УДК 004.056.5: 006.03 **DOI 10.52167/1609-1817-2024-131-2-393-403**

Е.Ж.Айтхожаева✉, Э.В.Ким
Satbayev University, Алматы, Казахстан
E-mail: ait_djam@mail.ru

СТАНДАРТИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

Аннотация. С расширением сферы применения облачных сервисов возрастает их уязвимость к различным видам киберугроз. Риски безопасности в облачных сервисах разнообразны и достаточно велики, представляют большую потенциальную опасность для критических данных. В решении этой проблемы ведущая роль принадлежит стандартизации. Данная работа посвящена исследованию и анализу сферы стандартизации информационной безопасности облачных сервисов. Приводятся статистические данные исследований международных агентств (Gartner, Palo Alto, VK Cloud Solutions, ИКС Медиа) в сфере использования облачных сервисов и их информационной безопасности. Рассматриваются основные определения и понятия, связанные со стандартизацией облачных сервисов и их информационной безопасностью. Выполнен анализ рынка облачных технологий. Выполняется обзор и анализ ключевых организаций и ассоциаций, занимающихся разработкой стандартов в этой сфере, указывается их область деятельности и вклад в формирование безопасной и надежной облачной инфраструктуры. Особое внимание уделяется рассмотрению существующих международных и признанных мировым сообществом национальных стандартов информационной безопасности облачных сервисов. Затронут вопрос стандартизации информационной безопасности облачных сервисов в Республике Казахстан.

Ключевые слова. Облачные сервисы, информационная безопасность, стандартизация, международные стандарты, национальные стандарты.

Введение.

Применение облачных технологий является одним из компонентов достижения целей устойчивого развития (ЦУР – утверждены на конференции ООН в 2015 году), предоставляя равные и широкие возможности в области хранения, обработки данных и предоставления множества услуг любому пользователю независимо от пола, национальной принадлежности, гражданства и степени развития государства, способствует снижению уровня неравенства внутри стран и между ними. Облачные сервисы предлагают практически все общепризнанные ИТ-вендоры. Однако при использовании облачных сервисов возникают новые значимые риски, связанные с информационной безопасностью данных: конфиденциальностью, целостностью и доступностью информации. Поэтому необходимо понимать и учитывать уязвимости облачных сервисов к различным видам угроз и атак злоумышленников, что требует повышенного внимания к проблеме информационной безопасности облаков.

Общепризнано, что при переходе в облака главными критериями при выборе облачных сервисов для организаций, работающих с критической информацией, служат надежность и безопасность предоставления услуг хранения и обработки данных. В настоящее время, с точки зрения этих критериев, доверие к облачным сервисам намного выросло. Как показало исследование ИКС Медиа и VK Cloud Solutions, 81% компаний рассматривают облачные сервисы, как надежное решение для хранения данных бизнеса. Считается, что облачные системы имеют защитные контуры на всех уровнях, что

привлекает и дает уверенность организациям и компаниям в плане обеспечения информационной безопасности критических данных [1].

Тем не менее, исследование Palo Alto Unit 42 выявило проблемы, связанные с неправильной конфигурацией управления идентификацией и доступом (IAM) в облачных средах. Анализ 680 тыс. удостоверений и более чем 200 организаций показывает, что 99% облачных пользователей предоставляют необоснованно расширенные разрешения, которые длительное время не используются. Это создает потенциальные угрозы безопасности, так как злоумышленники, используя эти разрешения, имеют возможность расширять сферы действия атак. В исследовании указывается, что удаление неиспользуемых разрешений приведет к снижению риска угроз для облачных ресурсов и при этом область атаки минимизируется. Ошибки в настройках IAM являются причиной 65% обнаруженных инцидентов информационной безопасности в облаке, что указывает на необходимость тщательного управления доступом и идентификацией в облачных средах [2].

Но не только конкретная конфигурация управления идентификацией и доступом, а также и тип сервиса, и используемая модель облака (частное, коллективное/общественное, публичное/общедоступное, гибридное облако) в значительной мере влияют на уровень потенциального ущерба, который будет иметь организация в результате последствий рисков, имеющих место в облачных сервисах. Решение проблемы снижения рисков и минимизации возможных ущербов обеспечивается активным внедрением стратегии безопасности. Стратегия безопасности – это не только правильное управление IAM, но и использование многих разнообразных механизмов, как традиционно используемых для обеспечения безопасности не только в облачных средах, так и специфических механизмов. Регулярное резервирование данных и проведение аудитов безопасности, использование шифрования данных – это азбука информационной безопасности. А одно из главных условий поддержания информационной безопасности – это обеспечение соблюдения соответствующих нормативных и законодательных требований и стандартов.

В современном информационном пространстве, где постоянно появляются новые угрозы, классические угрозы совершенствуются и усложняются, стандартизация играет важную роль в обеспечении эффективной защиты данных и обеспечении надежности облачных услуг, так как в них нашли отражение лучшие практики, техники, процедуры и требования информационной безопасности мирового сообщества.

Стандартизация информационной безопасности – это процесс разработки и соблюдения унифицированных стандартов и нормативов в области информационной безопасности. Целью стандартизации является обеспечение единых требований и методологий для защиты информации и информационных услуг от угроз и рисков. Это относится и к облачным сервисам.

Стандарт информационной безопасности — это установленный набор норм, правил, и требований, разработанных для обеспечения защиты информации и данных от угроз, а также для управления рисками в области информационной безопасности. Эти стандарты создаются с целью предоставления организациям и индивидуальным пользователям тактик, техник, принципов и методов для обеспечения конфиденциальности, целостности и доступности информации. Стандарты информационной безопасности включают в себя рекомендации по управлению и защите данных, принципы аутентификации и авторизации, требования к физической и логической безопасности, а также меры по предотвращению и реагированию на кибератаки.

Международный стандарт — это документ с правилами, нормами или требованиями, разработанный международными организациями и утвержденный с участием представителей различных стран. Эти стандарты разрабатываются с целью

обеспечения единого подхода и согласованности в различных областях, чтобы облегчить взаимодействие и обмен информацией между участниками из разных стран. Примером международных организаций, разрабатывающих международные стандарты, являются: Международная организация по стандартизации - МОС (International Organization for Standardization - ISO) и Международная электротехническая комиссия – МЭК (International Electrotechnical Commission - IEC).

Национальный стандарт – это стандарт, принятый уполномоченным органом по стандартизации конкретного государства и действующий на его территории.

Материалы и методы.

В результате анализа данных за 2022 год объем глобального рынка предоставляемых облачных сервисов достиг уровня $478,32 млрд. Исследование, проведенное американской исследовательской и консалтинговой компанией Gartner и представленное 13 ноября 2023 года, выявило, что наибольший сегмент отрасли принадлежат решениям SaaS (программное обеспечение как услуга) [3].

В течение 2022 года сфера SaaS принесла доход в объеме $174,42 миллиарда. Вторым по размеру сегментом оказались услуги IaaS (инфраструктура как услуга) с объемом $120,33 млрд, за которым следуют службы PaaS (платформа как услуга) с результатом $119,58 млрд. В отчете Gartner обращается внимание на развитие таких облачных сервисов, как "бизнес-процессы как услуга" (BPaaS) и "десктоп как сервис" (DaaS). Статистика показывает, что BPaaS и DaaS становятся все более востребованными в сфере бизнеса (см. табл. 1).

Таблица 1 – Сравнительный прогноз расходов конечных пользователей на облачные услуги по всему миру (в миллионах долларов США) [3]

Типы облачных сервисов	**2022 г.**	**2023 г.**	**2024 г.**
Облачные сервисы инфраструктуры приложений (PaaS)	119 579	145 320	176 493
Облачные сервисы приложений (SaaS)	174 416	205 221	243 991
Облачные сервисы бизнес-процессов (BPaaS)	61 557	66 339	72 923
Облачные услуги виртуальных рабочих столов (DaaS)	2 430	2 784	3 161
Облачные сервисы инфраструктуры систем (IaaS)	120 333	143 927	182 222
Итого	**478 315**	**563 592**	**678 790**

Как отмечается в отчете Gartner, генеративный искусственный интеллект (GenAI) начинает все сильнее влиять на развитие рынка публичных облаков. Проекты в этой сфере требуют высокопроизводительных вычислительных ресурсов с возможностью масштабирования. К тому же организации, внедряющие GenAI, выдвигают дополнительные требования к облачным провайдерам. Требования касаются, помимо стоимости, усиленной безопасности (конфиденциальность и целостность данных, суверенитет).

В отчете указывается, что все больше появляется отраслевых облачных платформ, которые объединяют в себе услуги SaaS, PaaS и IaaS, предоставляя комплексные решения с настраиваемыми возможностями. Прогноз Gartner: к 2027 году более 70% предприятий будут использовать отраслевые облачные платформы для ускорения своих бизнес-операций (в настоящее время этот показатель составляет менее 15%).

Согласно прогнозам Gartner, рынок облаков продолжит расти, с общими затратами, ожидаемыми к 2024 году, в объеме $678,79 млрд. Сервисы SaaS, IaaS и PaaS продолжат быть лидерами. Увеличение роста прогнозируется во всех сегментах облачного рынка,

особенно в IaaS и PaaS, что свидетельствует о росте интереса и доверия к облачным технологиям [3].

В сфере информационной безопасности облачных сервисов важное место занимают организации, занимающиеся стандартизацией. Эти организации разрабатывают документы, которые определяют требования и методологии в области безопасности информации, что способствует развитию единых стандартов и нормативов. Диапазон документов обычно широк: начиная с базовых стандартов безопасности и до создания руководящих принципов для обеспечения конфиденциальности, целостности и доступности данных в облачных средах.

Ниже представлен обзор основных организаций, признанных мировым сообществом, занимающихся стандартизацией облачных систем и их безопасности, выявлена их сфера деятельности, указан их вклад в формировании безопасной и надежной облачной инфраструктуры.

Национальный институт стандартов и технологий США (The National Institute of Standards and Technology - NIST) — это агентство США, подразделение Министерства торговли, которое играет ключевую роль в разработке стандартов и рекомендаций для различных отраслей, включая область информационной безопасности. Относительно облаков: NIST создало несколько важных документов, которые служат основой для безопасности облачных систем. NIST также объявило и инициировало процесс Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC), который был разработан для поддержки внедрения облачных вычислений в переходный период [4].

Open Cloud Consortium (OCC) – некоммерческая организация, созданная в 2008 году с целью поддержки исследований в области облачных вычислений. Ее основная задача заключается в обеспечении открытого доступа к облачным ресурсам для исследовательских проектов. OCC объединяет учреждения и лаборатории, предоставляя ученым доступ к обширным вычислительным ресурсам и ресурсам хранилища. Организация активно участвует в проектах и исследовательских инициативах, направленных на развитие облачных технологий, и способствует установлению технических стандартов в этой области. Помимо этого, OCC поддерживает сотрудничество с научным сообществом, поддерживает распространение знаний и проведение научных исследований в области облачных вычислений.

Организация по совершенствованию стандартов структурированной информации (Organization for the Advancement of Structured Information Standards - OASIS) – международный консорциум, объединяющий представителей более 600 организаций из 100 стран и активно продвигающий различные облачные протоколы и стандарты, в том числе и с ориентацией на электронную коммерцию. Ниже некоторые из основных проектов, поддерживаемых OASIS: CAMP (Cloud Application Management for Platforms) для взаимодействия облачных платформ, IDCLOUD (Identity in the Cloud) для решения вопросов управления идентификацией в целях безопасности, TOSCA (Topology and Orchestration Specification for Cloud Application) для повышения переносимости облачных приложений и сервисов, а также CloudAuthZ (Cloud Authorization) для доставки контекстно-зависимых атрибутов в режиме реального времени в точки мониторинга соблюдения политик. Документ PACR (Public Administration Cloud Requirements) определяет атрибуты и требования по администрированию публичных (общедоступных) облаков, необходимые для эффективного функционирования облачных вычислений в области государственного управления.

Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC) играют важную роль в стандартизации облачных вычислений, разрабатывая международные стандарты и рекомендации для обеспечения единых подходов и методов в этой области. В рамках стандартизации облачных

вычислений ISO/IEC принимают участие в разработке стандартов, которые охватывают различные аспекты, такие как безопасность, управление сервисами, интероперабельность и другие.

SNIA (Storage Networking Industry Association) – это организация, созданная для развития стандартов и технологий в области сетевого хранения данных. В рамках облачных вычислений SNIA внесла значительный вклад через свои инициативы, такие как SNIA Cloud Data Management Interface (CDMI), ориентированный на управление данными в облачных хранилищах, и SNIA Swordfish, обеспечивающий стандартизированный интерфейс для управления хранилищами данных в облаке.

Организация Cloud Auditing Data Federation Working Group (CADF) работает над стандартизацией событий аудита для всех поставщиков облаков и услуг в целях решения проблем в облачных системах, связанных с несоответствием или несовместимостью. CADF стремится обеспечить правильное управление и соблюдение политик безопасности для потребителей систем облачных вычислений. Организации принадлежит стандарт DMTF CADF – модель событий аудита для облачных вычислений.

The Cloud Standards Customer Council (CSCC) - это команда сторонников конечных пользователей, ориентированная на ускорение принятия облаков пользователями. Уделяет особое внимание стандартам, безопасности и взаимодействию облачных сервисов. Работа организации заключается в: содействии снижению барьеров для широкого использования облачных сервисов; разработке лучших практик, руководств и дорожных карт стандартов по вопросам облачных вычислений, в том числе и безопасности; взаимодействии с организациями по разработке стандартов и участию в процессах разработки новых стандартов для облаков; ускорению и пониманию обмена реальными практиками, процедурами и техниками [5].

Деятельность организации Open Cloud Standards Incubator нацелена на помощь в организационном взаимодействии между коллективными/общественными, частными, публичными и гибридными облаками. Основная цель Open Cloud Standards Incubator - способствовать развитию открытых стандартов, которые обеспечивают безопасность, надежность и взаимодействие различных облачных сервисов.

Technical Committee Cloud (TC CLOUD) — это подразделение Европейского института телекоммуникационных стандартов (European Telecommunications Standards Institute - ETSI), которое занимается разработкой стандартов для облачных технологий. Его деятельность ориентирована на безопасность, интероперабельность и управление ресурсами в облачной среде с целью создания некоммерческих и действенных технических спецификаций для индустрии.

Cloud Security Alliance (CSA) - международная некоммерческая организация, ориентированная на обеспечение безопасности в облачных вычислениях, основана в 2008 году. В состав CSA входят эксперты, профессионалы и организации с целью разработки стандартов, на основе лучших практик, в области безопасности облачных технологий. CSA инициировала ряд проектов, включая Security, Trust & Assurance Registry (STAR) и Cloud Controls Matrix (CCM). В CCM представлен набор контрольных мер для обеспечения безопасности в облачных средах. STAR предлагает оценку безопасности облачных провайдеров, которая поможет пользователям облачных сервисов выбрать облачного провайдера. Организация активно работает и в области образования специалистов по облачной безопасности.

EuroCloud представляет собой европейскую ассоциацию, посвященную облачным технологиям и услугам. Она объединяет предприятия, занимающиеся облачными вычислениями, с целью содействия развитию, внедрению и популяризации облачных технологий в европейских странах. EuroCloud активно работает над стандартизацией в

сфере облачных технологий, предлагая правила и рекомендации для улучшения совместимости и безопасности.

Международный союз электросвязи (International Telecommunication Union - ITU) — это международная организация, объединяющая государства и компании для разработки стандартов и регулирования в области телекоммуникаций. ITU был создан в 1865 году и является специализированным агентством Организации Объединенных Наций. Сектор стандартизации телекоммуникации (ITU-T), входящий в состав организации ITU, разработал ряд стандартов и рекомендаций в области безопасности облачных сервисов, в том числе и распределенных: Cloud computing Infrastructure requirements, Requirements for desktop as a service (DaaS), Framework for inter-cloud computing, Overview and high-level requirements of distributed cloud, Security framework for cloud computing, Cloud Computing Framework & high-level requirements и др. [6].

Результаты.

Ниже представлен обзор нескольких основных стандартов информационной безопасности, ориентированных на облачные сервисы. Включены как международные стандарты, такие как ISO/IEC 27017 и ISO/IEC 27018, так и широко признанные национальные стандарты NIST.

ISO/IEC 27017:2015 Information technology - Security Techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Международный стандарт, предоставляющий рекомендации по управлению информационной безопасностью облачных сервисов на основе стандарта ISO/IEC 27002. Стандарт разработан к применению как для поставщиков облачных услуг (CSP), так и для конечных пользователей, с целью обеспечения безопасности облачной среды, путём внедрения дополнительных контрольных мер и рекомендаций, ориентированных на специфические аспекты безопасности в облачных средах. Стандарт включает в себя набор руководящих принципов и механизмов контроля, которые организации могут применять при использовании облачных услуг. Он предоставляет конкретные рекомендации по безопасному использованию облачных сервисов, охватывая такие аспекты, как управление доступом, шифрование данных, мониторинг, управление инцидентами и другие. В настоящее время находится в стадии разработки новая версия стандарта [7].

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Это международный стандарт с рекомендациями и практиками по управлению информационной безопасностью в облачных услугах с учетом защиты персональных данных. В центре внимания стандарта ISO/IEC 27018 - обеспечение конфиденциальности при обработке персональных данных в облачных средах. Основные положения стандарта включают в себя меры по контролю и защите персональных данных, обработка которых осуществляется в облаке. В нем определены требования к облачным поставщикам услуг для обеспечения прозрачности и контроля над данными клиентов, в том числе меры по шифрованию, обеспечению доступности, а также регулированию субподрядчиков. Этот стандарт предназначен для улучшения доверия потребителей к облачным услугам, особенно в плане обработки персональных данных. Он предоставляет для облачных поставщиков руководство, чтобы они могли эффективно управлять информационной безопасностью и защитой данных клиентов в соответствии с нормами и требованиями конфиденциальности [8].

Существуют также и другие стандарты ISO/IEC, которые касаются облачных сред и затрагивают вопросы информационной безопасности облачных систем: ISO/IEC 23751:2022, ISO/IEC 29151:2017, ISO/IEC 19944:2020, ISO/IEC 22624:2020 и другие.

National Institute of Standards and Technology Special Publication 800-145. The NIST Definition of Cloud Computing. Специальная публикация NIST 800-145 под названием "Определение облачных вычислений согласно NIST" представляет собой документ, опубликованный NIST, который предоставляет комплексное определение и структуру для понимания облачных вычислений. Выпущенный в 2011 году, этот документ направлен на стандартизацию и установление общих терминов и характеристик, связанных с облачными вычислениями. Документ описывает пять основных характеристик, три модели обслуживания и четыре модели развертывания облачных вычислений. К основным характеристикам относятся самообслуживание по запросу, широкий сетевой доступ, пулинг ресурсов, быстрая эластичность и измеряемое обслуживание. Три модели обслуживания включают программное обеспечение как услугу (SaaS), платформу как услугу (PaaS) и инфраструктуру как услугу (IaaS). Четыре модели развертывания — это частное облако, публичное облако/общедоступное, коллективное/общественное облако и гибридное облако. Определение облачных вычислений NIST стало широко признанным и принятым, используется повсеместно, помогает понять основополагающие принципы и отличительные особенности облачных вычислений [9].

National Institute of Standards and Technology Special Publication 800-146. Cloud Computing Synopsis and Recommendations. Специальная публикация NIST 800-146, под названием "Краткое изложение и рекомендации по облачным вычислениям", выпущенная NIST, который обеспечивает краткий обзор и рекомендации по облачным вычислениям. В этом документе представлены основные аспекты облачных вычислений, включая их определение, основные характеристики, модели обслуживания и модели развертывания. Он также содержит рекомендации для организаций по эффективному использованию облачных вычислений, а также предостережения от связанных с ними рисков. NIST 800-146 служит справочным ресурсом для тех, кто интересуется основами облачных вычислений, и предоставляет рекомендации для обеспечения безопасности и эффективности при использовании облачных ресурсов [10].

National Institute of Standards and Technology Special Publication 500-292. NIST Cloud Computing Reference Architecture. NIST 500-292 представляет собой документ, который описывает архитектурный подход к облачным вычислениям в рамках стандартов NIST. Этот документ предоставляет основополагающую архитектурную модель, которая помогает организациям лучше понять и внедрять облачные вычисления. Он включает в себя ключевые компоненты, связи и процессы, которые характеризуют архитектуру облачных вычислений. Спецификация NIST 500-292 предназначена для обеспечения общего понимания терминов и концепций, связанных с облачными вычислениями, и может быть использована в качестве основы для разработки и внедрения облачных решений в соответствии с принципами NIST [11].

Представленные выше стандарты в области облачных вычислений играют важную роль в формировании единого подхода к безопасности и стандартизации в использовании облачных сервисов. Эти стандарты не только предоставляют обширные рекомендации, тактики, техники, процедуры и требования, но и способствуют повышению доверия к облачным технологиям. Их активное внедрение в практику обеспечивает согласованность и безопасность в развертывании облачных систем.

Обсуждение.

В Законе Республики Казахстан от 24 ноября 2015 года «Об информатизации» акцентируется внимание на увеличение доли использования облачных сервисов в информационно-коммуникационном обеспечении деятельности органов власти, предусматривается реализация сервисной модели информатизации. При этом Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года

№ 129 утверждены правила реализации сервисной модели информатизации. Но в Концепции развития цифровой экосистемы на 2022-2027 года («Киберщит-2») указывается, что «облачные хранилища и онлайн сервисы часто основываются на непрозрачных или не стандартизованных решениях, в том числе с точки зрения безопасности данных» (цитата).

В Республике Казахстан утверждением национальных стандартов в области технического регулирования и информационной безопасности, включая облачные вычисления, занимается государственное учреждение "Комитет технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан" [12]. Проводится работа по гармонизации и адаптации востребованных международных стандартов по ИТ-технологиям, в том числе по безопасности облачных сервисов.

Одним из стандартов информационной безопасности облачных сервисов, утвержденным в РК, является стандарт СТ РК ISO/IEC 27017-2015. Данный стандарт идентичен международному стандарту ISO/IEC 27017-2015 [13]. Содержание стандарта включает практически все аспекты информационной безопасности: начиная от организации информационной безопасности и кончая криптографией. Все это с учетом обеспечения непрерывности деловой деятельности и соответствия законодательно-нормативным требованиям. Кроме того, стандарт включает приложения с расширенным набором мер контроля и управления для облачных услуг.

Заключение.

В современном информационном обществе важность и актуальность стандартизации информационной безопасности облачных сервисов становятся важными аспектами развития цифровых технологий и достижения ЦУР. Организации, занимающиеся стандартизацией в сфере облачных сервисов, играют ключевую роль в разработке стандартов, направленных на обеспечение безопасности, совместимости и результативности облачных решений. Их работа по разработке стандартов способствует созданию единых подходов к безопасности информации в облачных средах, взаимопониманию между поставщиками и потребителями облачных сервисов. К тому же их деятельность направлена не только на разработку стандартов, но и на их постоянное обновление и адаптацию к изменяющимся условиям информационной безопасности и к появлению новых угроз и рисков, на повышение квалификации специалистов в этой области. Разрабатываемые признанные в мире стандарты способны обеспечить высокий уровень доверия и надежности в сфере облачных вычислений.

ЛИТЕРАТУРА

[1] Названы тренды информационной безопасности в облаках в 2022 году//Tadviser. https://www.tadviser.ru/index.php/Статья:Главные_угрозы_безопасности_в_облаке.

[2] 99% облачных ресурсов предоставляют чрезмерные разрешения//SecurityLab. https://www.securitylab.ru/news/531147.php

[3] Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024 // Gartner. https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240

[4] NIST Cloud Computing Program//NIST. https://www.nist.gov/system/files/documents/itl/cloud/strategy_nist_cc_11_26_2010.pdf

[5] CSCC // Digwatch. https://dig.watch/actor/cloud-standards-customer-council

[6] Cloud Computing Standards: ITU-T//ETSI. http://csc.etsi.org/phase2/snapshot2/snapshot2/ITU-T.html

[7] ISO/IEC 27017:2015(en) Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services//ISO Online Browsing Platform. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27017:ed-1:v1:en

[8] ISO/IEC 27018:2019(en) Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors//ISO Online Browsing Platform. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en

[9] NIST SP 800-145. The NIST Definition of Cloud Computing//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-145.pdf

[10] NIST SP 800-146. Cloud Computing Synopsis and Recommendations//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-146.pdf

[11] NIST SP 500-292. NIST Cloud Computing Reference Architecture//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication 500-292.pdf

[12] Положение государственного учреждения «Комитет технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан»//Zakon.kz. https://online.zakon.kz/Document/?doc_id=31622218&pos=8;-59#pos=8; -59

[13] СТ РК ISO/IEC 27017-2015//Комитет технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан (Госстандарт).

REFERENCES*

[1] Nazvany trendy informatcionnoy bezopasnosti v oblakakh v 2022 godu//Tadviser URL: https://www.tadviser.ru/index.php/Статья:Главные_угрозы_безопасности_в_облаке

[2] 99% oblachnykh resursov predostavlyayut chrezmernye razresheniya//SecurityLab. https://www.securitylab.ru/news/531147.php

[3] Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024//Gartner. https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240

[4] NIST Cloud Computing Program//NIST. https://www.nist.gov/system/files /documents/itl/cloud/strategy_nist_cc_11_26_2010.pdf

[5] CSCC // Digwatch. https://dig.watch/actor/cloud-standards-customer-council

[6] Cloud Computing Standards: ITU-T//ETSI. http://csc.etsi.org/phase2/snapshot2/ snapshot2/ITU-T.html

[7] ISO/IEC 27017:2015(en) Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services//ISO Online Browsing Platform. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27017:ed-1:v1:en

[8] ISO/IEC 27018:2019(en) Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors//ISO Online Browsing Platform. https://www.iso.org/obp/ui/en/#iso:std:iso-iec: 27018: ed-2: v1: en.

[9] NIST SP 800-145. The NIST Definition of Cloud Computing//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800 -145.pdf

[10] NIST SP 800-146. Cloud Computing Synopsis and Recommendations//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-146.pdf

[11] NIST SP 500-292. NIST Cloud Computing Reference Architecture//NIST Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication 500-292.pdf

[12] Polozhenie gosudarstvennogo uchrezhdeniya «Komitet tekhnicheskogo regulirovaniya i metrologii Ministerstva po investitsiyam i razvitiyu Respubliki Kazakhstan»//Zakon.kz. https://online.zakon.kz/Document/?doc_id=31622218&pos=8;-59#pos=8;-59

[13] ST RK ISO/IEC 27017-2015// Komitet tekhnicheskogo regulirovaniya i metrologii Ministerstva po investitsiyam i razvitiyu Respubliki Kazakhstan.

Евгения Айтқожаева, т.ғ.к., профессор, Satbayev University Алматы, Қазақстан, ait_djam@mail.ru.

Элина Ким, магистрант, Satbayev University, Алматы, Қазақстан, kimelina123@gmail.com.

БҰЛТТЫ ҚЫЗМЕТТЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН СТАНДАРТТАУ

Аңдатпа. Бұлттық қызметтердің ауқымы кеңейген сайын олардың киберқауіптердің әртүрлі түрлеріне осалдығы артады. Бұлттық қызметтердегі қауіпсіздік тәуекелдері әртүрлі және өте үлкен, бұл маңызды деректерге үлкен ықтимал қауіп төндіреді. Бұл мәселені шешуде стандарттау жетекші рөл атқарады. Бұл жұмыс бұлттық сервистердің ақпараттық қауіпсіздігін стандарттау саласын зерттеуге және талдауға арналған. Бұлттық қызметтерді пайдалану және олардың ақпараттық қауіпсіздігі саласындағы халықаралық агенттіктердің (Gartner, Palo Alto, VK Cloud Solutions, ИКС Медиа) зерттеулерінің статистикалық деректері берілген. Бұлтты қызметтерді стандарттау және олардың ақпараттық қауіпсіздігіне қатысты негізгі анықтамалар мен түсініктер қарастырылады. Бұлтты технологиялар нарығына талдау жасалды. Осы саладағы стандарттарды әзірлеумен айналысатын негізгі ұйымдар мен бірлестіктерге шолу және талдау жүргізілді, олардың қызмет аясы және қауіпсіз және сенімді бұлтты инфрақұрылымды қалыптастыруға қосқан үлесі көрсетілген. Бұлттық қызметтердің ақпараттық қауіпсіздігінің қолданыстағы халықаралық және халықаралық мойындалған ұлттық стандарттарын қарастыруға ерекше назар аударылады. Қазақстан Республикасындағы бұлттық қызметтердің ақпараттық қауіпсіздігін стандарттау мәселесі қозғалады.

Түйінді сөздер. Бұлттық қызметтер, ақпараттық қауіпсіздік, стандарттау, халықаралық стандарттар, ұлттық стандарттар.

Yevgeniya Aitkhozhayeva, candidate of technical sciences, professor, Satbayev University, Almaty, Kazakhstan, ait_djam@mail.ru.

Elina Kim, master's student, Satbayev University, Almaty, Kazakhstan, kimelina123@gmail.com.

STANDARDIZATION OF INFORMATION SECURITY OF CLOUD SERVICES

Abstract. As the scope of cloud services expands, their vulnerability to various types of cyber threats increases. Security risks in cloud services are varied and quite large, representing a great potential danger to critical data. In solving this problem, standardization plays a leading

role. This work is devoted to research and analysis of the sphere of standardization of information security of cloud services. Statistical data from research by international agencies (Gartner, Palo Alto, VK Cloud Solutions, ИКС Медиа) in the field of use of cloud services and their information security is provided. The basic definitions and concepts related to the standardization of cloud services and their information security are considered. An analysis of the cloud technology market was performed. A review and analysis of key organizations and associations involved in the development of standards in this area is carried out, their scope of activity and contribution to the formation of a secure and reliable cloud infrastructure is indicated. Particular attention is paid to the consideration of existing international and internationally recognized national standards for information security of cloud services. The issue of standardization of information security of cloud services in the Republic of Kazakhstan is touched upon.

Keywords. Cloud services, information security, standardization, international standards, national standards.

****