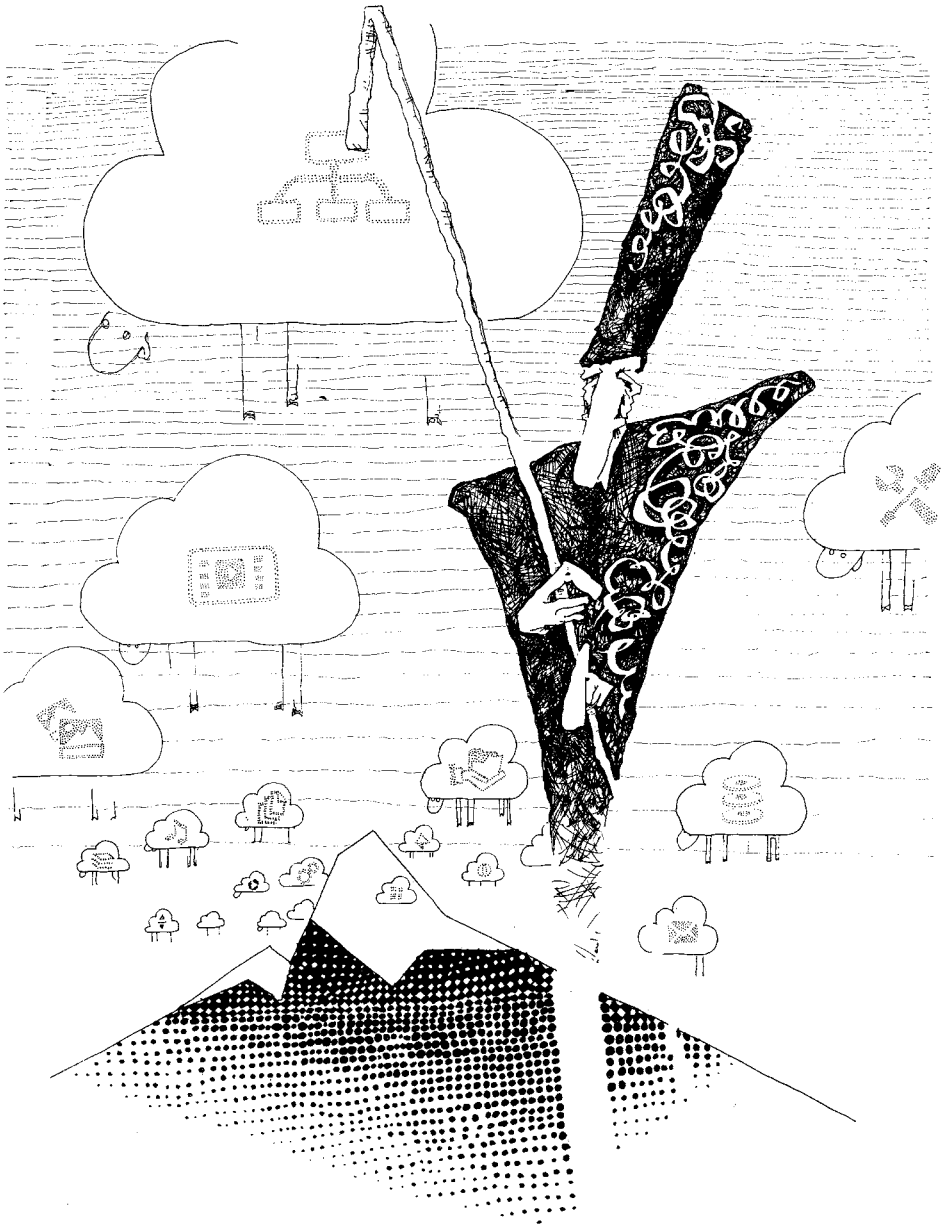
Я наблюдал за облаками...
Облака — вечные изменчивые
странники. Облака — как жизнь...
Жизнь тоже вечно меняется, она так же
разнообразна, беспокойна и прекрасна...
Эрих Мария Ремарк



Стандарты и руководства по использованию облачных вычислений

Для широкого и эффективного внедрения технологий нужны методические и нормативные документы, разъясняющие, в том числе, правовые рамки применения этих технологий, имеющиеся проблемы и риски и способы их минимизации. Облачные технологии – не исключение. Однако многие стандарты, которые сегодня применяются к облачным вычислениям, были разработаны для «дооблачных» технологий, таких как веб-сервисы и Интернет. Поэтому сейчас идет активная разработка стандартов и руководств, предназначенных именно для облачных вычислений.

Традиционно создание нормативно-методической базы начинается с разработки методических документов на национальном уровне. Несколько позже появляются стандарты – национальные, а затем и международные. В данной статье описаны проекты международных стандартов, работа над которыми сейчас идет в рамках Международной организации по стандартизации (ISO). Во многих странах мира разрабатываются стандарты и руководства, содержащие рекомендации по использованию облачных вычислений, и в статье дан их обзор. Основное внимание уделяется вопросам обеспечения информационной безопасности и защите персональных данных.

Наталья Храмцовская
К. и. н., ведущий эксперт по управлению документацией компании «ЭОС», член Гильдии Управляющих Документацией и ARMA International.

Проекты международных стандартов по облачным вычислениям

В настоящее время два технических подкомитета Объединенного технического комитета 1 ИСО (JTC 1) «Информационные технологии» ведут разработку международных стандартов в области облачных технологий. Они работают над следующими проектами:

Проект стандарта ISO/IEC 17788 «Информационные технологии – Распределенные прикладные платформы и сервисы – Облачные вычисления – Общие положения и словарь» (Information technology – Distributed application platforms and services – Cloud computing – Overview and vocabulary). Стандарт описывает концепцию облачных вычислений и содержит ряд терминов и определений. Он станет терминологической основой для дальнейшей работы по стандартизации в сфере облачных вычислений. Официальная публикация стандарта ожидается в четвертом квартале 2014 года.

Проект стандарта ISO/IEC 17789 «Информационные технологии – Облачные вычисления – Эталонная архитектура» (Information technology – Cloud computing – Reference architecture). Стандарт содержит обзор общих понятий и характеристик облачных вычислений, типов облаков, компонент облачных вычислений участвующих сторон, а также взаимоотношений между этими элементами. В нем сделан упор на требования к тому, что должны обеспечивать облачные сервисы, а не на вопросы проектирования и внедрения соответствующих решений. Официальная публикация стандарта ожидается в четвертом квартале 2014 года.

Проект технических спецификаций ISO/IEC TS 27017 «Информационные технологии – Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002[1]» (Information technology – Security techniques – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002). Стандарт содержит рекомендации по обеспечению информационной безопасности при облачных вычислениях. Он будет опираться на пересмотренную версию ISO/

[1]Стандарт ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности). В России действует ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью», идентичный предыдущей редакции этого стандарта 2000 года.

Проект стандарта ISO/IEC 27040 «Информационные технологии – Безопасность хранения данных» (Information technology – Security techniques – Storage security). Стандарт содержит детальные технические рекомендации относительно того, как организациям определить соответствующий уровень мер снижения рисков путем планирования, разработки и реализации системы безопасности при хранении данных. В нем дан обзор общих представлений о безопасности при хранении данных и соответствующие определения, а также рекомендации, касающиеся типичных технологий и сценариев хранения. Стандарт применим при обеспечении безопасности устройств и носителей и относящейся к ним управленческой деятельности; при обеспечении безопасности приложений и сервисов. Также охватываются вопросы безопасности, связанные с конечными пользователями. Этот стандарт имеет косвенное отношение к облачным вычислениям, так как тема хранения данных в облаках затронута в ограниченной степени.

IEC 27002 и будет содержать главным образом рекомендации по реализации многих описанных в этом документе мер информационной безопасности в контексте облачных вычислений. Отдельного стандарта, специфицирующего систему менеджмента информационной безопасности в облаке, не будет, поскольку считается, что вполне достаточно существующего стандарта ISO/IEC 27001[2]. Соответственно, нет и планов по отдельной сертификации информационной безопасности у поставщиков облачных вычислений.

Стандарт выйдет в паре с другим стандартом – ISO/IEC 27018, в котором рассматриваются вопросы защиты персональных данных при использовании облачных вычислений. Это означает, что в ISO/IEC TS 27017 эти вопросы не затронуты.

Проект стандарта ISO/IEC 27018 «Свод практик по мерам защиты персональных данных при оказании публичных облачных услуг» (Code of practice for data protection controls for public cloud computing services). Стандарт предназначен для поставщиков услуг «публичного облака», которые ведут обработку персональных данных (и, возможно, являются операторами персональных данных). Он содержит рекомендации по различным аспектам и элементам защиты персональных данных и неприкосновенности личной информации в публичном облаке. Стандарт не будет дублировать или модифицировать рекомендации стандарта ISO/IEC 27002. В нем будут определены дополнительные цели и меры контроля и управления, связанные с защитой персональных данных в облачной среде.

Стандарт выйдет в паре с ISO/IEC TS 27017 (см. выше), в котором вопросы обеспечения информационной безопасности в облаке рассматриваются в более широкой плоскости.

Стандарты и руководства США

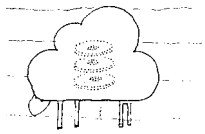
CIO правительства США (U.S. Chief Information Officer) поручил Национальному институту стандартов и технологий (National Institute of Standards and Technology, NIST) взять на себя лидерство в разработке стандартов облачных вычислений. Цель – ускорить развертывание в федеральных органах власти безопасных и эффективных облачных решений, которые позволят снизить затраты и одновременно повысить качество услуг. В NIST была создана специальная рабочая группа по стандартам в сфере облачных вычислений (Cloud Computing Standards Working Group). Она провела обследование существующего ландшафта стандартов. В качестве приоритетных выделили три области:

- информационной безопасности,
- интероперабельности (совместимости);
- требования к переносимости облачных услуг.

Рабочая группа выявила ряд пробелов в имеющихся стандартах, начиная от таких фундаментальных вопросов, как обеспечение безопасности и защиты личной информации, до пользовательских интерфейсов и бизнес-ориентированных функций. Также были сформулированы приоритеты в области стандартизации для нужд правительства США, в частности в области аудита безопасности и соответствия законодательным актам, управления идентификацией и доступом. Как результат этих исследований весной 2011 года рабочая группа опубликовала «Дорожную карту разработки стандартов» [3].

Кроме того, с целью решения беспокоящих руководителей федеральных органов вопросов безопасности в институте создали отдельную рабочую группу по безопасности облачных вычислений.

[2]Стандарт ISO 27001:2005 Information technology – Security techniques – Information security management systems – Requirements («Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования»). В России действует идентичный ему ГОСТ Р ИСО/МЭК 27001-2006.



[3]NIST-SP 500-291 Cloud Computing Standards Roadmap, August 2011.

NIST SP 500–292 «Базовая архитектура облачных вычислений» (Cloud Computing Reference Architecture)[4]. Руководство содержит модель архитектуры и словарь, которые не зависят от поставщика облачных услуг. В нем определены пять ролей (действующих лиц): потребитель услуг, поставщик услуг, брокер, аудитор и оператор. Для них и описаны словарь и базовая архитектура. Переходящим на использование облачных вычислений государственным органам рекомендуется следовать изложенным в руководстве определениям и положениям, чтобы обеспечить согласованное внедрение облачных приложений в рамках федерального правительства.

NIST SP 800–144 «Руководство по обеспечению безопасности и защиты персональных данных при использовании публичных облачных вычислений» (Guidelines on Security and Privacy in Public Cloud Computing)[5]. Руководство содержит обзор проблем в области безопасности и защиты неприкосновенности частной жизни, возникающих при использовании публичных облаков, и рекомендации, которые следует принять во внимание организациям при аутсорсинге данных, приложений и инфраструктуры в среду публичного облака. В аннотации отмечается: «Данный документ дает представление об угрозах, технологических рисках и мерах предосторожности, связанных со средой публичных облачных вычислений. Это должно помочь организациям принимать обоснованные решения относительно использования этой технологии».

«Публичные облака, как и другие модели развертывания облачных вычислений, являются вполне реальным вариантом для многих приложений и услуг, – отметил соавтор документа Тим Гренс[6]. – Тем не менее, ответственность за безопасность и неприкосновенность частной жизни в публичном облаке не может быть делегирована поставщику облачных услуг и остается обязанностью, выполнять которую должна сама организация».

Ключевые рекомендации следующие:

- до внедрения облачных решений тщательно планируйте аспекты их использования, связанные с безопасностью и защитой персональных данных;
- разберитесь в особенностях среды публичных облачных вычислений, предлагаемой поставщиком облачных услуг;
- сделайте так, чтобы облачное решение – как облачные ресурсы, так и размещенные в облачной среде приложения – удовлетворяло требованиям организации к безопасности и защите персональных данных;
- поддерживайте систему подотчетности в отношении защиты персональных данных и приложений и обеспечения их безопасности, внедренную и развернутую в среде публичных облачных вычислений.

В руководстве широко используются перекрестные ссылки, в него включен подробный список федеральных стандартов по обработке информации (Federal Information Processing Standards, FIPS) и специальных публикаций института, содержащих материалы, имеющие непосредственное отношение к облачным вычислениям и рекомендуемые для использования совместно с SP 800–144 (это уже стало отличительной чертой отчетов NIST по облачной тематике). Таким образом подчеркивается, что один из недостатков масштабного производства стандартов институтом: документы часто взаимно дополняют друг друга и их лучше читать и использовать совместно. В руководстве перечислено не менее пятнадцати других специальных публикаций, которые «особенно актуальны в области облачных вычислений и поэтому должны использоваться совместно с настоящим документом».

Требования к поставщикам облачных услуг для государственных органов. В рамках федеральной программы управления рисками и авторизацией (Federal Risk and

[4]Fang Liu, Jin Tong, Jian Mao, Robert B. Bohn, John V. Messina, Mark L. Badger, Dawn M. Leaf, September 2011.

[5]Timothy Grance and Wayne Jansen, December 2011.

[6]Пресс-релиз, выпущенный NIST 24 января 2012 года по поводу выхода руководства.

Многие стандарты, которые сегодня применяются к облачным вычислениям, были разработаны для «дооблачных» технологий, таких как веб-сервисы и Интернет

Authorization Management Program, FedRAMP), предназначенной для отбора поставщиков услуг облачных вычислений для государственных органов, федеральное правительство США установило порядка 170 мер по обеспечению безопасности.

Отобранные меры безопасности согласованы с рекомендациями, содержащимися в 3-й редакции специальной публикации NIST SP 800–53 «Рекомендуемые меры безопасности для федеральных информационных систем и организаций»[7] для систем, инциденты в которых способны оказать небольшое или умеренное воздействие на деятельность и активы государственных органов. Чтобы получить разрешение на оказание облачных услуг федеральным органам государственной власти, поставщики обязаны реализовать у себя эти меры безопасности.

Порядок реализации мер безопасности FedRAMP детализирован в ряде документов, которые были выпущены 2013 году:

- «План обеспечения безопасности системы» (System Security Plan)[8]. Документ разъясняет, каким образом требования, связанные с каждой из мер безопасности, должны выполняться в среде облачных вычислений. Он готовился в соответствии с руководством NIST SP 800–18 «Руководство по разработке планов обеспечения безопасности ИТ-систем»[9];
- «Шаблон плана оценки безопасности» (Security Assessment Plan)[10] Документ подробно описывает, как будет оцениваться и проверяться каждая из реализованных мер, чтобы обеспечить ее соответствие требованиям;
- «Шаблон отчета об оценке безопасности» (Security Assessment Report)[11]. В документе разъясняются проблемы, выводы и рекомендации по итогам оценок мер безопасности, описанных в плане оценки безопасности.

Эти документы согласованы с публикацией NIST SP 800–37 «Концепция управления рисками»[12]. Правительство США не позволит федеральным органам власти использовать услуги поставщика облачных вычислений до тех пор, пока тот не представит доказательства того, что его меры безопасности проверены и одобрены аккредитованной при программе FedRAMP организацией.

Национальный институт стандартов и технологий (NIST) выделил три приоритетные области стандартизации: информационную безопасность, интероперабельность (совместимость) и требования к переносимости

Проект NIST SP 500–299 «Базовая архитектура обеспечения безопасности облачных вычислений» (Cloud Computing Security Reference Architecture). Документ дополняет руководство NIST SP 500–292 «Базовая (референсная) архитектура облачных вычислений» полномасштабной моделью безопасности. Эта модель определяет базовый набор компонент обеспечения безопасности, рекомендуемых для создания успешных и надежных экосистем облачных вычислений. Документ помогает понять взаимозависимость действующих лиц для обеспечения безопасности облачных сервисов, а также разобраться с требованиями, которые должны сформулировать группы технического планирования и внедрения органов исполнительной власти, чтобы обеспечить приобретение облачных сервисов с уровнями безопасности, соответствующими потребностям.

Руководства Евросоюза и европейских стран

Евросоюз: «Безопасность и жизнеспособность в государственных облаках: принятие взвешенных решений» (Security & Resilience in Governmental Clouds: Making an Informed Decision)[13]. Руководство Европейского агентства по сетевой и информационной безопасности ENISA (European Network and Information Security Agency) по использованию облачных вычислений государственными органами. Руководство адресовано тем высшим руководителям государственных органов, которые должны принимать решения о том, как использовать облачные вычисления с точки зрения обеспечения безопасности и непрерывности деятельности. Основная задача документа – помочь государственным ор-

[7]NIST SP 800-53 R3 Recommended Security Controls for Federal Information Systems and Organizations.

[8]Version 1.0, January 2013.

[9]NIST Special Publication 800-18 Revision 1Guide for Developing Security Plans for Information Technology Systems.

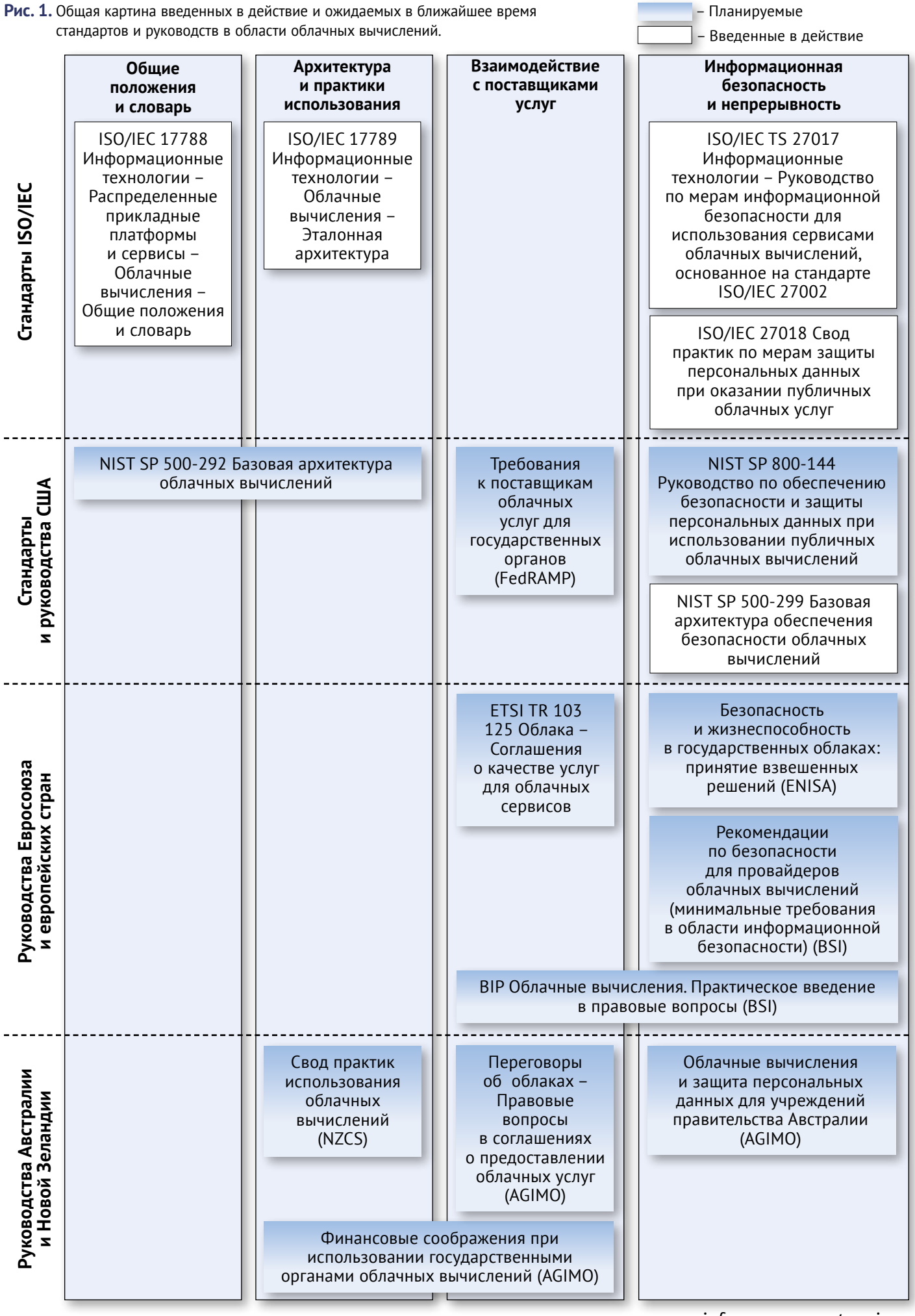
[10]Version 1.0, January 2013.

[11]May 2013.

[12]NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

[13]ENISA, January 2011.

Рис. 1. Общая картина введенных в действие и ожидаемых в ближайшее время стандартов и руководств в области облачных вычислений.



ганам принять обоснованные решения на основе оценки рисков в области безопасности данных, непрерывности получения услуг и исполнения существующих законодательно-нормативных требований. В отчете рассмотрены плюсы и минусы с точки зрения безопасности и непрерывности коллективных, частных и публичных облачных услуг в плане их использования государственными органами.

«В новом отчете высшим руководителям предлагается модель принятия решений, помогающая выбрать оптимальное облачное решение с точки зрения безопасности и непрерывности»,– отмечает автор документа Даниэль Катеду (Daniele Catteddu). В отчете подробно описаны и разъяснены различные элементы модели принятия решения. Применение модели продемонстрировано на четырех примерах оказания услуг: услуги электронного здравоохранения, электронные административные процедуры, электронная почта и приложения для управления кадрами. Анализ и выводы основаны главным образом на трёх сценариях, описывающих переход на облачные вычисления органа здравоохранения, органа муниципальной власти, а также создание инфраструктуры государственного облака.

В настоящее время использование публичных облачных сервисов должно ограничиваться приложениями, не требующими конфиденциальности информации и/или не являющимися критически важными

Авторы руководства делают вывод о том, что частные и коллективные облака, по всей видимости, являются решениями, наилучшим образом соответствующими потребностям тех государственных органов, которым необходимо достичь максимально высокого уровня управления данными. В то же время отмечают, что если инфраструктура частного или коллективного облака не наберет необходимой «критической массы», то большинство достоинств облачной модели в плане устойчивости и живучести не будет реализовано.

Исполнительный директор агентства ENISA профессор Удо Хельмбрехт (Udo Helmbrecht) комментирует: «Публичное облако обеспечивает очень высокий уровень доступности услуг и является наиболее экономически эффективным. Тем не менее, в настоящее время его использование должно ограничиваться приложениями, не требующими конфиденциальности информации и/или не являющимися критически важными в рамках четко определенной стратегии освоения облачных вычислений, включающей четко сформулированную стратегию выхода из облака».

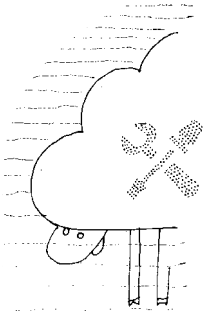
В докладе содержится ряд рекомендаций для государственных органов, в том числе: «Облачные вычисления скоро будут обслуживать значительную часть граждан Евросоюза, малых и средних предприятий и органов государственной власти. В этой связи национальные правительства должны разработать стратегию использования облачных вычислений и изучить роль, которую эти вычисления будут играть с точки зрения защиты важнейших элементов информационной инфраструктуры».

Евросоюз: Технический отчет ETSI TR 103 125 «Облака – Соглашения о качестве услуг для облачных сервисов» (Technical Report Cloud; SLAs for Cloud services)[14]. Технический отчет опубликован Европейским институтом телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI). В предисловии к документу отмечается: «Соглашения о качестве услуг (Service Level Agreements, SLA), которые широко используются операторами связи и поставщиками услуг для широкого спектра телекоммуникационных услуг (как оплачиваемых «по факту», так и на основе подписки). Такого рода соглашения хорошо известны в этом сообществе, и накоплен обширный опыт в отношении их структуры, содержания и последствий как для поставщиков, так и для потребителей услуг. Эти соглашения являются основой для контрактов, в них сформулированы ожидания потребителей при получении услуг и компенсации в случае невыполнения поставщиком его обязательств. По историческим причинам соглашения о качестве услуг менее распространены в сфере ИТ, где модели предоставления услуг появились сравнительно недавно. Исключением был ИТ-аутсорсинг, но в этих сценариях соглашения

[14] ETSI TR 103 125 v1.1.1, ноябрь 2012.

о качестве услуг, как правило, формулировались исходя из конкретных условий и были рассчитаны на то, чтобы обеспечивать длительную передачу ответственности за операции от клиента третьей стороне».

Авторы документа отмечают, что у предложений облачных сервисов есть определенное сходство в функциональных возможностях, особенно при оказании услуг по модели «инфраструктура как услуга» (Infrastructure as a Service, IaaS), но вопросы качества и правила и условия оказания услуг у каждого поставщика могут определяться и формулироваться по-разному. Поскольку переход на использование облачных услуг потенциально несет серьезные риски для оперативной деятельности и управления, то отсутствие ясности относительно деталей предлагаемых услуг представляет проблему.



Документ задуман как «практическое пособие, помогающее руководителям, принимающим в организациях решения по бизнес- и ИТ-вопросам, анализировать и учитывать соглашения о качестве обслуживания, предлагаемые различными поставщиками облачных услуг». В нем приводятся проблемы, с которыми сталкиваются потенциальные потребители облачных услуг. Основной упор делается на услуги, связанные с предоставлением физических хранилищ, вычислительных и сетевых ресурсов (IaaS), хотя отчасти положения отчета применимы и к другим моделям предоставления облачных услуг.

Отчет содержит обзор существующих стандартов ETSI, связанных с качеством телекоммуникационных услуг (включая соглашения о качестве услуг) в контексте особенностей облачных услуг. Это сделано с целью выяснить, в какой степени данные стандарты остаются применимыми, а где требуются новые стандарты, специфические для облачных вычислений.

Германия: Рекомендации по безопасности для провайдеров облачных вычислений (минимальные требования в области информационной безопасности). Документ разработан Федеральным управлением по безопасности информационных технологий (Bundesamt für Sicherheit in der Informationstechnik, BSI)[15]. Он содержит минимальные требования к обеспечению информационной безопасности при использовании облачных услуг. Согласно BSI, документ представляет собой «свод хорошей практики».

[15]Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit), Bundesamt für Sicherheit in der Informationstechnik, Februar 2012.

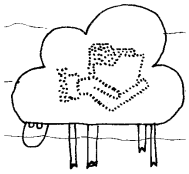
Великобритания: BIP 0117 «Облачные вычисления. Практическое введение в правовые вопросы» (Cloud Computing. A Practical Introduction to the Legal Issues)[16]. Руководство опубликовано Британским институтом стандартов (BSI), однако не имеет статуса национального стандарта. Документ знакомит (вкратце) с облачными вычислениями тех, кто впервые сталкивается с этой концепцией, и сравнивает развитие этой новой парадигмы вычислений с другими способами приобретения вычислительных ресурсов. В нем суммируются возникающие правовые проблемы, часть которых характерна для облачных вычислений, а другие имеют более общий характер, но специфически проявляются в отношении «облаков».

[16]Автор – юрист Ренцо Марчини (Renzo Marchini), ноябрь 2010 года.

Тем, кто участвует в закупке ИТ-технологий, часто требуется оценить возникающие правовые проблемы и понимать, каким образом можно свести их к минимуму в контрактах. С другой стороны, как поставщикам услуг облачных вычислений реагировать на правовые вопросы, беспокоящие их клиентов? В публикации рассматриваются эти правовые вопросы, охватывающие такие области, как безопасность в «облаках», защита персональных данных, уровни обслуживания и контрактные вопросы. Руководство является полезным практическим документом для тех, кто закупает или предоставляет облачные услуги, определяя практические шаги, направленные на решение правовых вопросов как в области исполнения законодательно-нормативных требований, так и в области договорных отношений между клиентами и поставщиками. Рассматриваются также вопросы, возникающие при использовании облачных услуг организациями, работающими в жестко регулируемых отраслях, таких как сфера финансовых услуг.

Основное внимание в стандартах и руководствах уделяется вопросам обеспечения информационной безопасности и защите персональных данных

Руководства Австралии и Новой Зеландии



Австралия: Руководства области облачных вычислений. В феврале 2012 года департамент управления информацией правительства Австралии (Australian Government Information Management Office, AGIMO) выпустил три руководства в области облачных вычислений:

- «Облачные вычисления и защита персональных данных для учреждений правительства Австралии» (Privacy and Cloud Computing for Australian Government Agencies);
- «Переговоры об облаках – Правовые вопросы в соглашениях о предоставлении облачных услуг» (Negotiating the Cloud – Legal Issues in Cloud Computing Agreements);
- «Финансовые соображения при использовании государственными органами облачных вычислений» (Financial Considerations for Government use of Cloud Computing).

Глен Арчер (Glen Archer), первый помощник секретаря отделения AGIMO по вопросам политики и планирования, отметил: «Руководства были разработаны с целью отобразить ответственность и обязанности органов государственной власти, вытекающие из закона об управлении финансами и подотчетности, в контексте австралийской нормативно-правовой среды».

Руководства говорят о необходимости постоянного мониторинга и контроля использования облачных услуг, ежедневного анализа счетов и отчетов. Это поможет избежать скрытых «накруток» и зависимости от поставщиков облачных услуг

Руководства говорят о необходимости постоянного мониторинга и контроля использования облачных услуг посредством ежедневного анализа счетов и отчетов. Это поможет избежать скрытых «накруток» и попадания в зависимость от поставщиков облачных услуг. AGIMO отмечает, что «государственные органы должны сделать так, чтобы контракт с поставщиком облачных услуг не привел к зависимости государственного органа от поставщика за пределами срока действия договора».

В руководстве **«Облачные вычисления и защита персональных данных для учреждений правительства Австралии»** особое внимание уделено вопросам обеспечения неприкосновенности частной жизни и безопасности при хранении данных. Руководство содержит контрольный список связанных с персональными данными вопросов, о которых агентство должно подумать при рассмотрении возможности перехода «в облака». Также в нем отмечается, что «последствия для защищенности персональных данных зависят от того, как они [облачные вычисления] используются. Тем не менее, при использовании облачных вычислений могут возникнуть риски для персональных данных, поскольку возможно ослабление контроля над тем, как персональные данные обрабатываются поставщиком облачных вычислений и как к ним предоставляется доступ третьим сторонам».

В руководстве **«Переговоры об облаках – Правовые вопросы в соглашениях о предоставлении облачных услуг»** содержится обзор основных правовых проблем, связанных с облаками, например, защита информации, ответственность, управление производительностью, прекращение соглашения, разрешение споров и др. Также обсуждаются последствия перехода на облачные вычисления для защиты персональных данных и безопасности.

Последнее, третье руководство **«Финансовые соображения при использовании государственными органами облачных вычислений»** охватывает следующие темы:

- финансовые вопросы, связанные с закупками и проведением переговоров по контракту;
- анализ рынка и конкуренции на рынке;
- платежи, связанные с началом и прекращением договора;

- переход финансирования из капитального бюджета в бюджет операционных расходов.

В нем обсуждаются требования к облакам и данные, которые понадобятся для выбора облачной платформы, наилучшей с точки зрения хранения, безопасности и надежности. Руководство предупреждает, что «одним из ключевых финансовых вопросов, стоящих перед государственными органами при переходе на облачные решения, является перемещение выделяемого государственному органу соответствующего финансирования из капитальных затрат в операционные расходы».

Новая Зеландия: «Свод практик использования облачных вычислений» (Cloud Computing Code of Practice). Опубликован Компьютерным обществом Новой Зеландии (New Zealand Computer Society, NZCS). Цель документа – дать возможность профессиональным поставщикам облачных услуг с помощью общепризнанной третьей стороны продемонстрировать и провести оценку своей практики, процессов и этики, с тем чтобы завоевать доверие потенциальных клиентов. Поставщики услуг могут решить эту задачу, выполнив содержащиеся в «Своде» требования и получив подтверждение соответствия в виде права на использование специального обозначения и включения в реестр поставщиков облачных вычислений, соответствующих требованиям.

Руководство также полезно конечным пользователям, так как поможет им принять обоснованные решения благодаря раскрытию поставщиком сведений о практике оказания услуг. Это позволит пользователям доверять поставщику услуг и его способности удовлетворить их потребности. По сути дела, основная часть документа представляет собой форму для раскрытия сведений о процессах поставщика услуг, где он должен заполнить определенные поля и/или выбрать определенные варианты ответов. Из этой формы видно, какие вопросы пользователю следует задавать при выборе поставщика услуг облачных вычислений.

Заключение

Облачные технологии, как и любые другие технологии, не являются «хорошими» или «плохими». У них большой потенциал, но при их применении можно столкнуться с рядом проблем. Задача организаций при работе в облаках заключается в том, чтобы максимально использовать преимущества облачных вычислений, избегая при этом рисков. Для того чтобы перевод деятельности в облака дал ожидаемые результаты, нужно создать соответствующую нормативно-правовую и методологическую базы, поэтому на формирование таких баз, в том числе с учетом накопленного зарубежного опыта, следует обратить самое серьезное внимание. Изучение и активное использование международных и национальных стандартов и руководств в этой области позволит сократить сроки разработки отечественных документов, повысить их качество и гармонизировать с мировой практикой.