086-1: 2016 для SLAs[7]<br>– ISO / IEC 22313[8] | ДА<br>– ISO 27001[9]<br>– ISO 27002[10]<br>– ISO 27017;<br>– ISO 27018[11] | НЕТ |

1 Стандарты Национального института стандартов и технологий США

2 Система публикаций Федеральных стандартов обработки информации (Federal Information Processing Standards Publications, FIPS Publications)

3 ISO/IEC 20000-1 «Требования к системе управления услугами»

4 ISO/IEC TR 20000-9 «Руководство по применению ISO/IEC 20000-1 к облачным сервисам»

5 ISO / IEC 27017 «Свод правил по управлению информационной безопасностью» (включающий стандарты аудита информационных систем и облачных служб)

6 ISO / IEC 27018 «Свод правил по защите персональных данных в облаке»

7 ISO / IEC 19086-1: 2016 «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции»

8 ISO / IEC 22313 «Менеджмент непрерывности бизнеса. Руководство по внедрению»

9 ISO 27001 «Системы обеспечения информационной безопасности»

10 ISO 27002 «Свод норм и правил менеджмента информационной безопасности»

11 ISO 27018 «Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки».

| | Критерий | ЕС | США | Италия | Германия | Россия |
|---|---|---|---|---|---|---|
| 8. | возможность государственного органа предъявлять собственные требования к безопасности данных | - | ДА | НЕТ | ДА, если внедряется отдельное облако | НЕТ |
| 9. | соблюдение законодательства о защите персональных данных | ДА | ДА | ДА | ДА | ДА |
| 10. | предусмотрены стандарты аудита | ДА | ДА | ДА | ДА | НЕТ |
| 11. | страхование поставщиков от киберрисков | добровольное | добровольное | добровольное | добровольное | добровольное |
| 12. | наличие маркетплейса / каталога поставщиков облачных услуг | ДА, в проекте European cloud services marketplace | ДА, маркетплейс и каталог | ДА, маркетплейс и каталог | ДА, каталог | В процессе разработки |
| 13 | осуществление закупок через общий портал для закупок | ДА (закупки ЕС институтов и институтов в государствах-членах ЕС) | ДА, часть закупок осуществляется через него | ДА, все закупки осуществляются через него | ДА, все закупки осуществляются через него | ДА, все закупки осуществляются через него |
| 14. | реализация метода ценообразования «pay as you go» | ДА, метод рекомендован европейской ассоциацией CISPE | ДА, в форме метода времени и материалов «Time & Materials», где плата варьируется от счета к счету в течение периода предоставления услуг | ДА, в форме установления цены по тарифам | ДА, в форме оплаты за время фактического предоставления услуги | НЕТ, т.к. закупка либо по твердой цене, либо с применением НМЦК |
| 15. | использование рамочных контрактов с привлечением нескольких поставщиков-победителей | ДА, рекомендовано к использованию | возможно по общему правилу | ДА | ДА, в процессе внедрения | НЕТ, такой тип рамочного контракта не предусмотрен |
| 16. | внедрение рекомендаций по использованию SLA/ создание проекта типового SLA | ДА, Рекомендации по стандартизации SLA (Cloud Service Level Agreement Standardisation Guidelines 2014) | НЕТ | ДА | ДА | НЕТ |
| 17. | регулирование разделения ответственности за безопасность данных между поставщиком и пользователем | ДА, устанавливается в SLA в зависимости от типа услуг IaaS / PaaS / SaaS | ДА, устанавливается в SLA в зависимости от типа услуг IaaS / PaaS / SaaS | ДА, устанавливается в SLA в зависимости от типа услуг IaaS / PaaS / SaaS | ДА, устанавливается в SLA в зависимости от типа услуг IaaS / PaaS / SaaS | специальные правила не разработаны |

# IV. Анализ международного опыта по созданию гособлаков

В рамках анализа международных практик рассматриваются основные стратегии стран в отношении внедрения облачных технологий, а также основные проекты стран, опыт внедрения принципа мультиоблачности, аспекты обеспечения информационной безопасности, управления данными, сертификации, ценообразования и пр.

## 1. Международные стандарты для государственных облаков

Сегодня международные организации анализируют проблемы работы государственных облаков и разрабатывают отдельные стандарты и рекомендации в части режима защиты данных (передачи данных, интероперабельности, переноса данных и пр.), проведения аудита систем, сертификации, осуществления государственных закупок и пр.

### Стандарты Организация экономического сотрудничества и развития (ОЭСР)

В части развития облачных технологий для государственного сектора ОЭСР концентрируется на стандартах защиты данных и информационной безопасности.

В публикации 2021 г. «Понимание цифровой безопасности продуктов» ОЭСР отмечает проблему обеспечения цифровой безопасности облачных сервисов[1]. Например, может возникать конфликт в отношении того, **какие обязанности, в том числе юридические, несут поставщик услуг, клиент, центр обработки данных** и другие участники системы в отношении конфиденциальности данных, например, в обеспечении баланса между защитой данных и доступом государственных органов к данным.

Также риском является ситуация, когда учетные данные пользователей повторно используются в нескольких облачных сервисах, так как утечка данных в одном сервисе может привести к нарушению режима в других облачных сервисах.

ОЭСР отмечает, что **обязанности в отношении данных у поставщиков услуг IaaS, PaaS и SaaS по сравнению с пользователем различаются**: ответственность поставщика SaaS выше, так как контролируется и инфраструктура, и программное обеспечение, тогда как у поставщика IaaS, который контролирует только инфраструктуру, ответственность ниже (рис. 3).

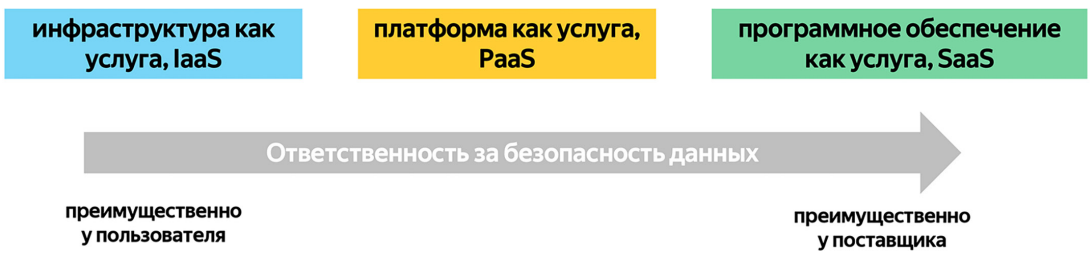



**Рис. 3. Распределение ответственности в отношении данных поставщиков услуг IaaS, PaaS и SaaS и пользователей**

**Источник**: Cloud Security Alliance, Security Guidance (https://cloudsecurityalliance.org/research/guidance/)

1 OECD (2021), "Understanding the Digital Security of Products", OECD Digital Economy Papers, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en

ОЭСР отмечает, что распределение ответственности за защиту данных может быть сложным: пользователи могут и не знать о своих обязанностях, особенно в системах PaaS и IaaS. Например, часто возникает путаница в отношении распределения ответственности за такие действия, как шифрование архивов или обновление программного обеспечения.

**NB!** ОЭСР говорит о необходимости разработки общих стандартов для уточнения ролей и обязанностей каждого участника в отношении режима данных, например, какие меры информационной безопасности должен принимать поставщик облачных услуг, а какие пользователь.

Кроме того, типовые условия **соглашений об уровне обслуживания** (Service Level Agreement, SLA) могут **содержать оговорки, ограничивающие ответственность поставщика** услуг в случае инцидента с информационной безопасностью, поэтому может быть неясным распределение ответственности, например, при неправильной конфигурации сервера.

ОЭСР отмечает, что поставщики облачных услуг должны предоставлять государственным учреждениям четкие и простые способы **мониторинга, управления и аудита оказываемых услуг.**

**NB!** ОЭСР отмечает важность внедрения механизма **сертификации для оценки рисков безопасности данных**, включая проверку соглашений об уровне обслуживания. Также важно обеспечение совместимости и переносимости данных, позволяющих пользователям переключаться с одного сервиса на другой.

### Стандарты других международных организаций и объединений

Ряд международных коммерческих и некоммерческих организаций занимается вопросами разработки стандартов в сфере облачных технологий.

Прежде всего стандарты разрабатывает **Международная организация по стандартизации** (ИСО). Так, например, разработаны стандарты по обеспечению информационной безопасности при использовании облачных служб (ISO/IEC 27017), информационной безопасности для отношений с поставщиками (ISO/IEC 27036-4), стандарты облачных вычислений (ISO/IEC 19086), стандарты совместимости и переносимости данных (ISO/IEC 19941), использования данных (ISO/IEC 19944, ISO/IEC TR 23186), включая трансграничные потоки данных, доступ к данным (ISO/IEC 22624) и пр.

Также разрабатываются стандарты по аудиту облачных услуг (ISO/IEC TR 3445), по концепции мультиоблачного и другого взаимодействия нескольких облачных сервисов (ISO/IEC 5140) и пр.

Стоит отметить, что в России принят ряд ГОСТов для имплементации стандартов ИСО. Например, ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология», который устанавливает понятие *облачных вычислений (cloud computing) – парадигма для предоставления возможности сетевого доступа к масштабируемому и эластичному пулу общих физических или виртуальных ресурсов с предоставлением самообслуживания и администрированием по требованию.*

Вопросами облачных вычислений также занимается **Международный союз электросвязи** (МСЭ), который разработал ряд **технических рекомендаций по облачным вычислениям**, например рекомендации в части набора параметров облачных вычислений для мониторинга (ITU-T Q.3914), по требованиям к архитектуре интеллектуальных периферийных вычислений (ITU-T Q.5001), к структуре и обзору тестирования функциональной совместимости облачных вычислений (ITU-T Q.4040) и пр.

Существует и ряд других инициатив, направленных на развитие стандартов облачных технологий, например, **Институт инженеров электротехники и электроники** (IEEE) разрабатывает интерфейсы переносимости, интерфейсы функциональной совместимости, форматы файлов и правила работы для участников экосистемы облачных вычислений; **Инженерный совет Интернета (**IETF) изучает и разрабатывает модели услуг виртуальных частных сетей.

Стандарты перечисленных международных организаций предназначены как для использования облачных вычислений в бизнес-целях, так и для создания гособлаков, так как поставщики должны обеспечивать безопасность данных, интероперабельность и совместимость систем, проводить аудит и пр.

# 2. Опыт США

По данным Счетной палаты США, внедрение облачных технологий позволяет снизить риски безопасности государственных информационных систем (ГИС), а также сократить расходы на обслуживание. Например, эксплуатация и обслуживание **10 ГИС США**, которые работают от 8 до более 50 лет, обходится в **337 млн долл. США в год**[1].

При этом, по оценкам Frost & Sullivan, обслуживание федерального портала USA.gov в настоящее время обходится в **650 тыс. долл. США** ежегодно, что на **72%** (**1,7 млн долл. США**) меньше, чем его содержание до внедрения облачных технологий[2], а время обновления портала сократилось с **9 месяцев до 1 дня**, в том числе за счет внедрения принципа мультиоблачности.

### Стратегические документы, устанавливающие меры по переходу государственных органов на облачные технологии

Базовым документом по развитию облачных сервисов в государственном секторе является государственная стратегия США **Cloud Smart** 2018 г. (ранее была Стратегия Cloud First 2011 г.), которая определяет перечень мер по переходу Федерального правительства США к облачным технологиям[3].

Реализацией стратегии занимаются следующие государственные органы: Административно-бюджетное управление (Office of Management and Budget, OMB), Администрация общих служб (General Services Administration, GSA) и другие агентства, например Совет уполномоченных по информационным технологиям (Chief Information Officers Council).

**Стратегия Cloud Smart содержит три основных элемента**:

- **Безопасность.** Каждый федеральный орган определяет собственную модель управления данными, размещенными в облаке, которая соответствует его системам управления идентификацией и учетными данными.

То есть, помимо общих стандартов безопасности, государственные органы разрабатывают дополнительные требования к безопасности, например, такой стандарт управления идентификацией лиц, имеющих доступ к ресурсам Министерства и федеральной информации, определен Министерством финансов (Department of Treasury) в Директиве 71-12[4].

1 https://www.gao.gov/assets/gao-21-524t.pdf

2 http://www.frost.com/prod/servlet/cio/232651119

3 https://cloud.cio.gov/strategy/

4 https://home.treasury.gov/about/general-information/orders-and-directives/td71-12

Блок Стратегии по безопасности включает ряд мер, связанных, с установлением **требований к заключению соглашений поставщиками облачных услуг**. Так, предусматривается обновление Программы Управления идентификацией, учетными данными и доступом (Identity, Credential, and Access Management, ICAM) (5 действие Стратегии) в части заключения соглашений об уровне обслуживания (SLA) с поставщиками облачных решений, которое теперь должно содержать требования безопасности, в том числе о постоянном информировании государственного органа о конфиденциальности, целостности и доступности информации, о доступе государственных органов к данным журналов событий, об информировании в случае инцидентов и пр.

Кроме того, в рамках действий по безопасности разработана **система выдачи разрешений на эксплуатацию для поставщиков облачных услуг** в части их доступа к федеральным данным (P-ATO), система аккредитации услуг «программное обеспечение как услуга» в рамах FedRAMP Tailored и пр[1].

Для разработки требований безопасности ИТ-систем в США в 2011 г. запущена **Федеральная программа управления рисками и аккредитацией (FedRAMP)**[2], в рамках которой разрабатываются стандарты безопасности облачных технологий, стандарты аккредитации поставщиков облачных услуг и пр.

- **Закупки.** Cloud Smart содержит меры по совершенствованию использования соглашений об уровне обслуживания (SLA), которые должны соответствовать федеральному регулированию закупок, а также содержать договорные условия, специфичные для облачных коммерческих предложений (то есть соответствовать коммерческой практике, а не только требованиям к закупкам).

**Соглашения должны содержать:** роли и обязанности каждой стороны (например, распределять ответственность в отношении обеспечения безопасности данных), показатели производительности, планы устранения несоответствий, предоставлять государственным органам постоянный доступ к информации об их активах; позволять проводить оценку безопасности и конфиденциальности; требовать от поставщиков применения передовых методов проектирования, развертывания и защиты информационных систем.

Администрацией общих служб (GSA) создана Группа облачных решений — межведомственная команда специалистов по закупкам и облачным технологиям для разработки общегосударственных стандартов внедрения облачных технологий. Например, команда разработала **Программы закупки технологий**, среди которых возможны закупки облачных и связанных с ними технологий по специальному номеру закупки (Special Item Number), который обозначает вид ИКТ-решения для госорганов в зависимости от категории (электронная торговля, услуги по обслуживанию ПО, беспроводные технологии, облачные и связанные с ними технологии и др.)[3]. Группа облачных решений также занимается оценкой государственных контрактов на облачные услуги для разработки перечня рекомендованных контрактов, которые смогут использовать госорганы для закупок.

- **Рабочая сила.** Государственные органы разрабатывают стратегии переквалификации сотрудников.

Таким образом, Стратегия Cloud Smart является базовым стратегическим документом США, который устанавливает основные меры по переходу на облачные технологии федерального правительства. Система правового регулирования развития перехода государственных органов на облачные услуги представлена на рис. 4.

1 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

2 https://www.fedramp.gov/program-basics/

3 https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology/sins-and-solutions-we-offer/cloud-and-cloudrelated-it-professional-services


**Рис. 4. Система базовых документов правового регулирования развития перехода государственных органов на облачные услуги**

## Проекты по созданию государственных облаков

В США действует множество проектов по созданию гособлаков для разных федеральных органов. Одним из проектов по переходу на облачные технологии является **проект Федеральной избирательной комиссии** (FEC), которая через cloud.gov (государственный поставщик облачных услуг) переместила данные в облако и экономит примерно **85%** затрат на хостинг в год (**1,2 млн долларов**)[1]. Проект предназначен для того, что политические кампании и комитеты по всей стране представляли в FEC финансовые отчеты, которые затем публикуются на FEC.gov. FEC планирует запустить через облако электронную систему подачи заявок в рамках избирательной кампании.

**NB!** В США отсутствует единая система государственного облака, на которую переходят всех ГИС, каждое агентство самостоятельно определяет необходимость перехода на облако и отдельно закупает услуги у разных поставщиков с учетом предъявляемых требований безопасности (каждое агентство также может предъявлять свои требования помимо действия общих стандартов безопасности).

**Национальное управление океанических и атмосферных исследований** (NOAA) заключило контракты с **AWS**, **Google** Cloud и **Microsoft** на поставку услуги **IaaS**, чтобы предоставить общественности облачный доступ к экологическим данным агентства[2] в рамках Программы больших данных NOAA (Big Data Program)[3].

**Министерство по делам ветеранов США** (VA) создает облачный ресурс данных VA Data Commons (VADC)[4] с использованием услуг **SaaS**. Платформа включает в себя вычислительную инфраструктуру, совместно размещенные данные и программное обеспечение, инструменты и приложения для управления, анализа и обмена данными. VADC будет работать с несколькими поставщиками, включая **Amazon** Web Services, **Microsoft** Azure и **Google** Cloud Platform.

**Налоговое управление США** также запускает отдельный проект – Программу корпоративного облака (Enterprise Cloud Program)[5] по постепенной миграции работы Налогового управления в облако, на первом этапе происходит перенос электронного документооборота в облако.

1 https://cloud.gov/docs/customer-stories/fec/
2 https://www.noaa.gov/media-release/cloud-platforms-unleash-full-potential-of-noaa-s-environmental-data
3 https://www.noaa.gov/information-technology/big-data
4 https://gcn.com/cloud-infrastructure/2021/08/va-readies-cloud-based-data-platform/316208/
5 https://www.treasury.gov/tigta/auditreports/2020reports/202020010fr.pdf

Таким образом, особенность перехода на облачные технологии в США в том, что каждый государственный орган самостоятельно определяет какие сферы деятельности он перевести на облачные технологии, выбрав несколько поставщиков услуг для разных услуг.

### Мультиоблачный подход (multicloud) к получению облачных услуг

На данный момент, исходя из представленного опыта по реализации проектов по переходу отдельных государственных органов США на облачные услуги, большинство государственных органов привлекают сразу **несколько поставщиков для разных услуг**. Однако такой подход существовал не всегда.

**NB!** В США Стратегия Cloud Smart закладывает мультиоблачный подход к получению облачных услуг с возможностью вовлечения множества поставщиков услуг.

- **Проект Joint Warfighter Cloud Capability**

Проект Joint Warfighter Cloud Capability (JWCC) **Министерства обороны США**. Отличительная особенность проекта в том, что изначально у Министерства обороны был проект JEDI (Joint Enterprise Defense Infrastructure) по созданию единого облака в качестве объединенной корпоративной оборонной инфраструктуры, при этом **поставщиком облачных услуг могла стать только одна компания**.

Однако Министерство обороны изменило подход и в рамках проекта JWCC, и реализует идею проекта JEDI, но уже с применением **мультиоблачного подхода**. На данный момент основными претендентами на получение контракта являются **Microsoft** и **AWS**, при этом участвовать в закупках будут и другие компании (**Google**, **Oracle** Corp.)[1]. По аналогии с собственным облаком Министерства и ВВС США (Cloud One) пользователи с правами администратора могут решить, в каком из двух облаков они хотят размещать свои данные, исходя из того, какие функции им подходят, при этом данные будут перемещаться между облаками.

- **Проект коммерческого облачного предприятия C2E ЦРУ**

Аналогичный переход произвело ЦРУ в рамках контракта на создание коммерческого облачного предприятия C2E. В 2013 году такой **контракт был заключен только с компанией Amazon** Web Services (проект C2S) на предоставление различных услуг облачных вычислений для ЦРУ и спецслужб, включая Агентство национальной безопасности и ФБР, в частности, AWS отвечал за все уровни защиты информации в зависимости от класса, в том числе совершенно секретных данных.

Теперь ЦРУ перешло на **мультиоблачный подход**, и в контракте будут участвовать уже 5 компаний – **Amazon** Web Services, **Microsoft**, **Google**, **Oracle** и **IBM**. ЦРУ необходимо несколько поставщиков и IaaS, и PaaS, и SaaS, но в настоящее время роль каждой компании в проекте не обозначена[2]. Однако известно, что, например, **за размещение совершенно секретных данных AWS будет конкурировать с Microsoft**.

На данный момент переход **Министерства юстиции США** на облачные технологии осуществляется с вовлечением **Microsoft** Azure и **Amazon** Web Services (AWS), что является **мультиоблачным подходом**. При этом компания Veritone стала первым одобренным поставщиком технологии искусственного интеллекта через свою платформу aiWARE для работы в мультиоблачной среде[3].

Пример Министерства юстиции говорит о том, что мультиоблачный подход позволяет легче внедрять инновации по сравнению с подходом, когда облако обслуживает один поставщик. Например, если закупать услуги только у одного поставщика, такой поставщик может не предоставлять отдельных видов инноваций (например, искусственный интеллект, Интернет вещей, 5G и пр.). Поэтому Министерство юстиции в рамках мультиоблачного подхода закупило такие услуги у стороннего поставщика облачных услуг.

1 https://www.defenseone.com/technology/2021/07/how-jedis-ghost-will-bring-bitter-rivals-together/183109/

2 https://about.bgov.com/news/cias-next-cloud-contract-may-be-worth-10b-this-is-it/

3 https://marketplace.fedramp.gov/#!/product/aiware-government?sort=productName&productNameSearch=veritone

**Министерство внутренней безопасности** планирует применять облачные вычисления, чтобы модернизировать свою технологическую инфраструктуру и повысить кибербезопасность[1]. В публичном запросе информации к поставщикам облачных услуг (то есть, Министерство направило опросник поставщикам в целях поиска наиболее подходящего предложения) Министерство указало на использование нескольких моделей облачных услуг – IaaS, PaaS, SaaS[2]. **Контракт будет заключен с одним поставщиком**. При этом для осуществления миграции ЦОД Министерства в облако этот поставщик должен будет **привлечь еще две компании, предоставляющие облачные услуги** и имеющие опыт работы с государственными структурами[3]. Миграционная и таможенная служба США, которая входит в Министерство внутренней безопасности, также разрабатывает собственный проект в области облачных технологий[4]. Государственный орган планирует закупать услуги хостинга облачной инфраструктуры в средах AWS и Microsoft Azure.

Стоит отметить, что **государственные органы США сами становятся поставщиками облачных услуг**. Перечень государственных поставщиков облачных услуг представлен на портале Cloud Information Center в разделе закупок[5]:

- **Проект Cloud.gov**

Например, на данный момент **Администрация общих служб (GSA) создала платформу cloud.gov – платформу как услугу (PaaS)**[6]. Cloud.gov предназначена для упрощения перехода государственных органов на облачные системы и предлагает перечень услуг для госорганов в части миграции их информационных систем в облако.

**Cloud.gov работает на IaaS, поставщиком которой является AWS**. При покупке услуг cloud.gov существует возможность также приобрести некоторые услуги AWS[7]. То есть, cloud.gov является государственным поставщиком облачных услуг, который привлекает другие компании для отдельных видов услуг, например услуг инфраструктуры, а также конкурирует с другими компаниями в предоставлении облачных услуг.

Государственный орган может закупать услуги cloud.gov посредством **межведомственного соглашения** – юридического инструмента, используемого для межведомственного приобретения, обмена фондами или имуществом между двумя госорганами. Межведомственное приобретение представляет процедуру, с помощью которой госорган, нуждающийся в поставках или услугах (запрашивающее агентство), получает их от другого госоргана (обслуживающего агентства)[8]. Поскольку cloud.gov является разработкой госоргана (Администрации общих служб), то для приобретения облачных услуг cloud.gov другим федеральным органом необходимо межведомственное соглашение.

**NB!** Cloud.gov создан на основе проекта с открытым исходным кодом Cloud Foundry, который был разработан для **обеспечения совместимости с несколькими поставщиками IaaS** . Поэтому планируется, что услуги для cloud.gov сможет поставлять Google Cloud Platform, Microsoft Azure или любой другой поставщик общедоступного, коммерческого или частного облака, поддерживающий OpenStack. Это говорит о **развитии концепции мультиоблачности в США**.

- **Проект Cloud One**

Собственные проекты по продаже услуг для создания гособлаков также есть у Министерства обороны США. Проект Cloud One – совместный проект **Министерства обороны и ВВС США**, в рам-

1 https://washingtontechnology.com/2021/02/dhs-makes-tweaks-to-34b-cloud-contract/359448/

2 https://src.bna.com/FPF

3 https://www.datacenterdynamics.com/en/news/department-homeland-security-issues-33bn-data-center-and-cloud-solicitation/

4 https://www.datacenterdynamics.com/en/news/ice-plans-100-million-cloud-spend-aws-and-azure/

5 https://cic.gsa.gov/acquisitions/acquisition-resources

6 https://cloud.gov/docs/overview/what-is-cloudgov/

7 https://cloud.gov/docs/services/intro/

8 https://www.gsa.gov/cdnstatic/B2_S5_Interagency_Acquisition_CLP.pdf

ках которого поставляются услуги **IaaS**, **PaaS**, **SaaS**[1]. Частью проекта является проект milCloud 2.0 – представляет собой совокупность облачных сервисов **IaaS**. Например, через проект milCloud 2.0 подключаются коммерческие облачные сервисы к сетям Министерства обороны (DoD), осуществляется поддержка заключения контрактов на услуги, выставление счетов, учет и автоматическая инициализация. Услуги milCloud 2.0 покупают службы, которые входят в состав Министерства обороны, для миграции своих систем в облачные системы.

- **Проект Federalist**

Администрация общих служб запустила проект Federalist (**услуги SaaS**). Federalist включает в себя поддержку блогов, настраиваемых веб-страниц, интерфейс поиска, встроенную аналитику сайта, возможность размещения и просмотра визуализаций данных, а также подключение к хранилищу Cloud.gov через программный интерфейс приложения (API).

- **Другие проекты**

Геологическая служба США (USGS) и Cloud Hosting Solutions предоставляют услуги облачного хостинга (IaaS, PaaS), доступные через виртуальный центр обработки данных, размещенный AWS по контракту с USGS.

Министерство сельского хозяйства США (USDA), Управление уполномоченного по информационным технологиям (OCIO), Центр услуг цифровой инфраструктуры (DISC) управляют Центром данных государственного предприятия (Government Enterprise Data Center), предоставляющим облачные услуги госорганам (IaaS, PaaS, SaaS).

**FedRAMP Marketplace**

Для реализации мультиоблачного подхода в рамках программы FedRAMP был запущен Маркетплейс (FedRAMP Marketplace) – доступная для поиска и сортировки база данных предложений поставщиков облачных услуг, одобренных по стандартам безопасности в рамках FedRAMP, а также список федеральных агентств, использующих аккредитованные предложения облачных услуг FedRAMP, и признанных FedRAMP аудиторов (сторонних оценочных организаций), которые могут проводить оценку FedRAMP[2]. То есть в рамках FedRAMP Marketplace происходит **аккредитация поставщиков облачных услуг по стандартам безопасности** (поставщики получают аккредитацию FedRAMP), а государственные органы могут выбрать для себя поставщиков, с которыми они планируют сотрудничать. Кроме того, на Маркетплейсе сами поставщики могут узнать информацию о проектах органов власти по переходу на облачные технологии, чтобы узнать о возможностях участия в закупке, а также ознакомиться с перечнем сторонних оценочных организаций FedRAMP.

На маркетплейсе представлено 249 аккредитованныхпоставщиков облачных услуг. Среди них: cloud.gov, Accenture, Adobe, AWS, Deloitte, Google Services, Hire-Vue, IBM, Microsoft Azure, Oracle и др.[3]

## Прохождение аккредитации, сертификации поставщиками облачных услуг

1. **Процесс аккредитации по требованиям FedRAMP**

Для того чтобы попасть на Маркетплейс поставщику облачных услуг, необходимо пройти процесс аккредитации по требованиям FedRAMP. Аккредитация заклю-

**NB!** Для выбора поставщика облачных услуг государственный орган может воспользоваться Маркетплейсом FedRAMP, где уже содержится перечень поставщиков облачных услуг, аккредитованных по стандартам безопасности FedRAMP.

1 https://www.cloud.mil/milcloud-20/

2 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Marketplace_Designations_for_Cloud_Service_Providers.pdf

3 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Marketplace_Designations_for_Cloud_Service_Providers.pdf

чается в **оценке соответствия поставщика облачных услуг стандартам в области безопасности информационных систем,** например, требованиям идентификации и аутентификации, интероперабельности, альтернативного хранения информации, аудита и др. Процесс аккредитации включает в себя три стадии[1]:

- **готов к аккредитации**

Статус «готов к аккредитации» присваивается тем поставщикам облачных услуг, в отношении которых уполномоченная FedRAMP сторонняя организация по оценке подтверждает, что поставщик обладает необходимыми механизмами для обеспечения безопасности данных при предоставлении своих услуг, а также тем, в отношении которых был рассмотрен и признан приемлемым органом управления программой FedRAMP Отчет об оценке готовности.

То есть, статус «готов к аккредитации» поставщикам присваивается сторонней организацией, уполномоченной FedRAMP. Поскольку аккредитация в FedRAMP основывается на оценке рисков безопасности и конфиденциальности поставщика облачных услуг, сторонняя организация по оценке ориентируется на национальные стандарты NIST, в рамках которых была выработана Структура управления рисками. Изначально выстраивая свою работу в соответствии с данной Структурой, поставщик облачных услуг повышает свои шансы на получение аккредитации FedRAMP.

- **в процессе аккредитации**

Статус «в процессе аккредитации» присваивается тем поставщикам облачных услуг, которые активно работают над авторизацией FedRAMP, либо с Объединенным советом по аккредитации (JAB) (если поставщик будет работать с правительственными данными), либо с федеральным агентством.

- **аккредитован**

Статус «аккредитован» присваивается тем поставщикам облачных услуг, которые успешно завершили процесс аккредитации FedRAMP в Объединенном совете по аккредитации (JAB) или в федеральном агентстве.

По окончании процесса аккредитации FedRAMP компаниям выдается **временное разрешение на эксплуатацию** (Provisional Authority to Operate, P-ATO) на уровне умеренного воздействия от Объединенного совета по авторизации FedRAMP (Joint Authorization Board, JAB), который оценивает системы безопасности и соответствие требованиям[2].

P-ATO не выдается организациям, проходившим процесс аккредитации FedRAMP под руководством госоргана, который планирует закупать их услуги. Вместо этого при получении статуса «аккредитован» компании получают разрешение на эксплуатацию (Authority to Operate, ATO).

P-ATO выдается для облачных сервисов, которые будут содержать любые правительственные данные. Например, Cloud.gov имеет разрешение умеренного уровня, что означает, что это проверенный и надежный сервис для данных, где последствия их потери ограничены или серьезны, но не катастрофичны. P-ATO требует ежегодных проверок и мониторинга со стороны FedRAMP.

**Уровни воздействия** определяются стандартом FIPS PUB 199 «Стандарты категоризации безопасности федеральной информации и информационных систем», входящим в систему публикаций Федеральных стандартов обработки информации (Federal Information Processing Standards Publications, FIPS Publications), разработанных Национальным институтом стандартов и техно-

1 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Marketplace_Designations_for_Cloud_Service_Providers.pdf

2 https://cloud.gov/docs/overview/fedramp-tracker/

логий (NIST) и Министерством торговли США[1]. Стандарт определяет три уровня потенциального воздействия на организации или отдельных лиц в случае нарушения безопасности данных:

- **низкий уровень** – потеря конфиденциальности, целостности или доступности данных может оказать **ограниченное** неблагоприятное воздействие на деятельность организации, активы организации или отдельных лиц;

- **умеренный (средний) уровень** – потеря конфиденциальности, целостности или доступности данных может оказать **серьезное** неблагоприятное воздействие на деятельность организации, активы организации или отдельных лиц;

- **высокий уровень** – потеря конфиденциальности, целостности или доступности данных окажет **серьезное или катастрофическое неблагоприятное воздействие** на деятельность организации, активы организации или отдельных лиц.

Также FedRAMP отдельно выделяет категорию облачных услуг **с низким уровнем потенциального воздействия** – программное обеспечение как услуга с низким уровнем потенциального воздействия (Low-Impact SaaS, LI-SaaS)[2]. Данная категория включает в себя приложения, которые не хранят личную информацию помимо той, которая обычно требуется для входа в систему (например, имя пользователя, пароль и адрес электронной почты). FedRAMP Tailored – это перечень требований, предъявляемых к LI-SaaS, который соответствует стандарту NIST SP 800-37 «Структура управления рисками информационных систем и организаций», на который опирается FedRAMP при аккредитации поставщиков облачных услуг[3].

FedRAMP Tailored содержит критерии, которые позволяют госорганам самостоятельно одобрять определенные типы облачных услуг с учетом потребностей госоргана или его конкретных задач. Так как в рамках **FedRAMP Tailored не осуществляется хранение персональной информации**, происходит **упрощенная аккредитация**, что сокращает время и средства для получения аккредитации FedRAMP для систем с низким уровнем воздействия, при этом сохраняется соблюдение законодательства в данной области.

### 1. Структура управления рисками

Структура управления рисками (Risk Management Framework) – это руководство, стандарт и процесс **управления рисками федерального правительства** США, разработанные Национальным институтом стандартов и технологий (NIST) для защиты информационных систем (компьютеров и сетей). Структура управления рисками (RMF) позволяет интегрировать требования информационной безопасности, конфиденциальности и управления рисками в жизненный цикл облачной системы на всех ее этапах: от разработки до развертывания и работы системы.

**RMF включает 7 шагов:**

1. подготовка к управлению рисками безопасности и конфиденциальности;
2. категоризация рисков, определение неблагоприятного воздействия при потере конфиденциальности, целостности и доступности систем и информации, обрабатываемой, хранимой и передаваемой этими системами;
3. выбор и применение средств контроля для защиты системы (на основании стандарта NIST SP 800-53);
4. включение элементов управления в планы безопасности и конфиденциальности;
5. оценка правильности реализации элементов управления относительно требований безопасности и конфиденциальности;

1 https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf#page=6

2 https://tailored.fedramp.gov/policy/

3 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

6. оценка приемлемости имеющихся рисков безопасности и конфиденциальности;
7. поддержание постоянной осведомленности о состоянии безопасности и конфиденциальности для управления рисками.

## 2. Стандарты сертификации ЦОД

Вместе с тем на рынке ЦОД США применяются **независимые добровольные стандарты сертификации.** Так, в США были разработаны и стали популярны во всем мире стандарты сертификации ЦОД «Tier Standards» от института инжиниринговой сертификации Uptime Institute (с 1993 г.)[1].

Стандарты Tier позволяют сертифицировать уровень производительности ЦОД независимо от используемых технологий и брендов поставщиков оборудования. Получение сертификата означает подтверждение устойчивости ЦОД на протяжении всего его жизненного цикла.

**Стандарты делятся на 4 уровня:**

**Tier 1** – с производительностью 99.671% (это значит, что время функционального простоя в год составляет 29 часов в год);

**Tier 2** – 99.741% (23 часа в год);

**Tier 3** – 99.982% (95 минут);

**Tier 4** – 99.995% (26 минут).

Количество минут простоя означает максимальное количество времени, которое может потребоваться для приведения системы в порядок после какого-либо технического сбоя.

Стандарты Tier свидетельствуют о безопасности обработки данных в ЦОД. Таким образом облачные провайдеры в США определяют стандарты безопасности, которым они готовы соответствовать в зависимости от адресата облачных услуг:

- если ЦОД ориентированы на коммерческое обслуживание частного сектора, то проходят сертификацию по наиболее востребованным стандартам, как Tier;
- если облачный провайдер намерен поставлять услуги ЦОД государственным органам, то он может присоединиться к FedRAMP Marketplace и соблюсти соответствующие требования.

Противоречий между стандартами и требованиями безопасности не возникает.

Следует отметить, что стандарты Tier являются международно-признанными стандартами, по ним выдано более 2500 сертификатов для ЦОД в 98 странах. По стандартам Tier сертифицированы ЦОД таких компаний, как Huawei (Китай), Schneider Electric (Германия), Verizon (США), из России – МТС, Мегафон, Транснефть (Backup Data Center) и др. При этом на данный момент в России аналогичный стандарт сертификации ЦОД не разработан.

### Стандарты безопасности услуг облачных поставщиков, аудита и страхования услуг

Стандарты информационной безопасности государственных информационных систем заложены в Федеральный закон об управлении информационной безопасностью от 2002 г. (FISMA, 44 USC § 3541), который требует, чтобы каждое федеральное агентство создавало программу по обеспечению информационной безопасности своих информационных систем, в том числе при получении услуг от частных подрядчиков.

1 https://uptimeinstitute.com/tiers

Ответственность за разработку стандартов безопасности была возложена на **Национальный институт стандартов и технологий** (NIST)[1].

Во исполнение Закона для развития стандартов безопасности облачных систем была принята **Федеральная программа управления рисками и авторизацией** (FedRAMP)[2]. NIST разрабатывает стандарты и рекомендации в рамках программы FedRAMP **для обеспечения стандартизированных требований безопасности для облачных сервисов**, программ оценки соответствия, стандартизированных пакетов авторизации и языка договора, репозиториев пакетов авторизации и пр.

Для государственных учреждений США существует ряд требований и стандартов, которым должны соответствовать поставщики облачных услуг и их системы, при этом такие требования могут варьироваться от учреждения к учреждению. Так, среди общих требований для всех федеральных органов можно выделить следующие:

- **стандарт NIST SP 800-145** «Определение понятия облачных вычислений», созданный в 2011 г., закладывает основу для развития облачных технологий и технических требований к облачным услугам, а также рассматривает наилучшие способы их применения[3];

- аккредитация в FedRAMP, осуществляемая на основе **стандартов NIST SP 800-53** и **NIST SP 800-37**.

Стандарт **NIST SP 800-53 «Средства управления безопасностью и конфиденциальностью для информационных систем и организаций»[4]** – это обязательный стандарт, который устанавливает категории безопасности информационных систем, конфиденциальности, целостности и доступности, например, в случае подключения к системам с мобильных устройств; содержит требования к тестированию, настройкам конфигурации, системам альтернативного хранения информации и пр.[5]. Также устанавливаются требования к аудиту облачных систем, среди которых наличие политики аудита и подотчетности в компании, требования к данным аудиторских записей, к объему хранилища журнала аудита, к безопасности информации аудита и др.

Стандарт **NIST SP 800-37 «Структура управления рисками для информационных систем и организаций: подход к жизненному циклу системы для обеспечения безопасности и конфиденциальности»** применяется в отношении федеральных информационных систем, которые представляют собой дискретные наборы информационных ресурсов, организованных для сбора, обработки, обслуживания, использования, совместного использования, распространения или распоряжения информацией независимо от того, находится ли такая информация в цифровой или нецифровой форме[6]. Стандарт включает требования к категоризации информационной безопасности, контролю отбора, реализации и оценки, системным и общим разрешениям на управление, требования к постоянному мониторингу и пр.;

- **федеральный стандарт обработки информации FIPS PUB 140-2** – это стандарт правительства США, определяющий минимальные требования к безопасности криптографических модулей в продуктах информационных технологий[7];

- **стандарт NIST SP 800-161** «Практики управления рисками цепочки поставок для федеральных информационных систем и организаций» содержит рекомендации для федераль-

1 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
2 https://www.fedramp.gov/program-basics/
3 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
4 https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1
5 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
6 https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
7 https://csrc.nist.gov/Projects/cryptographic-module-validation-program

ных агентств по выявлению, оценке и смягчению рисков цепочки поставок ИКТ в их организациях[1]. Процессы и элементы управления, описанные в стандарте, основаны на указаниях FedRAMP;

- **стандарт NIST SP 800-171** направлен на защиту контролируемых неклассифицированных сведений в нефедеральных информационных системах и организациях[2]. Требования безопасности предназначены для применения федеральными агентствами в контрактах или других соглашениях, заключенных между этими агентствами и нефедеральными организациями (в том числе поставщиками облачных услуг);

- **стандарт NIST SP 800-63** «Руководство по цифровой идентификации» содержит технические требования к цифровой идентификации, включая проверку личности и аутентификацию пользователей, взаимодействующих с государственными ИТ-системами по открытым сетям[3];

- **стандарт NIST SP 800-207** «Архитектура нулевого доверия» содержит принципы нулевого доверия, основы внедрения нулевого доверия в организациях и объясняет необходимость такой системы для обеспечения кибербезопасности[4].

В мае 2021 г. был издан Исполнительный указ об улучшении национальной кибербезопасности для поддержки и защиты критической инфраструктуры и сетей Федерального правительства[5]. Планируется переход Федерального правительства к безопасным облачным сервисам и концепции «нулевого доверия» (Zero Trust), **независимые добровольные стандарты сертификации** и **шифрования** за счет внедрения **базовых стандартов безопасности** для разработки программного обеспечения, продаваемого правительству, включая требования для разработчиков обеспечивать прозрачность данных о программном обеспечении и общедоступность данных о безопасности.

Ввиду этого Агентство по кибербезопасности и безопасности инфраструктуры (CISA) разработало Модель зрелости нулевого доверия (Zero Trust Maturity Model)[6] – дорожную карту для перехода к архитектуре с нулевым доверием.

Например, если ранее государственное агентство проверяло подлинность личности с помощью паролей или многофакторной аутентификации, то теперь агентство будет внедрять системы постоянной проверки личности, а не только при первоначальном предоставлении доступа. Если ранее агентство определяло риски идентификации на основе простой аналитики и статических правил, то теперь агентство должно анализировать поведение пользователей в режиме онлайн с помощью алгоритмов машинного обучения для определения рисков и обеспечения постоянной защиты. Или, например, если ранее некоторые критически важные облачные приложения были доступны пользователям напрямую через Интернет, а все остальные приложения были доступны через виртуальную частную сеть (VPN), то теперь все облачные приложения будут доступны пользователям напрямую через Интернет.

Кроме того, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) совместно с Цифровой службой США (USDS) и FedRAMP разработало **Техническую эталонную архитектуру облачной безопасности** (Cloud Security Technical Reference Architecture (TRA))[7] с рекомен-

1 https://csrc.nist.gov/publications/detail/sp/800-161/final

2 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

3 ttps://pages.nist.gov/800-63-3/sp800-63-3.html

4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

5 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

6 https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

7 https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20

дациями по миграции федеральных информационных систем в облако и защите данных, включая обозначение рисков внедрения облачных сервисов по мере того, как агентства переходят к архитектуре с нулевым доверием.

Например, агентствам рекомендовано развертывать интегрированную систему безопасности централизованно по всей организации с целью снижения риска кибератак; разработать и поддерживать планы реагирования на инциденты кибербезопасности и восстановления после них, поскольку такие планы играют ключевую роль в смягчении последствий кибератак, обеспечивают непрерывность работы и сохранение доказательств для последующего криминалистического анализа.

**Важным вопросом обеспечения безопасности является разделение ответственности между поставщиком облачных услуг и пользователем (государственным органом).**

Например, **AWS** использует Модель общей ответственности (Shared Responsibility Model)[1]. Безопасность и соответствие требованиям являются обязанностью и поставщика, и заказчика. AWS отвечает за защиту инфраструктуры, на которой работают все сервисы, предлагаемые в облаке AWS. Заказчик может отвечать за ПО, свои данные, операционную систему и другие аспекты в зависимости от набора услуг, который он приобретает у поставщика. Такое разграничение ответственности называют безопасностью «вне» облака и безопасностью «в» облаке (Security «of» the Cloud versus Security «in» the Cloud).

**Cloud.gov** также имеет собственную политику разграничения ответственности с заказчиком[2]. Как платформа как услуга (PaaS) cloud.gov отвечает за обслуживание и безопасность платформы cloud.gov. Заказчик несет ответственность за обслуживание и безопасность своего пользовательского кода.

**Oracle** также применяет Shared Security Model для разграничения ответственности в отношении процессов, касающихся облака[3]: Oracle обеспечивает безопасность облачной инфраструктуры и операций, а заказчик несет ответственность за безопасную настройку своих облачных ресурсов. В мультиоблачной среде Oracle отвечает за безопасность базовой облачной инфраструктуры (например, объектов ЦОД), а заказчик отвечает за защиту своих рабочих нагрузок и настройку своих сервисов сети, хранилища и базы данных.

**Google Cloud** имеет модель распределения ответственности, построенную на принципе количества рабочих нагрузок – чем больше услуг закупается у Google, тем больше ответственность компании[4].

Что касается вопросов **страхования**, в США на государственном уровне не установлены требования к страхованию услуг облачных систем. Для поставщиков существует возможность **добровольного страхования ответственности** в отношении рисков, связанных с деятельностью в киберпространстве (cyber liability insurance)[5].

### Управление персональными данными при создании государственных облаков

В США нет единого закона, регулирующего конфиденциальность всех типов персональных данных. Действуют законы, регулирующие отдельные сферы, например данные о кредитной задолженности, о здоровье, образовании детей и др.

---

Architecture_Version%201.pdf

1 https://aws.amazon.com/compliance/shared-responsibility-model/

2 https://cloud.gov/docs/technology/responsibilities/

3 https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm

4 https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke

5 https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/

При этом в США действует **Закон о конфиденциальности 1974 г.** (Privacy Act of 1974), который устанавливает кодекс добросовестной информационной практики, регулирующий сбор, хранение, использование и распространение информации о физических лицах, которая хранится в системах записей федеральных агентств[1]. Система записей – это группа записей, находящихся под контролем агентства, из которых информация извлекается по имени физического лица или по какому-либо идентификатору, присвоенному физическому лицу.

Закон о конфиденциальности требует, чтобы агентства публично уведомляли о своих системах записей путем публикации в Федеральном реестре. Закон о конфиденциальности запрещает раскрытие записи о лице из системы записей без письменного согласия лица, за исключением случаев, когда раскрытие осуществляется в соответствии с одним из двенадцати установленных законом исключений. Закон предоставляет физическим лицам средства для получения доступа к своим записям и внесения в них поправок, а также устанавливает различные требования агентств к ведению записей.

Советом Уполномоченных по информационным технологиям были разработаны **Рекомендации по обеспечению конфиденциальности при использовании облачных вычислений федеральными органами власти**[2].

Согласно рекомендациям, **госорган является ответственным за обеспечение конфиденциальности данных** в соответствии с Законом о конфиденциальности 1974 г. и обязан исследовать практику защиты данных поставщика облачных услуг. Также настоятельно рекомендуется выработать специальные положения о защите данных в случае работы с персональными данными для контракта между поставщиком и госорганом, поскольку стандартные соглашения об условиях обслуживания имеют тенденцию не во всем соответствовать Закону о конфиденциальности 1974 г.

Таким образом, госорганы США, использующие облачные технологии в том числе для работы с данными физических лиц, попадают под действие Закона о конфиденциальности, ввиду чего им необходимо обеспечить тот уровень защиты, который бы свел к минимуму риск утечки персональных данных.

### Формирование ценообразования при осуществлении государственных закупок облачных услуг

В рекомендациях по ценообразованию Cloud Information Center указывается, что поскольку облако представляет собой услуги, а не готовый продукт, возникают сложности со сравнением предложений поставщиков[3]. Государственным органам рекомендуется использовать коммерческую и общедоступную информацию о ценах, чтобы сформулировать собственное предложение. Как правило, государственные цены должны быть меньше или равны самой низкой коммерческой цене. В целом можно использовать следующие типы ценообразования в контрактах:

1. **Модель времени и материалов (Time & Materials)** – плата варьируется от счета к счету в течение периода предоставления услуг. Для сравнения предложений поставщиков предлагается умножать или делить на 60, если один поставщик облачных услуг взимает плату за час, а другой за минуту.

При этом государственным органам придется включать в контракты предельные значения, которые нельзя превышать (Not To Exceed), – максимальные затраты, которые госорган может понести в отношении конкретной услуги или группы связанных услуг.

1 https://osc.gov/Pages/Privacy-Act.aspx#:~:text=The%20Privacy%20Act%20of%201974%20is%20a%20federal%20law%20that,in%20a%20system%20of%20records.&text=the%20right%20to%20be%20protected,disclosure%20of%20their%20personal%20information.

2 https://www.steptoe.com/images/content/2/4/v1/2487/4128.pdf

3 https://cic.gsa.gov/acquisitions/pricing

2. **Модель твердой фиксированной цены (Firm Fixed Price)** – оценивается количество единиц (например, пользователей), которые госоргану понадобятся для определенного периода работы.

Возможно также **сочетание этих двух методов ценообразования**. Например, некоторые государственные органы США закупают часть услуг с учетом предсказуемых ежегодных вычислительных потребностей по модели твердой фиксированной цены, а еще часть по модели времени и материалов, чтобы сэкономить средства, если потребность в услугах окажется меньше, чем предполагалось.

Как показывает практика, государственные учреждения в США осуществляют закупки с фиксированной ценой контракта. Например, в рамках облачного контракта JEDI Министерство обороны проводило открытый конкурс, в результате которого должен был быть заключен контракт с твердой фиксированной ценой на коммерческие товары (например, облачную инфраструктуру и вычислительные услуги). С последующим контрактом JWCC Министерство продолжает придерживаться политики твердой фиксированной цены[1].

Контракт с твердой фиксированной ценой также заключило ЦРУ[2]. Контракт Министерства внутренней безопасности имеет фиксированную стоимость в размере 3,4 млрд долл. США, при этом для реализации проекта привлекается сразу несколько поставщиков облачных услуг[3].

Сами поставщики облачных услуг применяют в том числе стратегию «pay-as-you-go» – оплата услуг в зависимости от их использования. Например, Google Cloud[4] и AWS[5] включают данный в принцип в собственную систему ценообразования на услуги придерживается этой же стратегии.

# 3. Опыт Европейского союза

*«Облако с безопасным гибридным мультиоблачным предоставлением услуг»*
(Облачная стратегия ЕС до 2022 г.)

В ЕС **не рассматривается концепция создания единого европейского облака**, которое бы объединяло публичные службы всех стран-членов ЕС и обеспечивало публичные услуги гражданам ЕС. Это обусловлено тем, что государства-члены ЕС намерены сохранять суверенный контроль в отношении данных (*data sovereignty*)[6].

Вместе с тем страны ЕС стремятся создать единый европейский цифровой рынок (single data market), поэтому в ЕС принимают инициативы в области облачных технологий для публичного сектора[7].

1 https://federalnewsnetwork.com/defense-main/2021/12/in-jwcc-cloud-procurement-pentagon-plans-a-novel-approach-to-competition/

2 https://www.nextgov.com/it-modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227/

3 https://washingtontechnology.com/2021/02/dhs-makes-tweaks-to-34b-cloud-contract/359448/

4 https://cloud.google.com/pricing

5 https://aws.amazon.com/pricing/

6 Data sovereignty понимается как способность управляющих институтов юрисдикции действовать независимо в цифровой экономике, включая использование защитных механизмов и механизмов стимулирования цифровых инноваций (само понятие появилось в политическом дискурсе как концепция противопоставленная влиянию компаний GAFA (Google, Amazon, Facebook, Apple).

7 https://www.cloudflight.io/expert-views/public-cloud-public-sector-a-european-trust-challenge-46031/

## Стратегические документы, устанавливающие меры по переходу на облачные технологии

**NB!** В 2019 г. Еврокомиссия опубликовала Облачную стратегию до 2022 года . Стратегия устанавливает принципы предоставления облачных услуг:

- **безопасность**: принцип управления рисками, обеспечения безопасности данных;
- использование **гибридных облаков**: использование услуг поставщиков публичных облачных сервисов и частного облака, управляемого Еврокомиссией;
- **мультиоблачность** за счет вовлечения Еврокомиссией разных поставщиков облачных услуг в зависимости от запрашиваемой услуги;
- **энергоэффективность**: снижение выбросов углекислого газа и политика зеленых государственных закупок.

Облачная стратегия до 2022 г. содержит видение ЕС по развитию облачных технологий в странах ЕС как для частного, так и для публичного секторов. В стратегии излагаются основные пункты:

- по **миграции информационных систем в облако** (включая перенос существующих информационных систем в облако, перестраивание компонентов систем под облачные технологии, замену информационных систем на приложения Saas и пр.);
- по **внедрению цифровых решений** (digital solutions) (например, Комиссия планирует не только использовать Saas-сервисы, но и проводить разработки в облаках для конкретных политик, для этого необходимо внедрение стандартов DevSecOps по автоматизации интеграции задач безопасности на всех этапах жизненного цикла разработки ПО, включая проектирование, интеграцию, тестирование, развертывание ПО и пр.);
- по распространению практики применения в ЕС цифровых облачных **решений многократного пользования** (reusable digital solutions). Так, в ЕС уже применяются такие «ИТ-решения многократного пользования», как Commission Notification System (система автоматических уведомлений европейских и национальных органов по стандартизации); структурные компоненты европейской информационной системы Connecting Europe Facility, как EU Login (сервис аутентификации для получения доступа к онлайн-услугам Еврокомиссии для граждан ЕС);
- по **созданию европейской экосистемы данных** (data ecosystem), которая позволяет предоставлять данные как услугу (DaaS) через платформу данных;
- по **развитию гибридных облачных систем** (cloud on premise), которые сочетают в себе преимущества облачных систем (развертывание программ на удаленном сервере) и преимущества систем, устанавливаемых локально (on premise). Такие гибридные решения представляются наиболее надежными и стабильными при сохранении таких свойств облачных решений, как удаленный доступ, масштабируемость и др.;
- по вопросам **безопасности облачных систем** (внедрение средств контроля и инфраструктур безопасности; мониторинга безопасности, обнаружения инцидентов и реагирования; поддержка процессов DevSecOps за счет автоматизированной оценки безопасности, сканирования уязвимостей, аудита кода и пр.);
- по вопросам **закупок облачных сервисов**; по управлению облачными рисками благодаря платформе GovSec Cloud.

Итак, центральными компонентами облачной системы ЕС являются:

1. **GovSec Cloud**

В 2018 г. Еврокомиссией инициировано создание GovSec Cloud, европейской платформы по управлению рисками информационной безопасности. GovSec Cloud – **это инструмент** в виде базы данных (реестра), который **содержит информацию** о рисках использования облачных систем. Поставщики и пользователи систем могут использовать реестр рисков для анализа собственных рисков, что позволяет разрабатывать решения для избежания и предотвращения таких рисков. Платформа GovSEC построена на основе методологии управления рисками ИТ-безопасности ITSRM2 (по стандарту ISO/IEC 27005).

**Пять основных задач платформы**:

- оценка ИТ-рисков облачных услуг и определение необходимых мер;
- помощь в разработке индивидуальных планов безопасности;
- стандартизация подходов к безопасности;
- предоставление чек-листа технических элементов управления;
- обеспечение аудиторов средствами контроля.

**Платформа включает три модуля**:

1. **модуль оценки рисков** (risk assessment module) – каталог мер управления специфическими облачными рисками, как привязка к единому поставщику, потеря управления, сбой интерфейса управления, небезопасное или неэффективное удаление данных, сбой механизма обслуживания и др.;

2. **модуль принятия решений и управления** (decision making and governance module) - задает методологию для принятия решений о вариантах хостинга, классификации бизнес-данных и определения на бизнес-уровне, где и как следует управлять этими данными;

3. **модуль плана безопасности** (security plan module) – модуль включает методологию по реагированию на киберугрозы.

Таким образом, платформа обеспечивает владельцев облачных систем инструментами для решения рисков, связанных с изменением юрисдикции, проблем защиты данных, подотчетностью и владением данных, конфиденциальностью пользователей и вторичным использованием данных.

2. **Развитие системы закупок**

Обеспечение закупки облачных систем и сервисов входит в компетенцию Генерального директората по информационным технологиям (Directorate-General for Informatics, DIGIT) – интер-институциональный облачный брокер[1].

DIGIT разрабатывает **общий рамочный контракт для облачных услуг** (Framework contract for Cloud services), обеспечивает динамическую систему закупок (электронную систему закупок, к которой поставщик может присоединиться в любое время, что обеспечивает покупателю доступ к пулу предварительно одобренных поставщиков), следит за соблюдением принципов безопасности и защиты данных, энергоэффективности при закупках, применением кодексов саморегулирования.

Также DIGIT предоставляет заинтересованным сторонам в Европейской комиссии **рекомендации по архитектуре облачных решений** (включая разработку шаблонов, руководящих принципов, методов и услуг по анализу архитектуры, направленных на повышение безопасности и снижение затрат на эксплуатацию), по архитектуре данных, требованиям к безопасности.

1 https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

3. **Развитие облачных решений всех уровней (IaaS, PaaS, SaaS + BaaS (business as a service), XaaS (everything as a service)**

В этом отношении меры гармонизации, стандартизации и регулирования облачных систем позволяют реализовать проект цифрового рабочего места (Digital Workplace Program) для оптимизации рабочего процесса всех европейских предприятий и их сотрудников. Проект адресован предприятиям и институтам во всех направлениях. Программа «Цифровое рабочее место» основана на гибридной инфраструктуре, сочетающей локальные и онлайн-сервисы (облачные).

В октябре 2020 г. принята Декларация государств-членов ЕС по созданию нового поколения облачных сервисов для бизнеса и публичного сектора[1], в рамках которой учрежден **Европейский Альянс по промышленным данным, прорывным технологиям и облачным сервисам** (European Alliance for Industrial Data, Edge and Cloud).

Одна из функций Альянса – разработка **рекомендаций по гармонизированной имплементации облачных технологий** и созданию интероперабельных пространств данных[2]. Цель Альянса – увеличить долю европейских компаний, использующих облачные технологии[3] до 70% к 2020 г.[4]

Еврокомиссией принимаются шаги содействия диверсификации проектов облачной инфраструктуры, поэтому в ЕС реализуется **проект High Impact Project on European data spaces and federated cloud infrastructures**. Проект проводится до 2027 г. и направлен на материальную и техническую поддержку единых европейских пространств данных и взаимосвязанной облачной инфраструктуры. В рамках данного проекта Еврокомиссия намерена финансировать инфраструктуру, инструменты обмена данными, архитектуры и механизмы управления для успешного обмена данными и экосистем искусственного интеллекта[5].

### Проекты по созданию облаков

Несмотря на то, что в ЕС **нет единой публичной облачной системы**, там создаются облачные системы по отдельным направлениям и отраслям.

Например, **European Open Science Cloud (EOSC)**[6] – облачная система обмена научными данными, запущенная в 2018 г. по инициативе Европейской Комиссии (работает на уровне PaaS). EOSC включена в Стратегию по данным как **платформа для объединения данных европейских программ исследований** и обеспечения межотраслевого обмена данными. Проект должен сокращать материальный эквивалент издержек, связанных с ограниченным доступом к научным данным, учитывая, что в среднем ежегодно страны ЕС в совокупности тратят около 10 лрд евро на инфраструктуру данных в научных центрах и университетах[7].

**EOSC организована как мультиоблачная система**. Портал публично приглашает к участию облачных провайдеров, соответствующих нескольким **техническим условиям**[8]:

- облачные сервисы доступны для пользователей за пределами одной юрисдикции
- услуга предоставляется с помощью общего алгоритма (шаблона)

1 https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance
2 https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance
3 https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance
4 https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance
5 https://www.euractiv.com/section/digital/news/leak-commission-outlines-plan-to-create-single-eu-data-space-by-2030/
6 https://digital-strategy.ec.europa.eu/en/policies/open-science-cloud
7 https://sciencebusiness.net/system/files/reports/Who-pays-what-European-Open-Science-Cloud-.pdf
8 https://eosc-portal.eu/for-providers

- публикуемые данные могут быть найдены по поисковому запросу, данные доступны пользователям системы; данные представлены в интероперабельном формате; данные могут повторно использоваться
- сервисами предусмотрены службы поддержки, службы приема сообщений об ошибках

Таким образом, система поддерживает участие множества облачных провайдеров, устанавливая низкие пороги доступа к пользовательскому рынку в виде минимальных технических требований.

Отметим, что Еврокомиссия поддерживает реализацию национальных инициатив на общеевропейском уровне – как, например, **проект Gaia-X**[1]. Инициатива GAIA-X направлена на создание в Европе единой инфраструктуры данных: безопасной, федеративной и децентрализованной облачной системы на уровне PaaS.

Инициатива основана на идее платформы открытых данных (open-source). В рамках проекта GAIA-X разработаются **общие требования к европейской инфраструктуре данных** с правилами безопасного обмена данными для бесшовного обеспечения облачных сервисов среди различных облачных.

### Мультиоблачный подход (multicloud) к получению облачных услуг

Все облачные проекты, запускаемые в ЕС, разрабатываются как мультиоблачные и доступны для присоединения новых облачных провайдеров при соответствии техническим условиям. При этом ограничений по юрисдикции поставок облачных услуг нет. Отметим, что **68% рынка** облачных услуг в Европе приходится на **Amazon** Web Services, **Microsoft** Azure, Google Cloud. Поэтому содействуя мультиоблачному подходу ЕС прежде всего поддерживает диверсификацию поставщиков и участие европейских компаний.

Для реализации мультиоблачного подхода Еврокомиссия поддерживает проект Европейского маркетплейса облачных сервисов (**European cloud services marketplace**). Проект предложен Еврокомиссией в рамках стратегии ЕС по данным.

Цель проекта – помочь публичным институтам выбирать облачное программное обеспечение и предложения платформ, которые уже соответствуют требованиям ЕС. Рынок должен быть единой точкой доступа для облачных и гибридных сервисов и иных ПО. Маркетплейс должен дополнять платформу AI-on-demand. Маркетплейс может предоставлять брокерские услуги для транзакций и предоставления облачных инфраструктур и услуг государственного сектора.

**NB!** Европейская комиссия выбирает мультиоблачный подход без привязки к одному поставщику публичных облаков. Принципы мультиоблачного подхода:

- получение услуги от поставщика облачных услуг, который лучше всего подходит для требуемой услуги;
- облачная платформа с типовыми облачными сервисами делает открытой возможность присоединения облачных провайдеров (как, например, на платформе EOSC).

### Прохождение аккредитации, сертификации поставщиками облачных услуг

Если говорить о публичном регулировании облачных систем в части безопасности, то облачные системы в ЕС подлежат соблюдению положений **Акта по кибербезопасности** от Европейского агентства по кибербезопасности (EU Cybersecurity Act – Регламент 2019/881).

1 https://www.ifri.org/sites/default/files/atoms/files/pannier_european_cloud_computing_2021.pdf

Регламент задает и устанавливает основные горизонтальные требования для разработки европейских **схем сертификации кибербезопасности**; позволяет признавать и использовать европейские сертификаты кибербезопасности и заявления о соответствии ЕС для продуктов ИКТ, услуг ИКТ или процессов ИКТ во всех государствах-членах. Регламент предлагает основы для добровольных схем сертификации.

Сегодня в Европе большинство компаний проходят сертификацию облачных технологий по стандарту **ISO/IEC 27001**. Данный стандарт считается de facto **обязательным** и уже дополнительные сертификации могут давать конкурентные преимущества. Но в ЕС разрабатываются отдельные стандарты безопасности облачных технологий.

Так, в ЕС действует общеевропейский транснациональный стандарт **EN 50600**, который содержит спецификации для планирования, строительства и эксплуатации центров обработки данных[1]. Стандарт разработан Европейской организацией по стандартизации CENELEC (Европейский комитет по электротехнической стандартизации). Стандарт определяет требования для строительства, электроснабжения, кондиционирования воздуха, прокладки кабелей, систем безопасности и определяет критерии эксплуатации центров обработки данных. Стандарт является модульной системой и допускает свободу выбора решений компаниями.

Отличие стандарта EN 50600 от стандарта ISO/IEC 27001 заключается в том, что, требования стандарта EN 50600 сосредоточены на физической безопасности, тогда как стандарты ISO ориентированы на организационный уровень и уровень процессов. Стандарт EN 50600 в первую очередь разработан не как метод оценки, а как руководство. Поэтому для применения стандарта для сертификации возможно только при разработке соответствующего каталога критериев, соответствие которым можно проверить.

Сейчас среди европейских облачных провайдеров популярен каталог критериев оценки **TSI. STANDARD** (в разработке TÜViT)[2].

В ЕС готовится проект **Схемы облачной сертификации по информационной безопасности** (European Union Cybersecurity Certification Scheme on Cloud Services (EUCS)[3]. По проекту схема является **добровольной**; сертификаты схемы применяются во всех государствах-членах ЕС; сертификация для всех уровней облачных сервисов; сертификация охватывает три уровня гарантий: «Базовый», «Существенный» и «Высокий»; сертификация на 3 года может быть продлена[4].

Примечательно, что схема построена на **презумпции разграничения зон ответственности облачного провайдера и потребителя облачных услуг**, и соответственно, ставит в приоритет такие требования прозрачности, как место обработки и хранения данных для обеспечения возможности принятия информированных решений[5].

### Стандарты безопасности услуг облачных поставщиков, аудита и страхования услуг

Для государственных облачных систем разрабатываются стандарты Европейского агентства по кибербезопасности (ENISA), включая Руководство ENISA по лучшим практикам для публичных облаков 2013 г.; Основы по безопасности публичных облаков 2014 г.

Например, **Руководство по лучшим практикам** включает рекомендации по составлению политики нивелирования проблемы «утраты контроля» над данными в облачных системах; политики по решению проблемы соблюдения требований локализации видов данных в юрисдикциях;

1 https://www.tuvit.de/en/services/data-centers-colocation-cloud-infrastructures/din-en-50600/

2 https://www.techerati.com/features-hub/opinions/the-en-50600-how-to-meet-the-european-standard-for-data-centres/

3 https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme

4 https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

5 https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme стр. 9

модельного соглашения об уровне обслуживания; по определению стандартов соответствия и мер безопасности, и др.[1]

**Основы информационного обеспечения** (Information Assurance Framework ENISA) соблюдаются всеми иностранными облачными провайдерами, входящими на европейский рынок для предоставления сервисов как в частном, так и публичном сегменте[2].

Разработке стандартов в области информационной безопасности содействует **CloudWATCH2** (Европейская облачная обсерватория, поддерживающая облачные политики, стандартные профили и услуги), финансируемая Еврокомиссией из европейского фонда Horizon 2020.

Одной из основных целей CloudWATCH2 является **анализ стандартов интероперабельности и безопасности** путем мониторинга меняющегося ландшафта существующих частных стандартов, новых реализаций, расширений и протоколов с фокусом на создание ценности интероперабельных и безопасных сервисов. Практическая работа CloudWatch заключается в выявлении пробелов и предоставлении рекомендаций по их устранению.

Также в ЕС действуют **частные инициативы по вопросу контроля за информационной безопасностью**, которые поддерживаются ЕС.

Например, для обеспечения интероперабельности информационных систем, необходимой в мультиоблачных системах европейским облачным провайдерам рекомендовано имплементировать **Кодексы поведения по переносу данных и переключению на облако**, разработанных рабочей группой по переключению поставщиков облачных услуг и переносу данных (**SWIPO**)[3].

Кодексы охватывают облачные сервисы «инфраструктура как услуга» (**IaaS**) и облачные сервисы «программное обеспечение как услуга» (**SaaS**)[4]. Кодекс по переносимости данных включает рекомендации по определению таких технических мер, как обеспечение возможностей экспорта и импорта данных; обеспечение возможности передачи с использованием структурированного, широко используемого, машиночитаемого формата». **Кодексы регулируют поток неличных данных** (free flow of non-personal data)[5].

### Управление персональными данными при создании облаков

Вопросы развития облачных систем в Европе включены в **Европейскую стратегию по данным 2020 г.** (A European strategy for data)[6]. В частности, Стратегия указывает на основные проблемы развития облачных систем в ЕС[7] и на необходимость разработки единых стандартов безопасности, например, специального европейского регулирования облачных технологий (Framework for Cloud Services) в формате **«Cloud Rulebook»**, то есть сборника рекомендаций поставщикам облачных сервисов[8]. В 2021 г. разработка Cloud Rulebook была поручена Европейскому Альянсу по промышленным данным и облакам.

---

1 https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

2 https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-eu-enisa-iaf?toc=/compliance/regulatory/toc.json&bc=/compliance/regulatory/breadcrumb/toc.json

3 https://swipo.eu/

4 https://swipo.eu/news/swipo-codes-published/

5 https://digital-strategy.ec.europa.eu/en/news/presentation-codes-conduct-cloud-switching-and-data-portability

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066

7 В качестве основных препятствий для развития европейских облачных систем отмечаются риски для европейских данных, когда иностранные провайдеры подчиненны иностранному законодательству и использование данных иностранными провайдерами для публичных целей своих стран.

8 https://www.lexology.com/library/detail.aspx?g=9ab4ac31-ba5c-4c0e-8be6-1ee36db3c64e

На данный момент в части управления данными облачные системы в ЕС подпадают под общее европейское регулирование данных – **Регламент о защите персональных данных** (GDPR), **Регламент о потоках неперсональных данных** (Free Flow of non-personal Data Regulation).

Во исполнение ст. 28.5 Регламента по защите персональных данных 2016/679 в ЕС при поддержке Еврокомиссии с участием европейских компаний и профильных НКО был разработан **Кодекс поведения для поставщиков облачных сервисов** (EU Cloud Code of Conduct, ECOC)[1]. Кодекс поведения ECOC состоит из требований к поставщикам облачных сервисов и рекомендаций для поддержки эффективного и прозрачного внедрения, управления и развития Кодекса. Кодекс является добровольным инструментом, компании демонстрируют соблюдение требований Кодекса как посредством **самооценки** и **декларирования соответствия**, так и через сертификацию третьей стороной.

**Кодекс поведения для поставщиков облачных** включает **рекомендации**:

- для оказания услуг с помощью облачных технологий между поставщиком и пользователем обязательно должно быть заключено **Соглашение об облачных услугах** (Cloud Services Agreement), соответствующее требованиям GDPR (ст. 28.3);
- обработка данных происходит **транспарентно** и в порядке, предусмотренном законном;
- поставщик облачных услуг может привлекать в качестве **субисполнителей других обработчиков данных** (subprocessors), получив предварительное согласие пользователя (general authorization) по ст. 28.2 GDPR;
- проведение **должной осмотрительности** в отношении правового режима данных при передаче данных пользователя в третью страну за пределами юрисдикции ЕС с учетом требований ст. 45 и 46 GDPR;
- **аудит** деятельности поставщика облачных услуг учитывает обязательства по обеспечению конфиденциальности и безопасности данных; по минимизации риска разрывов в деятельности поставщика и пользователей его услуг; по обеспечению соответствия деятельности законодательным и регуляторным предписаниям; по соблюдению обязательств в соглашениях с пользователями. Аудит может проводиться по таким признанным стандартам, как ISO 27001, ISO 27001 SSAE SOC 2;
- поставщик облачных услуг должен иметь **канал взаимодействия** по защите данных пользователей (data protection point of contact). Поставщик может назначить уполномоченное лицо по защите данных;
- поставщик и пользователь признают, что основным контактом для субъектов данных выступает **контролер** данных в соответствии с GDPR. Поэтому, когда поставщик получает запрос от субъектов данных, то он может его перенаправить к пользователю;
- поставщик **добросовестно** взаимодействует с пользователем и контролирующими органами (supervisory authorities);
- поставщик **оказывает поддержку** пользователям **в случае нарушений** прав субъектов персональных данных, например, в части соблюдения обязательства уведомления о нарушении по ст. 33.1 и 34 GDPR.

Поскольку в мультиоблачной системе каждый провайдер несет ответственность только за свои облачные сервисы, требование транспарентности относится и к распределению зон ответственности. Вопросы, связанные с действиями владельца самой облачной системы, регулируются

1 https://eucoc.cloud/en/about/about-eu-cloud-coc/

между владельцем и облачными провайдерами. Хотя владелец облачной системы может участвовать в компенсации нарушенных прав пользователей облачных услуг в той мере, в которой его деятельность способствовала этому нарушению[1].

### Формирование ценообразования при осуществлении закупок облачных услуг

В ЕС нет прямого регулирования ценообразования для облачных сервисов. Тем не менее Ассоциация CISPE (Cloud Infrastructure Services Providers in Europe) представляет рекомендации по ценообразованию в Руководстве по покупке облачных сервисов в публичном секторе.

Рекомендовано определять **минимальные требования**[2]:

- **цены на услуги**: клиенты облачных сервисов должны использовать модель с оплатой по факту использования;
- **прозрачное ценообразование**: ценообразование облачного провайдера должно быть общедоступным и прозрачным;
- **динамическое ценообразование**: цены на облачные услуги могут колебаться в зависимости от рыночных цен (это нужно для поддержки облачных инноваций);
- **контролируемые расходы**: CISPE должны предоставлять инструменты отчетности, мониторинга и прогнозирования, которые позволяют клиентам;

**NB!** В отношении сравнения облачных поставщиков для закупки облачных услуг помимо использования таких критериев оценки, как лучшая стоимость, наиболее экономически выгодное предложение (most economical advantageous tender) или самая низкая цена, рекомендуется учитывать **уникальные особенности облака**, оправдывающие превышение ценовых ожиданий.

## 4. Опыт Италии

### Стратегические документы, устанавливающие меры по переходу государственных органов на облачные технологии

В Италии развитие государственных облаков началось с принятия Стратегии цифрового роста на 2014–2020 гг.[3], которая заложила **цель по развитию облачных технологий**, развитию рынка поставщиков ЦОД и пр.

На основе Стратегии цифрового роста на 2014–2020 годы был разработан **Трехлетний план развития ИТ** в области государственного управления на 2020–2022 гг.[4], который курирует Агентство по цифровизации Италии (AgID). План устанавливает **меры по миграции госорганов в безопасные ЦОД и облачные инфраструктуры** и услуги, сертифицированные AgID; по развитию процесса закупок, включая создание каталога облачных услуг для госорганов и запуск платформы поиска сертифицированных поставщиков облачных услуг (Cloud Marketplace di AgID) и пр.

1 https://eucoc.cloud/en/about/about-eu-cloud-coc/ P. 4

2 https://cispe.cloud/website_cispe/wp-content/uploads/2019/05/Public-Policy-strategy-on-Procurement-Handbook-Final-190528.pdf стр. 28

3 https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/strategia_crescita_digitale_ver_def_21062016.pdf

4 https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/index.html

В 2021 г. в рамках Стратегии цифрового роста и Трехлетнего плана была принята **Облачная стратегия государственного управления (Strategia Cloud Italia)** для внедрения модели облачных вычислений[1].

Облачная стратегия также направлена на квалификацию услуг и облачных инфраструктур в соответствии с конкретными параметрами безопасности и надежности, подходящими для нужд органов государственного управления, с соблюдением принципов повышения уровня доступности, удобства использования и безопасности облачных сервисов; интероперабельности; снижения риска «привязки к поставщику» (то есть, реализация **подхода мультиоблачности**); расширения и диверсификации рынка поставщиков, включая МСП; защиты данных.

**Облачная стратегия закладывает меры** по:

- **созданию Национальных стратегических хабов** (Polo Strategico Nazionale, PSN[2]): ИТ-инфраструктуры (централизованные или распределенные), принадлежащие государству, для предоставления облачных услуг на постоянной основе государственным органам (частные облака) с привлечением частных поставщиков;

- **классификации данных и услуг**, управляемых государственными органами, чтобы определить, какие данные будут размещаться на PSN (государственном частном облаке), а какие – на сертифицированном публичном и гибридном облаке.

Выделяются 3 типа данных: стратегические (влияющие на национальную безопасность); критические (данные и услуги, компрометация которых может нанести ущерб поддержанию функций, имеющих отношение к обществу, здоровью, безопасности и экономическому и социальному благополучию страны, например, медицинские данные граждан); обычные (данные, компрометация которых не влияет на прекращение оказания государственных услуг, не наносит ущерб экономическому и социальному благополучию страны);

- внедрению AgID **системы сертификации поставщиков облачных услуг** (по требованиям безопасности и надежности), внедрению систематического процесса проверки и квалификации облачных сервисов, используемых госорганами; разработке требований к договорным условиям соглашений об уровне обслуживания (SLA), заключаемым государственными органами; созданию маркетплейса поставщиков облачных услуг.

Таким образом, Облачная стратегия государственного управления (Strategia Cloud Italia) заложила основные меры по переходу государственных органов в облака, концентрируясь на внедрении стандартов безопасности для последующей сертификации поставщиков облачных услуг, создания гибкой системы закупок и процесса миграции государственных органов в облака.

### Проекты по созданию государственных облаков

В рамках Облачной стратегии был принят документ «**Облако государственного управления**» (Il Cloud della Pubblica Amministrazione), который содержит описание основных элементов государственного облака в Италии[3]. Согласно данному документу, физические и виртуальные ИТ-инфраструктуры, предназначенные для использования госорганами, должны отвечать определенным требованиям:

1 https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/index.html

2 В соответствии с Циркуляром № 1/2019 госорганы проходили опрос для определения безопасности своих ЦОД, которые впоследствии были разделены на две группы — группу «А» и группу «Б», а также специальную третью категорию — «Может использоваться для Национального стратегического хаба (PSN)» . ЦОД группы «Б» не обладают необходимыми требованиями безопасности, поэтому в соответствии с Облачной стратегией они должны быть заменены на ЦОД группы «А», имеющими сертификацию AgID.

3 https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/index.html

- **организационным** – поставщики должны быть сертифицированы в отношении предоставления услуг, управления ресурсами и процессами, поддержки пользователей, управления изменениями;

- **безопасности и надежности** – должны быть определены уровни обслуживания, конфиденциальности, безопасности и защиты данных;

- **производительности и интероперабельности** – должны быть созданы гарантии производительности инфраструктур и возможности взаимодействия с другими подобными инфраструктурами через открытые стандарты, а также возможность экспорта данных предоставляемых услуг в открытые форматы.

Проверка соблюдения этих требований составляет фундаментальную часть процесса квалификации ИТ-инфраструктур, которые могут работать в облаке госорганов.

При миграции государственных органов в облако сначала будет проводиться оценка класса данных, которые переносятся в облако, далее система будет давать возможности размещать данные в одном из трех блоков, из которых состоит Облако государственного управления:

1. **Публичное облако (Public Cloud)** – предоставление общедоступных облачных услуг поставщиками (Cloud Services Providers, CSP), квалифицированными AgID.

Такие облачные услуги возможно закупить посредством рамочного контракта (Convenzioni) или с помощью системы закупок «Электронный маркетплейс» – дополнительной квалификации в Consip (государственной компании, учрежденной Министерством экономики и финансов для осуществления закупок для госорганов (Центр инновационных закупок) и последующим (не всегда, также возможна закупка сразу после квалификации) тендером госоргана.

Перечень квалифицированных поставщиков облачных услуг размещается на **Облачном маркетплейсе** (Cloud Marketplace) – специализированной платформе, на которой доступны сервисы и инфраструктуры, одобренные AgID[1].

2. **Частное облако (Private Cloud)** – инфраструктура и услуги, предоставляемые Национальными стратегическими хабами (Polo Strategico Nazionale).

Хабы предназначены для управления стратегическими данными, то есть, данными, связанными с национальной безопасностью (имеют повышенный уровень защиты). Предусматривается прямой контроль государства над ИТ-инфраструктурами (закупку проводит внутренняя компания Министерства обороны Difesa Servizi SpA).

Управление PSN будет поручено **квалифицированному поставщику**, соответствующему техническим и организационным требованиям в части защиты стратегических данных. Хабы будут предоставлять услуги IaaS, PaaS[2].

3. **Облако сообщества (Community Cloud)** – услуги SPC Cloud Lotto 1.

Госорганы могут закупать облачные услуги с помощью Consip в рамках Системы общего доступа (SPC, Sistema Pubblico di Connettività) – программы по обеспечению госорганов интероперабельными телематическими услугами, которая выделяется в качестве отдельной категории в Облаке государственного управления[3].

1 https://catalogocloud.agid.gov.it/

2 https://innovazione.gov.it/dipartimento/focus/polo-strategico-nazionale/

3 https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita


**Рис. 5. Элементы государственного облака в Италии**

Lotto 1 – термин для обозначения категории услуг (облачные услуги), которые возможно закупить посредством специального рамочного соглашения (Contratto / L'Accordo Quadro), определяющего общие условия предоставления облачных услуг одним из поставщиков, выигравших тендер. Происходит закупка услуг Iaas, Paas[1].

Среди поставщиков в настоящее время телекоммуникационная компания Telecom Italia, американская ИТ-компания DXC Technology, итальянский оператор почтовой связи Poste Italiane, поставщик решений в сфере электронного документооборота, инвойсинга и иных услуг Postel[2]. В дополнение к рамочному соглашению заключается еще одно, определяющее индивидуальные условия предоставления облачных услуг госоргану[3].

Таким образом, государственное облако будет состоять из трех элементов. Схема элементов облачной модели органов власти приведена на рис. 5.

Как осуществляется переход итальянских государственных органов в государственное облако? В рамках Облака государственного управления AgID и Team Digitale разработали План внедрения облачных технологий (Cloud Enablement)[4], на который государственные органы должны ориентироваться при внедрении облачных технологий.

План состоит из трех элементов:

**1. принципа Cloud First**

Новые проекты и инициативы государственных органов должны разрабатываться с учетом модели Облака государственного управления. Государственным органам при переходе на облачные технологии рекомендуется **в приоритетном порядке** рассматривать облачные услуги **SaaS**. Услуги SaaS должны предоставляться через одну или несколько квалифицированных инфраструк-

1 https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=c9c346967a0548c7
2 https://www.cloudspc.it/ContrattoQuadro.html
3 https://www.cloudspc.it/FAQ.html?domanda=1
4 https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-enablement.html

тур, доступных через Cloud Marketplace (маркетплейс поставщиков облачных услуг, сертифицированных AgID). Далее госорганы могут рассматривать решения PaaS и IaaS.

**2. стратегии внедрения облачных технологий** для миграции существующих инфраструктур и переноса приложений в модель Облака государственного управления

Стратегия состоит из двух элементов:

- национальная программа Cloud Enablement, то есть набор **проектов**, которые позволят госорганам **мигрировать в облако**.
- структура Cloud Enablement, состоящая из набора ресурсов, операционных стратегий, методологий и инструментов, необходимых для реализации **Плана по внедрению облачных технологий госорганами**.

Структура Cloud Enablement состоит из двух основных элементов: блока управления и исполнительного блока.

**Блок управления** осуществляет деятельность по разработке методологий, программному менеджменту, контролю качества и мониторингу, что в совокупности составляет контроль за миграцией в облако.

**Исполнительный блок** представляет собой организации, отвечающие за разработку и выполнение конкретного проекта миграции в облако, включая первоначальную оценку инфраструктуры и приложений государственного органа для его миграции в облако, разработку и проведение процесса миграции, проверку безопасности системы с выявлением критических рисков; обучение государственных органов и пр. То есть, организации помогают конкретному государственному органу перейти в облако.

**3. центров компетенций**

**Создается расширенное сообщество** ИТ-специалистов, экспертов и менеджеров для обсуждения, предложения стандартов и регламентов цифровых услуг, обмена информацией, решениями и навыками, полезными для обслуживания, обновления и повышения надежности систем, автоматизации процедур.

Такие центры могут выполнять функцию агрегаторов, администрируя облачные сервисы от имени других госорганов. По окончании процесса облачной трансформации/миграции обновление, обучение, управление изменениями и оптимизация облачных ресурсов будут возложены на центры компетенций.

Таким образом, в Италии создана инфраструктура для помощи государственным органам в миграции на облака с помощью специальных государственных организаций и специалистов по переходу на облачные технологии.

В соответствии с Облачной стратегией также было разработано **Руководство по внедрению облачных технологий** (Manuale di abilitazione al cloud) в дополнение к Плану внедрения облачных технологий[1]. Руководство ориентировано на предоставление набора методов, инструментов и лучших практик, которые госорганы могут использовать для миграции в облако существующих инфраструктур и приложений. Руководство содержит дорожную карту по миграции в облако[2], методы оценки и анализа существующей инфраструктуры, аспекты лицензирования ПО, лучшие практики по обеспечению безопасности, интероперабельности, масштабируемости и др., например:

1 https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/bozza/index.html

2 https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/bozza/come-iniziare/roadmap-di-una-migrazione.html

- для оценки стоимости миграции в облако госорганам рекомендуется использовать специальные **калькуляторы** (где они доступны) на **Cloud Marketplace**, а также учитывать расходы на консультационные услуги и лицензирование;

- в Руководстве рассматривается **шесть стратегий миграции в облако** с обозначением их преимуществ и рисков.

Например, стратегия «Изъятие» заключается в том, что с помощью нее госорганы могут идентифицировать неиспользуемые приложения, избавиться от них и сфокусироваться на наиболее используемых, однако при этом существует риск, связанный с адаптацией имеющихся инфраструктур (оставшихся приложений, которые госорган продолжает использовать) к облаку. Другая стратегия «Повторная закупка» заключается в замене приложения, установленного и управляемого локально, аналогом SaaS. Среди плюсов стратегии можно выделить низкие затраты, сокращение времени простоя для обновления системы и др., но существует риск привязки к одному поставщику, миграции данных в другую модель данных и др.;

- для снижения риска «привязки к поставщику» госорганам рекомендуется использовать **стандартные форматы данных**, обеспечивать интероперабельность.

Сертифицированные AgID поставщики облачных услуг не могут включать в договор никаких положений, ставящих заказчика в положение привязки только к данному поставщику;

- рекомендации по **подготовке к миграции в облако**: планирование оптимизации затрат с определением областей, в которых будут снижены издержки после перехода в облако; проверка совместимости приложений с новой версией операционной системы; оценка базы данных и формирование отчета об их миграции и др.;

- после миграции рекомендуется **оценить переход на основании KPI**, к которым относят: стоимость оборудования и срок его службы, стоимость миграции приложений, сколько времени потрачено на планирование и осуществление миграции, стоимость обучения и переквалификации сотрудников и др. показатели.

Таким образом, в Италии разработано руководство, используя которое государственный орган может определить свою собственную стратегию миграции в облако, определить перечень расходов, спланировать и провести процесс миграции, а также оценить эффективность перехода на облачные услуги.

### Мультиоблачный подход (multicloud) к получению облачных услуг

Облачная стратегия Италии выделяет в качестве риска «привязку к поставщику», то есть государственные органы не должны закупать услуги у одного поставщика, им следует вовлекать несколько поставщиков, реализуя **подход мультиоблачности**.

В сентябре 2021 г. государственный банк Cassa Depositi e Prestiti (CDP), компании-разработчики Leonardo, Sogei и телекоммуникационная компания TIM совместно представили Министерству технологических инноваций и перехода к цифровым технологиям Италии (MITD) предложение о государственно-частном партнерстве для создания **Национального стратегического хаба (PSN)** [1]**– частного облака, управляемого государством**.

Одна из ключевых задач PSN – оптимизация и консолидация государственных ЦОД и связанных с ними IT-систем. В рамках PSN должно быть обеспечено предоставление услуг IaaS и PaaS (формируется частное облако).

1 https://www.leonardo.com/en/press-release-detail/-/detail/28-09-2021-cdp-leonardo-sogei-and-tim-present-proposal-to-create-national-strategic-hub

В настоящее время объявлена закупка услуг по разработке и обслуживанию данного облака, заявки подаются до 16 марта 2022 г[1]. В пакет документов по закупке входит Предложение по реализации PSN по модели государственно-частного партнерства. Данный документ указывает, что в числе фундаментальных свойств государственного облака должны быть технологии и архитектурные решения, основанные на принципе мультиоблачности.

Отмечается также, что принцип мультиоблачности предлагается как комплексное решение для гибридных и мультиоблачных архитектур и как единый интерфейс для клиента, независимо от поставщика облака. На PSN могут разрабатываться индивидуальные решения для разных клиентов.

**NB!** Для **стратегических данных** (данных, связанных с национальной безопасностью, имеющих повышенный уровень защиты), а также **критически важных сервисов** (сервисов, прекращение работы которых может нанести ущерб функциям, важным для общества, здоровья, безопасности населения, экономического и социального благополучия страны) облачные технологии используются с привлечением частного сектора в рамках **государственно-частного партнерства**.

С учетом того, что в Италии применяется принцип мультиоблачности, с 1 апреля 2019 г. был запущен **Cloud Marketplace AgID** (маркетплейс облачных услуг AgID), где органы государственного управления могут приобретать инфраструктуры и решения через **Облачный каталог** (Catalogo dei servizi) (рис. 6).

В нем размещены провайдеры, соответствующие стандартам качества, которые можно классифицировать в зависимости от вида услуг: SaaS, PaaS и IaaS. При выборе услуги можно ознакомиться со всей необходимой информацией, включая детали каждой услуги, выбрать отдельные характеристики услуг в зависимости от целей получения услуг, стоимость и уровни обслуживания, заявленные поставщиком, связаться с поставщиком. То есть госорганы могут сравнивать аналогичные услуги и выбирать наиболее подходящие решения, исходя из своих потребностей.

Среди поставщиков находится Amazon Web services (услуги PaaS), Elogic SRL (услуги IaaS), Google Ireland Limited (PaaS), Palo Alto Networks Italia SRL (SaaS) и другие. Таким образом, поставщиками облачных услуг выступают как гиперскейлеры, так и местные итальянские компании, включая МСП.

Например, Oracle, TIM (Telecom Italia) и Noovle (дочерняя облачная компания TIM Group), в октябре 2021 г. объявили о подписании соглашения о сотрудничестве в рамках плана по предоставлению корпоративных мультиоблачных услуг для предприятий и организаций государственного сектора в Италии.[2]

Компания Noovle предлагает обширную сеть центров обработки данных в Италии, которая была разработана в соответствии высокими технологическими стандартами, стандартами безопасности и охраны окружающей среды с ESG-целями TIM Group (LEED Gold, TIER IV, стандарты ISO, Ansi-TIA и др.)[3]. TIM Group предоставляет облачные услуги IaaS, SaaS и PaaS, сертифицированные согласно стандарту ISO/IEC 27001[4]. Oracle также является поставщиком услуг IaaS, SaaS и PaaS[5].

В качестве способа закупки облачных услуг AgID указывает **портал для закупок государственных органов** – **AcquistinRetePA**, созданный Министерством финансов и подотчетным ему

1 https://innovazione.gov.it/dipartimento/focus/polo-strategico-nazionale/

2 https://www.oracle.com/news/announcement/oracle-tim-noovle-to-offer-multicloud-services-in-italy-2021-10-08/

3 https://www.noovle.com/it/datacenter/

4 https://www.gruppotim.it/en/investors/reports-presentations/sustainability-report/detailed-information/certifications.html

5 https://www.oracle.com/cloud/

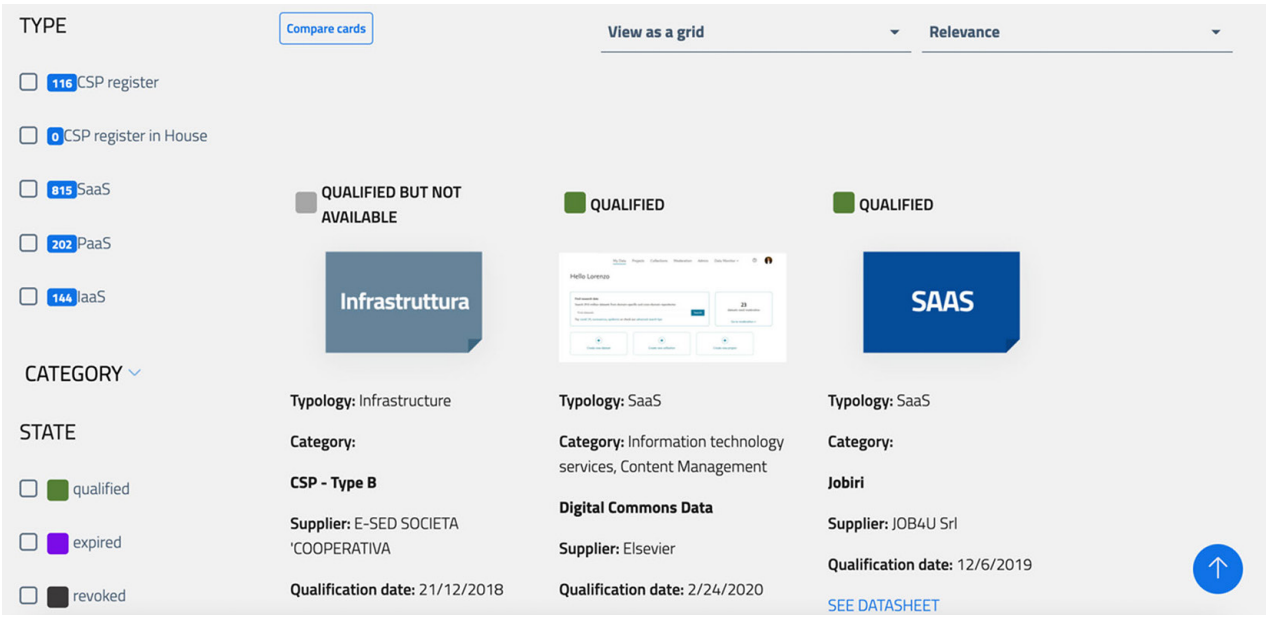



**Рис. 6. Каталог поставщиков на Маркетплейсе облачных услуг**

центром Consip[1]. Таким образом, на Маркетплейсе облачных услуг можно ознакомиться со всей необходимой информацией о поставщиках, а сама закупка услуг возможна через специальный портал закупок AcquistinRetePA.

## Прохождение аккредитации, сертификации поставщиками облачных услуг

Для того, чтобы попасть на Cloud Marketplace, поставщик облачных услуг должен быть **сертифицирован** Агентством по цифровизации Италии (AgID). Сертификация проходит по Циркулярам Агентства AgID № 2 и № 3 от 9 апреля 2018 г.[2], включающим требования безопасности, производительности и масштабируемости, функциональной совместимости, переносимости и пр., которые используются AgID при проведении сертификации.

Так, **Циркуляр № 2 регулирует вопросы квалификации поставщиков облачных услуг IaaS/PaaS**. Квалификационные требования можно разделить на организационные и особые требования. Квалификация действует в течение 24 месяцев с даты регистрации в государственном реестре.

Поставщик должен предоставить необходимую документацию, чтобы доказать **соответствие организационным требованиям**:

- об **управлении «критическими ситуациями»**, например, операциями аварийного восстановления, проверкой целостности данных и их возможным восстановлением;
- о системе управления **качеством** услуг;
- об информации **о службе поддержки клиентов**, работающей 24/7 и способной покрыть оперативные потребности, которые могут возникнуть при предоставлении услуг;
- о процедурах, регулирующих такие виды деятельности, как управление изменениями, конфигурацией и инцидентами (**безопасность и инфраструктура**);
- о **гарантиях прозрачности данных** и сведений в предоставляемой поставщиком документации.

1 https://www.acquistinretepa.it/opencms/opencms/index.html

2 https://cloud-italia.readthedocs.io/projects/cloud-italia-circolari/it/latest/

Эталонными стандартами для этого набора требований являются стандарты, принадлежащие к семейству **ISO/IEC 20000**, в частности, стандарты ISO/IEC 20000-1 и ISO/IEC TR 20000-9.

**Циркуляр № 3 регулирует вопросы квалификации облачных услуг SaaS**. Отличительной особенностью циркуляра является то, что заявителем может быть:

- **частный поставщик услуг SaaS**, который намеревается предоставлять эти услуги в одной или нескольких инфраструктурах гособлака; при этом поставщик услуг SaaS может сам быть квалифицированным поставщиком облачных услуг IaaS / PaaS согласно Циркуляру № 2;

- **государственный орган, который намеревается предоставлять услуги SaaS** в одной или нескольких инфраструктурах гособлака (Национальный стратегический хаб, квалифицированный поставщик облачных услуг, или поставщик облачных услуг в соответствии с рамочным соглашением Consip).

Квалификация действует 24 месяца с момента регистрации на Cloud Marketplace. Квалификационные требования можно разделить на организационные и особые требования.

**В организационные требования входит**:

- наличие структурированной **службы поддержки клиентов**, способной оперативно реагировать на обращения;

- наличие надежного механизма по обеспечению **постоянного обновления программного обеспечения** в рамках услуг SaaS;

- принятие **отраслевых «лучших практик»** (например, поставщик предоставляет покупателю панель управления и программные интерфейсы приложений (API), которые позволяют получать информацию о методах формирования стоимости оказываемых услуг), а также руководящих принципов, описанных Циркуляре, в отношении разработки, настройки и обслуживания программного обеспечения, используемого для реализации предоставляемых услуг.

Особые требования, предъявляемые к поставщикам облачных услуг, во многом пересекаются в рамках Циркуляров №№ 2 и 3 и включают следующие аспекты:

- **безопасности, конфиденциальности и защиты данных**. Поставщик SaaS должен убедиться, что код приложения был разработан в соответствии с принципами безопасной разработки.

Поставщик должен **пройти сертификацию по стандарту ISO / IEC 27001** «Системы обеспечения информационной безопасности», дополненному элементами управления стандартами ISO / IEC 27017 «Свод правил по управлению информационной безопасностью» (включающий стандарты аудита информационных систем и облачных служб) и ISO / IEC 27018 «Свод правил по защите персональных данных в облаке».

Сертификат должен быть выдан национальными органами по аккредитации, признанными ЕС. В качестве альтернативы согласно Циркуляру № 3 поставщик проводит **самооценку CSA STAR**[1] со ссылкой на услугу, которую он намеревается сертифицировать, создает соответствующую документацию и размещает ее в открытом доступе на своем веб-сайте;

- **производительности и масштабируемости**. Поставщик обязан обеспечивать качество и надежность услуги на протяжении всего жизненного цикла.

1 https://cloudsecurityalliance.org/star/

Поставщик указывает условия максимальной нагрузки, которые может выдержать система, как с точки зрения количества одновременных пользователей, так и/или объема запросов, которые могут быть обработаны. Госорганы, закупающие облачные услуги, проверяют соглашение об уровне обслуживания (SLA) на наличие раздела, касающегося «**гарантированных уровней обслуживания**».

Поставщик оценивается в соответствии со стандартами ISO / IEC 19086-1: 2016 «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции», ISO / IEC 22313 «Менеджмент непрерывности бизнеса. Руководство по внедрению»;

- **интероперабельности и переносимости**. Квалифицированные услуги IaaS и PaaS должны обеспечивать возможность взаимодействия с другими услугами того же типа за счет использования **открытых стандартов** (например, Open Virtualization Format) и соответствующего программного интерфейса приложения (API).

- **соблюдения законодательства**. Поставщик предоставляет информацию о соблюдении европейского и итальянского законодательства в контексте использования услуг и квалифицированной инфраструктуры. Поставщик раскрывает информацию об иностранных государствах, в которых находятся его ЦОД или облачная инфраструктура, через которые будет предоставляться услуга и / или в рамках которых будут передаваться данные.

### Стандарты безопасности услуг облачных поставщиков, аудита и страхования услуг

Система стандартов безопасности состоит из:

**1. стандартов безопасности и других стандартов**, по которым поставщики облачных услуг проходят сертификацию AgID для участия в Маркетплейсе – Циркуляры Агентства AgID N°N° 2 и 3 от 9 апреля 2018 г.

Циркуляры, в частности, включают процедуры в отношении **аудита**, основанные на стандарте ISO/IEC 27017 «Свод правил по управлению информационной безопасностью». Так, для аудита поставщика необходимо привлечь независимую организацию, которая выдаст заключение в соответствии с данным стандартом ISO / IEC. Например, стандарт содержит требования в отношении политик информационной безопасности (ИБ), требования к ИБ при управлении проектами и в отношении мобильных устройств, аспекты менеджмента активов и другие;

**2. «Минимальных мер безопасности ИКТ для государственных органов»** (Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni)[1].

Согласно Циркуляру N° 2/2017 от 18 апреля 2017 г. госорганы должны были внедрить эти **минимальные меры безопасности** до 31 декабря 2017 г. Меры состоят из технологических, организационных и процедурных средств контроля, на которые госорганы ориентируются при оценке своего уровня ИТ-безопасности[2].

В зависимости от сложности информационной системы минимальные меры могли быть внедрены постепенно по **трехуровневой системе**:

- **минимальный уровень**: те требования, которым должен соответствовать любой госорган независимо от его характера;

- **стандартный уровень**: уровень выше минимального, который каждый госорган должен рассматривать в качестве эталона с точки зрения безопасности и который отражает состояние систем в большинстве итальянских госорганов;

1 https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

2 ttps://www.agid.gov.it/sites/default/files/repository_files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

- **продвинутый (высокий) уровень**: он должен быть принят госорганами, наиболее подверженными рискам (например, из-за критичности обрабатываемой информации или предоставляемых услуг), а также должен рассматриваться как цель, к которой должны стремиться все госорганы.

Например, среди требований к инвентаризации авторизованных и неавторизованных устройств анализ трафика систем, подключенных к сети, является требованием высокого уровня и применяется только к соответствующим госорганам. В то же время требование о сканировании систем на наличие несанкционированного ПО является обязательным требованием для всех видов госорганов (все уровни минимальных мер) в блоке «Инвентаризация разрешенного и несанкционированного ПО».

Что касается вопросов **страхования**, то государственных требований к страхованию поставщиков облачных услуг не установлено, однако они имеют возможность добровольно застраховаться от киберрисков в частных страховых компаниях[1].

### Управление персональными данными при создании государственных облаков

К цифровым платформам в Италии применяются положения **Кодекса о защите персональных данных**[2]. Данный Кодекс устанавливает положения по адаптации национальной правовой системы к Общему Регламенту ЕС о защите персональных данных (GDPR).

Кодексом определены, в частности, правила обработки персональных данных органами власти, в том числе правила доступа к административным записям, обработки персональных данных о здоровье, правила уведомления субъектов данных об обработке их данных, а также правила обработки персональных данных для определенных целей (журналистских, исторических, целей маркетинга и т.д.).

Таким образом, в Италии применяются нормы GDPR[3], которые должны учитывать как государственные органы (как операторы данных), так и поставщики облачных услуг при наличии доступа к персональным данным.

### Формирование ценообразования при осуществлении государственных закупок облачных услуг

Для закупок облачных услуг используется метод **«цены за потребление»** (prezzo a consumo): в контракт включается условие, по которому оплата производится в конце в размере стоимости потребленных услуг[4].

**На портале государственных закупок AcquistinRetePA представлено 4 способа закупок:**

- **рамочные соглашения (Accordi Quadro)**

Для закупки облачных услуг в рамках SPC Cloud Lotto 1 используются рамочные соглашения (Accordo Quadro) – это контракты, заключенные Consip с одним или несколькими поставщиками облачных товаров или услуг.

Структура закупки по рамочному соглашению выглядит следующим образом. Consip объявляет тендер, поставщики подают свои предложения, и Consip присуждает тендер нескольким из них.

1 https://www.cybersecurity360.it/soluzioni-aziendali/polizze-assicurative-nel-settore-del-cyber-risk-soluzioni-operative/

2 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9740796

3 https://www.dataguidance.com/notes/italy-data-protection-overview

4 https://cispe.cloud/website_cispe/wp-content/uploads/2020/06/CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v-IT-2020-05-11.pdf

Используется рамочное соглашение для прямой закупки госорганом без внесения изменений, либо госорган объявляет специальный тендер для этих поставщиков, чтобы индивидуализировать рамочное соглашение.

Рамочные соглашения имеют конкретную продолжительность и количественный или экономический объем услуги / товара, который поставщик обязан гарантировать во время исполнения контракта. Такие контракты подразумевают заключение дополнительных соглашений с поставщиками для индивидуализации услуг под нужды конкретного госоргана (посредством специального тендера). Посредством рамочных соглашений возможна закупка IaaS, PaaS, SaaS[1].

Цена контракта может быть как выше, так и ниже пороговых значений ЕС. При этом стоимость формируется на основании цен за единицу, возможно применение процедуры корректировок[2].

Применительно к отдельным дополнительным соглашениям оплата услуг поставщика происходит раз в два месяца на основании фактически оказанных услуг в соответствии с Проектом требований к услугам в последней утвержденной версии. На сайте закупок в отношении IaaS и PaaS указано[3], что может быть как установлена максимальная цена за услугу, так и тарифы[4].

Таким образом, система закупок через рамочные соглашения (Accordo Quadro) создана **специально для закупки облачных услуг** и предполагает ограниченный перечень поставщиков, а также включает в себя возможность кастомизации условий предоставления услуг под нужды госорганов и систему **ценообразования с оплатой как за единицу** (тарифы), так и с установлением **максимальной цены**.

- **рамочные контракты (Convenzioni)**

Могут использоваться рамочные контракты (Convenzioni)[5] – это контракты, которые государственные органы могут использовать для приобретения или аренды товаров и услуг. Цена может быть как выше, так и ниже пороговых значений ЕС.

Такие контракты не подразумевают заключения дополнительных соглашений, все условия изначально включаются в рамочный контракт и не подлежат изменению. Госорганы формируют каталог услуг и товаров на основании того, что им необходимо, и подают заявку на контракт в Consip.

Система закупок в данном формате работает таким образом, что после формирования каталога госорганами Consip объявляет тендер с несколькими лотами на закупку определенных товаров или услуг, например, лицензированного ПО[6]. Поставщики подают заявки, затем Consip присуждает тендер некоторым из них. После присуждения тендера «активируется» рамочный контракт, на основании которого без дополнительных соглашений и без изменения условий договора госорган может закупить товар/услугу.

Цена устанавливается по итогам тендера, при этом она может отличаться в отношении разных лотов. Также может быть установлена минимальная цена закупки (например, 15 млн евро в случае закупки ПО). Рамочные контракты подходят для закупки IaaS, PaaS, SaaS[7].

1 https://cached.forges.forumpa.it/assets/Speeches/26784/co_08_laurenti.pdf
2 https://www.cloudspc.it/FAQ.html
3 https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=c9c346967a0548c7
4 https://www.acquistinretepa.it/downloadservices/getDocument?id=72f2d2ef7a6050cb&idIniziativa=c9c346967a0548c7
5 https://www.acquistinretepa.it/opencms/opencms/english/program_how_itWorks.html
6 https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=90257982e01ca4fa
7 https://cached.forges.forumpa.it/assets/Speeches/26784/co_08_laurenti.pdf

Таким образом, система закупок с помощью рамочных контрактов (Convezioni) не предполагает индивидуальных условий предоставления услуги/товара госоргану, а **цена формируется** либо по итогам **тендера**, либо устанавливается **минимальная цена**.

- **динамическую систему закупок (SDA)**

Динамическая система закупок (Sistema dinamico di acquisizione – SDA) – это цифровой рынок, на котором госорганы могут приобретать товары и услуги на суммы, равные пороговым значениям в ЕС или выше.

Consip запускает подачу заявок для получения статуса «квалифицированного поставщика» (Consip осуществляет проверку поставщика). Поставщики (экономические операторы) могут в любое время подать заявку на квалификацию для тендера. После отбора квалифицированных поставщиков госорган запускает тендер и предоставляет индивидуализированную информацию о тех товарах или услугах, которые хочет закупить.

Такая система характеризуется тем, что госорган сам составляет требования к товару или услуге. Поставщик выбирается на основании наиболее выгодного с экономической точки зрения предложения и по минимальной предложенной цене за товар/услугу[1]. Закупка SaaS осуществляется через динамическую систему закупок[2].

Таким образом, динамическая система закупок характеризуется привязкой цены контракта к ценам, установленным в ЕС. У госоргана также существует возможность приобрести услуги/товары с теми свойствами, которые подходят для удовлетворения его конкретных нужд.

- **электронный маркетплейс (MePA)**

Электронный маркетплейс (Mercato elettronico – MePA) – это цифровой рынок, на котором государственные органы могут приобретать товары, услуги и работы на суммы ниже пороговых значений ЕС.

Структура закупки в рамках электронного маркетплейса выглядит следующим образом: Consip запускает подачу заявок для получения статуса «квалифицированного поставщика» (Consip осуществляет проверку поставщика при закупке, даже если поставщик был квалифицирован AgID для выхода на Маркетплейс облачных услуг).

Поставщики (экономические операторы) могут в любое время подать заявку на квалификацию для тендера. Когда будут определены все квалифицированные поставщики, госорган либо сразу осуществляет закупку у какого-либо из них, либо проводит тендер, после чего присуждает контракт. Маркетплейс подходит для закупок IaaS, PaaS[3].

Данный инструмент для закупок характерен для приобретения облачных услуг госорганами через Маркетплейс облачных услуг. На портале закупок в рамках электронного маркетплейса создана отдельная категория закупок «Услуги ИКТ», куда входят облачные услуги[4]. Цена формируется индивидуально в ходе переговоров с поставщиками, однако для данной категории услуг установлена минимальная стоимость контракта – 500 евро.

Основные аспекты различий между системами закупок представлены в табл. 2.

1 https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=ca64945595b9125e

2 https://cached.forges.forumpa.it/assets/Speeches/26784/co_08_laurenti.pdf

3 https://cached.forges.forumpa.it/assets/Speeches/26784/co_08_laurenti.pdf

4 https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=b577cd18b64b21a3

**Таблица 2. Системы закупок Италии**

| Система закупок | Вид облачных услуг | Возможность индивидуальных условий | Ценообразование | Выбор поставщика |
|---|---|---|---|---|
| Рамочные соглашения (Accordo Quadro) | IaaS<br>PaaS<br>SaaS | Да, требуется заключение дополнительного соглашения | Как выше, так и ниже пороговых значений ЕС;<br>Могут быть тарифы и установление максимальной цены | Ограниченный выбор поставщиков |
| Рамочные контракты (Convenzioni) | IaaS<br>PaaS<br>SaaS | Нет | Как выше, так и ниже пороговых значений ЕС;<br>Может быть установление минимальной цены;<br>Формируется по итогам тендера | Выбор не ограничен |
| Динамическая система закупок | SaaS | Да, в рамках одного контракта | Как равная, так и выше пороговых значений ЕС;<br>Выбирается наиболее выгодное предложение | Выбор не ограничен |
| Электронный маркетплейс | IaaS<br>PaaS | Да, в рамках одного контракта | Ниже пороговых значений ЕС;<br>Формируется по итогам тендера;<br>Может быть установлена минимальная цена | Выбор не ограничен |

**Источник:** составлено авторами.

# 5. Опыт Германии

## Стратегические документы, устанавливающие меры по переходу государственных органов на облачные технологии

В Германии принята **Облачная стратегия управления** (Deutsche Verwaltungscloud-Strategie) в 2020 г. для организации процесса миграции госорганов в облако[1]. По сравнению со стратегическими документами Италии и США она менее детализирована и закладывает общие цели по стандартизации федеральных облачных решений для обеспечения возможности объединения облачных решений друг с другом.

Планируется создать стандарты разработки платформ (включая процессы и архитектурные спецификации для разработки приложений); стандарты доставки и обслуживания приложений на протяжении всего их жизненного цикла; репозиторий кода (стандартизированные среды для управления версиями кода приложения и централизованного зеркалирования или хранения децентрализованных исходных кодов с их документацией); стандарты аппаратных и программных компонентов, используемых для предоставления ИТ-услуг (инфраструктурных сервисов); операционные стандарты и операционную модель (гармонизация сотрудничества с поставщиками ИТ-услуг и предоставления услуг). Таким образом, Облачная стратегия управления Германии направлена на **разработку стандартов для облачных решений**.

В Облачной стратегии обозначены общие требования к этим областям облачной архитектуры: например, стандарты должны соответствовать базовым требованиям защиты ИТ Федерального управления информационной безопасности (BSI) (стандарт ISO 27001) и должны быть определены для категорий требований к защите данных «нормальный уровень защиты» и «высокий уровень защиты»; необходимо создание или использование модульных (облачных) архитектур с открытыми интерфейсами, которые позволяют автоматизировать весь жизненный цикл приложения; программная архитектура облачной инфраструктуры должна быть предпочтительно основана на открытом программном обеспечении, свободном от технических или юридических ограничений на использование, и др.

## Проекты по созданию государственных облаков

В Германии государственным облаком Федеральной администрации является **Bundescloud – частное облако**, которое представляет собой **единую платформу** для разработки органами власти программного обеспечения в соответствии с унифицированными стандартами и методами.

Разработка Bundescloud началась в 2015 году. Посредством Bundescloud облачные сервисы предоставляются по моделям IaaS, PaaS и SaaS[2]. В Bundescloud все данные хранятся на серверах в Германии. Функции разработчика и оператора платформы выполняет Федеральный центр информационных технологий (ITZBund) по поручению Федерального министерства внутренних дел и родины[3]. Примеры сервисов Bundescloud представлены на рис. 7.

Таким образом, на Bundescloud предоставляются следующие сервисы:

- BundescloudServer (**IaaS**) – виртуальные машины с операционной системой, памятью и сетевыми структурами. На данный момент доступны операционные системы Linux и Windows.
- Bundescloud Access Management (**PaaS**) – центральная система аутентификации. Все подключенные приложения находятся в сети единого входа (Web-Single-Sign-On, SSO). После

1 https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/deutsche_verwaltungscloudstrategie.pdf;jsessionid=FE7601F72F8952223FB2E9C87EF1EC6F.1_cid332?__blob=publicationFile

2 https://www.itzbund.de/DE/itloesungen/egovernment/bundescloud/bundescloud_node.html

3 https://www.itzbund.de/SharedDocs/Pressemitteilungen/DE/2020/2020-04-02_BC_Entwicklungsplattform.html

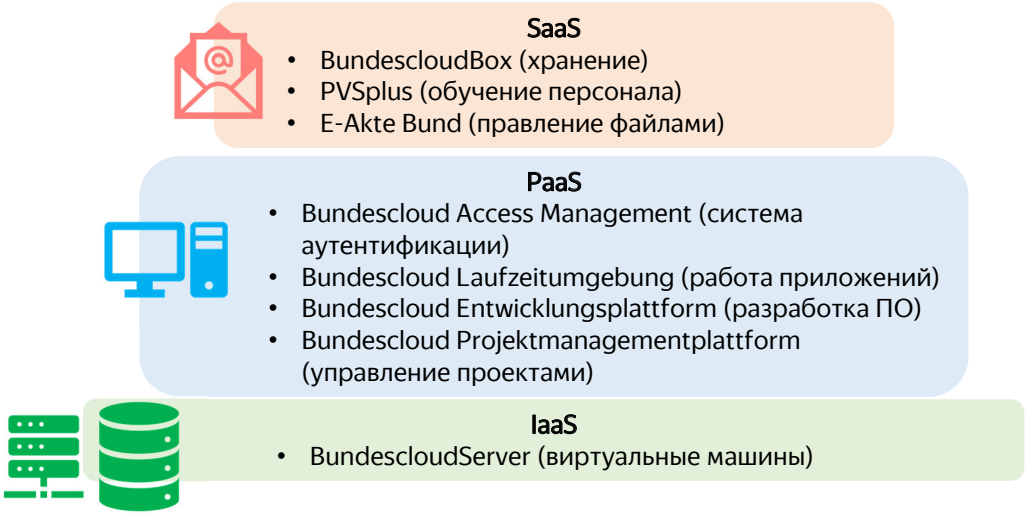



**Рис. 7. Сервисы по моделям IaaS, PaaS, SaaS, предоставляемые на Bundescloud**

однократной аутентификации все подключенные приложения можно использовать без повторного входа в систему.

- Bundescloud Laufzeitumgebung (**PaaS**) – платформа для работы приложений и веб-сервисов. На платформе можно запускать приложения Java Enterprise, например, для предоставления веб-служб. Трехуровневая архитектура включает веб-сервер NGINX, промежуточное ПО JBoss или Liberty и базу данных MariaDB.

- Bundescloud Entwicklungsplattform (**PaaS**) – платформа для разработки программного обеспечения, работающая на ПО с открытым исходным кодом Cloudogu[1]. Разработчики могут тестировать свое программное обеспечение через платформу.

- Bundescloud Projektmanagementplattform (**PaaS**) – платформа для управления проектами, включает в себя такие модули, как Redmine, Easy Redmine, Confluence и Jira.

- BundescloudBox, SIB Box (**SaaS**) – облачное хранилище файлов, базируется на программном обеспечении с открытым исходным кодом от компании-разработчика NextCloud[2]. Сервис используется для хранения, передачи и синхронизации данных.

- PVSplus (personal management system plus) training system (**SaaS**) – интегрированная система обучения персонала.

- E-Akte Bund (**SaaS**) – централизованная система управления электронными файлами.

Стоит отметить, что на Bundescloud размещается и **секретная информация с наивысшим уровнем защиты**, поэтому федеральное облако должно соответствовать критериям **конфиденциальности уровня VS-NfD** (то есть обеспечивать конфиденциальность секретной информации).

В Памятке по обращению с секретными материалами указывается, что, если информационные технологии используются для обработки элементов, классифицированных как VS-NfD, то должны быть приняты соответствующие ИТ-меры и/или физические и организационные меры для обеспечения защиты секретной информации[3].

1 https://www.itzbund.de/DE/itloesungen/standardloesungen/bundescloudentwicklungsplattform/bundescloudentwicklungsplattform_node.html

2 https://www.itzbund.de/DE/itloesungen/standardloesungen/sibbox/sibbox_node.html

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile

Например, перед обработкой или хранением данных, классифицированных как VS-NfD, необходимо убедиться, что компьютер или внутренняя сеть не подключены напрямую к Интернету (например, без защиты брандмауэра). В частности, при обработке данных, классифицированных как VS-NfD, необходимо учитывать следующие аспекты: создание перечня лиц, имеющих право доступа; использование механизмов идентификации и аутентификации (например, логин, пароль); использование соответствующей Инструкции по ИТ-безопасности (для отдельного рабочего места или для организации в целом). То есть, в Bundescloud хранятся в том числе данные с наивысшим уровнем защиты.

Таким образом, **Bundescloud** представляет собой **федеральное частное облако**, которое обслуживает государственная компания ITZBund. Данное облако содержит сервисы хранения и обмена данными, управления проектами и рабочими процессами, при этом привлекаются частные поставщики услуг (например, модули платформы Bundescloud Projektmanagementplattform предоставляются разработчиками Easy Software и Atlassian).

Помимо работы частного облака Bundescloud, федеральные органы запускают **свои проекты по переходу на облачные услуги** (в основном услуги **SaaS**).

Например, Bundeswehr Вооруженные силы Германии Федерального министерства обороны совместно с SAP (поставщиком услуг PaaaS и SaaS) запустили **облачную платформу для управления строительными объектами**: в основе ERP-система (система управления компанией) BW SAP, которая также позволяет осуществлять финансовый учет и управление персоналом, управление и обслуживание недвижимости[1]. Система позволяет экономить до **25 000 евро на один** проект в связи с минимизацией бумажных операций.

Свое облако запустило Федеральное министерство иностранных дел – «**Diplo-Cloud**», Федеральное управление уголовной полицией – облако «**Police 2020**», Федеральное министерство финансов и пр.

**Земли и муниципалитеты** также внедряют облачные сервисы. Так, например, в Баварии используется облачный **сервис BayernBox**. Данный сервис позволяет муниципальным администрациям Баварии обеспечивать доступ к собственной онлайн-платформе, которую служащие могут использовать **для централизованного управления данными**, совместного хранения, обмена и редактирования данных. BayernBox основан на программном обеспечении с открытым исходным кодом ownCloud (услуги **SaaS**) и был разработан Агентством по цифровизации, высокоскоростному Интернету и измерениям (LDBV) в сотрудничестве с ownCloud[2].

В федеральной земле Баден-Вюртемберг в конце 2019 г. Службой по информационным технологиям (BITBW) в сотрудничестве с компанией NextCloud[3] была запущена облачная **платформа BITBW Cloud**. Платформа служит **частным облачным хранилищем для документов** и позволяет обмениваться ими между сотрудниками, клиентами и партнерами. В конце 2020 г. облаком BITBW уже пользовались более 7000 сотрудников[4]. К BITBW Cloud также имеют доступ региональные министерства, например Министерство продовольствия, сельской местности и защиты прав потребителей[5] Таким образом, в Германии создано федеральное частное облако, при этом органы власти (на федеральном, региональном и местном уровне) создают собственные облака в сотрудничестве с частными поставщиками облачных услуг. Такое сотрудничество реализуется путем предоставления частными компаниями (Nextcloud, ownCloud) программных решений с открытым исходным кодом, которые органы могут адаптировать под свои нужды.

1 https://news.sap.com/germany/2020/12/cloud-gebaeudemanagement-bundeswehr/

2 https://owncloud.com/news/bayernbox-owncloud-delivers-central-cloud-solution-for-bavarian-municipalities/

3 https://nextcloud.com/blog/ congratulations-to-the-new-german-government-coalition-for-their-open-source-strategy/

4 https://www.bitbw.de/fileadmin/user_upload/Geschaeftsbericht_BITBW_2020.pdf

5 https://rp.baden-wuerttemberg.de/fileadmin/RP-Internet/Themenportal/Laendlicher_Raum/Entwicklungsprogramm_Laendlicher_Raum/_DocumentLibraries/ELR/elr-merkbl-gemeind.pdf

## Мультиоблачный подход (multicloud) к получению облачных услуг

Несмотря на единственного разработчика и оператора (ITZBund), в Bundescloud также реализован **принцип мультиоблачности**: платформа базируется на программном обеспечении немецкой компании Cloudogu GmbH, а облачное хранилище BundescloudBox основано на разработке компании NextCloud[1].

На федеральном уровне используются более **80 облачных сервисов** от частных провайдеров, большая их часть представляет собой сервисы **SaaS**.

Сервисы предоставляются, например, компаниями Adobe, BlueJeans Network, Cisco, Vitero, Zoom, Atlasian и др[2]. В числе сервисов IaaS используются, например, сервисы TrendMicro (защита от вирусов), haufe (создание документов), Tableau (визуализация данных), iLOQ (управление системами блокировки).

По опросу правительственных органов, предоставление платформ обмена данными с функциональностью сотрудничества осуществляют компании ACP IT Solutions, Brainloop, COYO, Google, IT.NRW, Microsoft, Sozialpädagogisches Institut Berlin в рамках услуг SaaS. Услуги по развертыванию сетей и серверов (IaaS, PaaS) предоставляют компании AWS, Dark GmbH, CD Gromke, Cisco, Hetzner Online, Kroll Discovery, Microsoft, Oracle и пр[3].

В работе Bundescloud используются сервисы внешних частных разработчиков, такие как Easy Redmine (управление проектами), Jenkins (сервис по автоматизации билдов и тестов приложений), Jira (планирование и управление рабочими процессами), Nexus (хранилище артефактов), Smeagol (wiki-система) и др.[4]

Стоит отметить, что Германия также является страной-сооснователем и участником общеевропейского **проекта Gaia-X**. В рамках проекта разрабатываются **облачные решения и стандарты для внедрения защищенной инфраструктуры данных.** Проект является совместной инициативой федерального правительства Германии, бизнеса и экспертного сообщества[5]. Всего на данный момент в Gaia-X участвуют более 300 членов, из них 11 из Германии . В национальном хабе Германии [6]информацию о проекте и связанных с ним сервисах размещает Министерство экономики и защиты климата Германии.

Органы власти и государственные организации Германии также используют решения на инфраструктуре Gaia-X – например, **Национальный метрологический институт** Германии (Physikalisch-Technische Bundesanstalt) использует инфраструктуру Gaia-X для цифровизации средств проверки метрологических устройств и данных о таких проверках, а также для гармонизации национальных метрологических стандартов с аналогичными стандартами стран ЕС (European Metrology Cloud)[7].

Министерство экономики и защиты климата Германии, Gaia-X формирует сеть облачных сервисов и платформ, за счет которой государства могут реализовывать собственные мультиоблачные стратегии[8].

---

1 https://www.itzbund.de/SharedDocs/Pressemitteilungen/DE/2020/2020-04-02_BC_Entwicklungsplattform.html

2 file:///C:/Users/kache/Downloads/1910826.pdf

3 https://dserver.bundestag.de/btd/19/108/1910826.pdf

4 https://www.itzbund.de/DE/itloesungen/standardloesungen/bundescloudentwicklungsplattform/bundescloudentwicklungsplattform.html

5 https://www.accenture.com/de-de/blogs/public-service/cloud-braucht-mehr-vielfalt

6 https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/quality-infrastructure-digital-qi-digital.html

7 https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/quality-infrastructure-digital-qi-digital.html

8 https://www.bmwi.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2020/09/onlinemagazin-schlaglichter-09-20.html?cms_textId=2019196&cms_artId=2018806

## Стандарты безопасности услуг облачных поставщиков, аудита и страхования услуг

По общему правилу, в соответствии с Законом о Федеральном управлении информационной безопасности (BSIG) указанное Управление осуществляет **сертификацию организаций и систем в сфере кибербезопасности**[1].

Сертификация продуктов[2], в том числе облачных сервисов, осуществляется на предмет **соответствия стандарту ISO 27001** «Системы обеспечения информационной безопасности», собственным критериям ИТ-безопасности Федерального управления информационной безопасности (BSI)[3].

Например, по стандарту ISO сертифицирована частная облачная инфраструктура ITDZ Berlin, облачные сервисы Vodafone, инфраструктура для функционирования облака в земле Рейнланд-Пфальц и др.[4]

**Стандарт ISO 27001** определяет такие основные показатели безопасности информации, как оценка рисков, с которыми сталкивается организация, соблюдение законодательных, нормативных и договорных требований формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности. В число основных элементов системы информационной безопасности входят защита от несанкционированного доступа, авторизация и аутентификация, защита каналов передачи данных, обеспечение целостности, обеспечение актуальности данных при обмене информацией с клиентами, управление электронным документооборотом, управление непрерывностью работы, а также внутренний и внешний аудит систем безопасности[5].

Для **добровольной сертификации/аттестации** облачных услуг чаще всего используются сертификаты **SaaS EuroCloud** (некоммерческого инновационного хаба), CSA STAR (система самооценки), **TÜV Trust IT** (независимый орган по сертификации в Германии и Австрии).

Сертификат **IT-Grundschutz BSI** (определяет соответствие базовым требованиям безопасности Федерального управления информационной безопасностью) также может использоваться пользователями облачных вычислений[6].

Федеральные и региональные органы государственной власти используют облачные сервисы, предлагаемые частными немецкими и европейскими провайдерами. Поэтому для разработки облачных стандартов и сертификации в Германии был разработан проект **Trusted Cloud**, изначально субсидированный государством, а сейчас возглавляемый некоммерческой организацией[7].

Kompetenznetzwerk Trusted Cloud e. V. – это ассоциация Сети компетенций Trusted Cloud, которая отвечает за присвоение маркировки Trusted Cloud облачным сервисам и идентифицирует доверенные облачные сервисы в коммерческих целях, особенно для МСП. Ассоциация Сети компетенций Trusted Cloud была основана в середине 2015 г. Федеральным министерством экономики и энергетики Германии (BMWi).

---

1 https://www.gesetze-im-internet.de/bsig_2009/__9.html

2 Немецкая система сертификации берет свое начало в разработанных в ЕС системах сертификации ITSEC (IT Security Evaluation Criteria, Критерии оценки ИТ-безопасности), которые в настоящее время уже не используются, и Common Criteria (Общие критерии оценки ИТ-безопасности) — сертификат, выдаваемый рядом стран, в т. ч. Германией

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itgruene_pdf.pdf?__blob=publicationFile&v=1

4 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifikate-ISO-27001-auf-Basis-von-IT-Grundschutz/zertifikate-iso-27001-auf-basis-von-it-grundschutz_node.html

5 https://rusregister.ru/standards/iso-27001/

6 https://www.bsi.bund.de/EN/Topics/CloudComputing/CloudCertification/CloudCertification_node.html;jsessionid=A7EFE06F90A854193DBC2F2B83F5491A.internet481

7 https://trusted-cloud.de/en/about-trusted-cloud

Одной из целей технологической программы стала разработка и установление знака качества для надежных облачных сервисов – **маркировки Trusted Cloud**. Проект обеспечивает **сертификацию** (**Trusted Cloud Label**) и **каталог для «доверенных» облачных сервисов** через **портал Trusted Cloud**. С помощью каталога можно выбрать вид услуги (IaaS, PaaS, SaaS), применимое к договору право и место размещения ЦОД[1]. Далее можно ознакомиться с каждой услугой: какая сертификация, порядок проведения аудита, SLA, данные о субподрядчиках и др.

**Критерии сертификации Trusted Cloud Label** включают безопасность ИТ и данных, качество и прозрачность, защиту данных и контракты на обслуживание. Таким образом, Trusted Cloud представляет собой полугосударственную систему маркировки поставщиков облачных услуг по стандартам безопасности данных. Trusted Cloud используется как частными заказчиками, так и госорганами.

Среди стандартов безопасности, которые применяются к поставщикам Trusted Cloud, используются Trusted Cloud Datenschutz-Profil für Cloud-Dienste (TCDP) и стандарт Федерального управления информационной безопасностью (BSI) Cloud Computing Compliance Controls Catalogue (C5)[2].

**Стандарты «C5»** (Cloud Computing Compliance Criteria Catalogue, Каталог критериев соответствия облачных вычислений) в первую очередь направлены на крупные и средние предприятия (поставщиков облачных услуг) и ориентированы на ИТ-безопасность и прозрачность[3].

Данные стандарты устанавливают **минимальные требования ИТ-безопасности** для госорганов и организаций, работающих с ними. Аттестация «C5» считается доказательством того, что требования к техническим и организационным мерам в рамках правового регулирования в Германии и GDPR выполнены.

В рамках «C5» предусмотрены требования к функциям безопасности поставщиков облачных услуг (организация информационной безопасности, политика безопасности, работники, физическая безопасность, криптография, идентификация, управление правами, верификация прав, аудит, обработка персональных данных и др.).

«C5» опирается и на международные стандарты в области облачных вычислений (**ISO 27001, ISO 27002, ISO 27017**). Также помимо стандартов ISO, например, в отношении аудита, согласно «C5», действует также международный стандарт **ISAE 3000** (стандарт подтверждения нефинансовой информации), устанавливающий правила процедур аудита, требования к лицам, которые уполномочены его осуществлять; по итогам аудита выдается **сертификат SOC 2** (System and Organization Controls, Системные и организационные методы контроля)[4]. Стоит отметить, что аттестат выдается не BSI, а сертифицированным государственным аудитором.

**Профиль защиты данных Trusted Cloud для облачных служб** (Trusted Cloud Datenschutz-Profil für Cloud-Dienste, TCDP) – это тестовый стандарт, который соответствует требованиям защиты данных Федерального закона о защите данных[5]. С 25 мая 2018 года Закон был заменен Общим регламентом ЕС по защите данных (GDPR).

Это изменило большую часть закона о защите данных, включая требования к обработке данных. Поэтому исследовательский проект AUDITOR в настоящее время разрабатывает стандарт сертификации защиты данных облачных сервисов в соответствии с GDPR. Требуется признание Европейским комитетом по защите данных в соответствии со статьей 42 (5) GDPR. Фонд защиты

1 https://trusted-cloud.de/de/cloud-service-suche

2 https://trusted-cloud.de/en/standards

3 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=3

4 https://www.iaasb.org/publications/isae-3000-revised-assurance-engagements-other-audits-or-reviews-historical-financial-information

5 https://tcdp.de/

данных консультирует консорциум, разрабатывающий стандарт, и может управлять созданным стандартом сертификации.

Помимо этого, чтобы быть **размещенным на Trusted Cloud**, поставщик должен удовлетворять **Каталогу критериев облачных услуг** (Trusted Cloud Kriterienkatalog[1]). Эти критерии определяют минимальные требования, предъявляемые к поставщику облачных услуг, которым он должен соответствовать, чтобы иметь маркировку Trusted Cloud и быть размещенным в каталоге.

Критерии также основываются на стандартах ISO (**ISO 27001, ISO 27002, ISO 27018**). Критерии разделены на несколько блоков, например, функционал предоставляемых услуг, организационная структура провайдера, данные о субподрядчиках и ЦОД, безопасность и безопасность данных, сертификация, SLA, интероперабельность и переносимость и др.

Что касается вопросов страхования, текущее регулирование деятельности поставщиков облачных услуг в Германии не содержит требований о страховании. При этом активно распространяется **добровольное страхование от киберрисков**.

### Вопросы управления персональными данными при создании облаков

В Германии любая (в частности, автоматизированная) обработка персональных данных регулируется GDPR и дополнительными положениями Федерального закона о защите данных (Bundesdatenschutzgesetz) 2018 г.[2]

Если используются облачные решения, данные для входа и другой контент, содержащий персональные данные, которые передаются и обрабатываются поставщиком, то **поставщики облачных вычислений обязаны соблюдать законодательство о защите персональных данных**.

С точки зрения GDPR обычно считается, что пользователь облака является ответственным контролером, принимающим решение об обработке персональных данных, в то время как поставщик облака обрабатывает данные от имени пользователя[3].

Для соблюдения GDPR стороны должны заключить соглашение об обработке данных. Оно включает положения, обязывающие облачного провайдера обрабатывать данные только в соответствии с инструкциями клиента и не привлекать субподрядчиков без согласия клиента.

Чтобы предоставить практическое руководство по использованию решений облачных вычислений в соответствии с Законом о защите данных, Конференция уполномоченных по защите данных федерального правительства и федеральных земель Германии выпустила **Совместное руководство «Облачные вычисления версия 2.0» 2014 г.**, где были обобщены наиболее важные риски при обработке данных в облаке, требования к настройке облачных сервисов и рекомендации по техническим и организационным требованиям[4]. На данный момент Руководство обновляется с учетом GDPR.

В 2021 г. Google совместно с немецкой компанией T-Systems запустили **проект «суверенное облако»**, в рамках которого разрабатываются облачные решения для организаций публичного и частного сектора[5] для обеспечения последними «**суверенитета данных**» – локализации и контроля доступа к данным пользователей на территории ЕС в соответствии с GDPR, Рекомендациями Европейского совета по защите данных о мерах, дополняющих инструменты передачи данных для обеспечения соответствия уровню защиты персональных данных ЕС и о европейских основ-

1 https://trusted-cloud.de/sites/default/files/trusted_cloud_kriterienkatalog_v2_0_en_final_1.pdf
2 https://www.gesetze-im-internet.de/englisch_bdsg/index.html
3 https://www.lexology.com/library/detail.aspx?g=ff94b8d9-e252-4c45-a432-b83789355c95
4 https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf
5 https://fortune.com/2021/09/08/germany-sovereign-cloud-google-t-systems/

ных гарантиях мер в сфере надзора[1]. Данный проект является частным, однако разрабатываемые в его рамках облачные сервисы могут использоваться органами власти.

### Вопросы формирования ценообразования при участии нескольких поставщиков услуг

В Германии органом, осуществляющим закупки в сфере IT для органов власти, является Центральное агентство по закупкам в сфере IT (Zentralstelle IT-Beschaffung, ZIB)[2].

В 2018 г. ZIB был опубликован обновленный **Документ по закупкам и оценке IT-услуг** (Unterlage für Ausschreibung und Bewertung von IT-Leistungen, UfAB) – практическое руководство по осуществлению указанных закупок. Данный документ распространяется в том числе на закупки облачных продуктов.[3]

В соответствии с данным документом **оценка предложений в рамках закупок IT-услуг** осуществляется в 4 этапа:

1. проверка формального соответствия заявок требованиям Закона о государственных закупках (VgV)[4];
2. проверка участников закупки на соответствие требованиям;
3. проверка разумности и достаточности цен с целью выявления неоправданно низких ценовых предложений;
4. оценка заявок с целью выявления наиболее экономичного предложения.

Ценообразование проверяется на 4-м этапе закупок. Оценка может проводиться простым методом (предложению присваиваются баллы на основе его соответствия указанным в документах о закупке требованиям к продукту, таким как качество, технические параметры, эстетика, удобство и доступность использования и др., баллы затем делятся на указанную в заявке стоимость) и расширенным (с добавлением диапазона колебаний результатов, далее проводится «отсеивание» заявок по критерию принятия решения, при этом заранее определяется приоритетный критерий, например цена или соответствие предложения целям закупки). Данный метод используется на первом раунде рассмотрения заявок.

Если проводится второй раунд рассмотрения, простой метод дополняется расширенным. Например, если предложения компаний A и B набрали равное число баллов по соотношению «цена-качество», но при этом цена является приоритетным критерием, на втором раунде будет отобрано предложение с более низкой ценой[5] . Для наглядности применения указанных методов UfAB 2018 дополнен Матрицей оценки[6].

Для закупок облачных сервисов Офисом Федерального Комиссара по информационным технологиям разработан **типовой контракт для закупок**, положения которого устанавливают специальные условия для закупок облачных сервисов по сравнению с обычными контрактами о государственных закупках (EVB-IT Cloud Vertrag)[7].

---

1 https://fortune.com/2021/09/08/germany-sovereign-cloud-google-t-systems/ https://iapp.org/news/a/hard-data-localization-may-be-coming-to-the-eu-here-are-five-concerns/

2 http://www.bescha.bund.de/DE/Beschaffung/ZIB/node.html

3 https://www.cio.bund.de/Web/DE/IT-Beschaffung/UfAB/ufab_node.html

4 https://www.gesetze-im-internet.de/vgv_2016/

5 https://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/ufab_2018_download.pdf?__blob=publicationFile

6 https://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/ufab_2018_bewertungsmatrix_download.xls?__blob=publicationFile

7 https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.

**NB!** В части ценообразования установлено, что услуги облачных сервисов могут оплачиваться в фиксированном размере за каждый месяц предоставления или, если услуга предоставляется по запросу (Leistungen auf Abruf) – за время фактического предоставления (день/час). Также, в сумму оплаты может входить компенсация расходов на предоставление услуг (затраченные часы работы персонала, материальные издержки, иные дополнительные расходы, определяемые индивидуально).

Для поиска тендеров используется **портал service.bund.de** – портал для доступа для граждан, компаний и администраций к тендерам, электронным объявлениям и предложениям о работе федеральных, органов власти земель и местных органов власти[1].

Например, сейчас размещен тендер на облачную инфраструктуру для Федерального института наук о земле и природных ресурсов (Bundesanstalt für Geowissenschaften und Rohstoffe)[2]. Service.bund.de дает первичную информацию о тендере, поэтому для более подробной информации и подачи заявки поставщику необходимо использовать **платформу электронных тендеров e-Vergabe**[3].

Стоит отметить, что в Германии для закупок облачных услуг **планируется использовать рамочные соглашения**[4].

Для облачных услуг был разработан **типовой контракт SLA**[5]. который содержит минимальные условия, например: если заказчик не может самостоятельно определить размер необходимого пространства для хранения данных, то подрядчик предоставляет заказчику достаточное место для использования услуги с учетом возникающих потребностей.

Для обеспечения безопасности подрядчик долен иметь документированную и внедренную концепцию безопасности и систему управления информационной безопасностью в соответствии с **ISO 27001** «Системы обеспечения информационной безопасности», включая аварийное управление.

**Концепция безопасности** формируется по ISO 27017 «Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб», обработка персональных данных должна соответствовать стандарту ISO 27018 «Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки».

html#doc4623280bodyText3

1 https://www.service.bund.de/Content/DE/Service/Ueber-service-bundde/ueber-service-bundde_node.html

2 https://www.service.bund.de/IMPORTE/Ausschreibungen/eVergabe/440865.html?nn=4641482&type=0&searchResult=true&templateQueryString=Cloud

3 https://www.evergabe-online.de/tenderdocuments.html?2&id=440865

4 https://e-beschaffung.bund.de/DE/Wissenswertes/Prozess_EB/Prozess_EB_node.html;jsessionid=9E89B9335AF7167256D1B074A9CC8A46.1_cid325

5 https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html#doc4623280bodyText3

# Авторы проекта

ЛЕВАШЕНКО Антонина (руководитель)

ГИРИЧ Мария (менеджер проекта)

МАГОМЕДОВА Ольга

ЧЕРНОВОЛ Кирилл

ИВАНОВИЧЕВА Кристина