ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

П Р Е Д В А Р И Т Е Л Ь Н Ы Й
Н А Ц И О Н А Л Ь Н Ы Й
С Т А Н Д А Р Т
Р О С С И Й С К О Й
Ф Е Д Е Р А Ц И И

ПНСТ

Информационные технологии

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ

Термины и определения

Москва
Стандартинформ
201

Предисловие

1 РАЗРАБОТАН Акционерным обществом «Российская венчурная компания» (АО «РВК»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Кибер-физические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от № -ст

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16–2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: Россия, 121205, Москва, Инновационный центр Сколково, улица Нобеля, тел. +7 (495) 777-01-04, e-mail: info@tc194.ru и/или в Федеральное агентство по техническому регулированию и метрологии: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

.

Содержание

Введение

В настоящем стандарте содержится общий набор терминов и определений, которые считаются релевантными и значимыми для промышленного Интернета вещей (IIoT) и используются во всей документации Консорциума Промышленного Интернета (Industrial Internet Consortium, IIC) .

Некоторые определения импортированы из других стандартов, что указывается в квадратных скобках под определением.

ПНСТ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ

Термины и определения

Information Technology. The Industrial Internet of things. Vocabulary

Дата введения – 201 – –

1 Область применения

Настоящий стандарт устанавливает термины и определения в области промышленного Интернета вещей, а также приводит различные термины, используемые в действующих национальных, межгосударственных и международных стандартов в области информационных технологий, относящихся к промышленному Интернету вещей.

2 Нормативные ссылки

В настоящем стандарте нормативные ссылки не используются.

3 Термины и определения

3.1 **автономность** (autonomy)**:** Способность интеллектуальной системы самостоятельно составлять и выбирать среди различных направлений действия для достижения целей, основанные на ее знании и понимании мира, себя и ситуации.

3.2 **авторизация** (authorization)**:** Процесс предоставления субъекту полномочий, в том числе предоставление доступа на основе полномочий доступа.

Примечание – Результатом авторизации являются привилегии (см.3.96).

[13]

3.3 **актив** (asset)**:** Основное приложение, общая система поддержки, высокоэффективная программа, физическая установка, критически важная система, персонал, оборудование или логически связанная группа систем.

[32]

3.4 **анализ влияния на бизнес** (business impact analysis)**:** Процесс (см.3.102) анализа оперативных функций и влияния, которое может оказывать на них нарушение функционирования бизнеса.

[ГОСТ Р ИСО/МЭК 27031-2012]

3.5 **анализ риска** (risk analysis)**:** Процесс (см.3.102) выявления механизма риска (см.3.105) и определения уровня риска.

Примечания

1 – Анализ риска обеспечивает основу для оценивания риска (см.3.87) и принятия решений относительно обработки риска.

2 – Анализ риска включает расчет риска.

[24]

3.6 **анализ угроз** (threat analysis)**:** Изучение источников угроз (см.3.127) уязвимостям системы для определения угроз для определенной системы в определенной функциональной окружающей среде (см.3.80).

[32]

3.7 **аналитика** (analytics)**:** Синтез знаний из информации (см.3.52).

[34]

3.8 **архитектура (системы)** (architecture)**:** Основные понятия или свойства системы в окружающей среде (см.3.80), воплощенной в ее элементах (см.3.149), отношениях и конкретных принципах ее проекта и развития.

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.9 **архитектурное представление** (architecture view)**:** Рабочий продукт, выражающий архитектуру (см.3.8) некоторой системы с точки зрения определенных системных интересов (см.3.48).

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.10 **атака «человек посередине»** (man-in-the-middle attack)**:** Атака, при которой нарушитель (см.3.76) перехватывает поток связи между двумя сущностями, представляясь каждой стороне (см.3.120) как другая и имея возможность читать и изменять сообщения в потоке связи.

3.11 **атрибут** (attribute)**:** Характеристика или свойство сущности (см.3.122), которое можно использовать для описания его состояния, внешнего вида или других аспектов.

[23]

3.12 **аудит** (audit)**:** Независимый анализ и проверка записей и деятельностей для оценки адекватности системного контроля, обеспечения соответствия установленным политикам и операционным процедурам и для рекомендации необходимых изменений в контроле, политике или процедурах.

[32]

3.13 **аутентификация** (authentication)**:** Обеспечение гарантии (см.3.25) того, что заявленные характеристики сущности (см.3.122) правильны.

[ГОСТ Р ИСО/МЭК 27000-2012]

3.14 **аутентификация идентичности** (identity authentication)**:** Формализованный процесс (см.3.102) верификации идентичности (см.3.21), результатом которой в случае успеха является аутентифицированная идентичность (см.3.15) сущности (см.3.122).

[23]

3.15 **аутентифицированная идентичность** (authenticated identity)**:** Идентификационная информация для сущности (см.3.122), созданной для записи результата аутентификации идентичности (см.3.14).

[23]

3.16 **безопасность** (security)**:** Свойство быть защищенным от непреднамеренного или несанкционированного доступа, изменения или уничтожения с обеспечением доступности (см.3.40), целостности (см.3.144) и конфиденциальности (см.3.67).

3.17 **браунфилд** (brownfield)**:** Существующая промышленная система, предназначенная для новой функциональности без нарушений при эксплуатации.

3.18 **валидация** (validation)**:** Подтверждение путем предоставления объективных доказательств того, что требования для определенного предполагаемого использования или приложения были выполнены.

[24]

3.19 **вектор атаки** (attack vector)**:** Путь или средства (например, вирусы, вложение электронной почты, веб-страницы и т.д.), с помощью которых нарушитель (см.3.76) может получить доступ к сущности (см.3.122).

3.20 **верификация** (verification)**:** Подтверждение путем предоставления объективных доказательств того, что указанные требования были выполнены.

Примечание – Синонимом термина является «испытание на соответствие».

[24]

3.21 **верификация идентичности** (identity verification)**:** Процесс (см.3.102) определения того, что представленная идентификационная информация (см.3.44), связанная с определенной сущностью (см.3.122), применима для распознавания сущности в определенном домене идентичности (см.3.36) в определенный момент времени.

[23]

3.22 **виртуальная сущность** (virtual entity)**:** Цифровая сущность или сущность данных, представляющая физическую сущность (см.3.135).

3.23 **возможность использования** (usage capacity)**:** Способность инициировать, участвовать в выполнении или использовать результаты некоторых задач (см.3.41) или функций.

3.24 **вредоносное программное обеспечение** (malware)**:** Опасное программное обеспечение, разработанное специально для повреждения или нарушения работы системы с атакой на конфиденциальность (см.3.67), целостность (см.3.144) или доступность (см.3.40).

[26]

3.25 **гарантия, гарантирование** (assurance)**:** Основание для утверждения, что требование выполнено или будет выполнено.

[ГОСТ Р ИСО/МЭК 15026-1-2016]

3.26 **граница** (edge)**:** Граница между соответствующими цифровыми и физическими сущностями (см.3.135), разграниченная устройствами IoT (см.3.131).

3.27 **граница доверия** (trust boundary)**:** Разделение разных приложений или доменов системы, в которых требуются разные уровни доверия .

3.28 **граничные вычисления** (edge computing)**:** Распределенные вычисления, которые выполняются вблизи границы (см.3.26), где приближенность определяется системными требованиями.

3.29 **гринфилд** (greenfield)**:** Новая промышленная система без нарушений при эксплуатации.

3.30 **данные** (data)**:** Предоставление информации в цифровом и формальном виде, пригодном для передачи, хранения, интерпретации или обработки.

[на основе ГОСТ 33707–2016 (ISO/IEC 2382:2015)]

3.31 **данные в движении** (data in motion)**:** Данные, переносимые из одного места в другое.

[26]

3.32 **данные в покое** (data at rest)**:** Хранимые данные, которые не обрабатываются и не передаются.

3.33 **данные в работе** (data in use)**:** Обрабатываемые данные.

3.34 **датчик IoT** (IoT sensor)**:** Устройство IoT (см.3.131), которое измеряет характеристики физического мира и преобразует их в цифровую форму.

3.35 **деятельность** (activity)**:** Заданная совокупность задач (см.3.41), необходимая для реализации возможностей системы.

Примечание – Деятельность может состоять из других деятельностей.

[17*]

3.36 **домен идентичности** (identity domain)**:** Окружающая среда (см.3.80), в которой сущность (см.3.122) может использовать набор атрибутов (см.3.11) для идентификации (см.3.45) и других целей.

[23]

3.37 **домен приложения** (application domain)**:** Функциональный домен (см.3.140) для реализации логики приложения.

3.38 **домен управления** (control domain)**:** Функциональный домен (см.3.140) для внедрения промышленных систем управления (см.3.100).

3.39 **достоверность** (trustworthiness)**:** Степень доверия к тому, что система работает согласно ожиданиям с такими характеристиками, как функциональная безопасность (см.3.137), безопасность (см.3.16), приватность (см.3.95), надежность (см.3.75) и способность к восстановлению (см.3.119) в условиях воздействия окружающей среды (см.3.80), ошибок персонала, системных сбоев и атак.

3.40 **доступность** (availability)**:** Свойство быть доступным и готовым к использованию по запросу авторизованной сущности (см.3.122).

[ГОСТ Р ИСО/МЭК 27000-2012]

3.41 **задача** (task)**:** Единица работы.

3.42 **заинтересованная сторона, правообладатель** (stakeholder)**:** Индивидуум, команда, организация или их группы, имеющие интерес в системе.

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011*]

3.43 **идентификатор** (identifier)**:** Идентификационная информация (см.3.44),

---

* *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

которая однозначно отличает одну сущность (см.3.122) от другой в данном домене идентичности (см.3.36).

[23]

3.44 **идентификационная информация** (identity information)**:** Набор значений атрибутов (см.3.11), при необходимости с любыми ассоциированными метаданными в идентичности (3.47).

Примечание – В системе информационных технологий (см.3.50) и коммуникационных технологий идентичность (см.3.47) присутствует в качестве идентификационной информации.

[23]

3.45 **идентификация** (identification)**:** Процесс (см.3.102) распознавания сущности с различением от другой сущности (см.3.122) в определенном домене идентичности (см.3.36).

[23]

3.46 **идентификация риска** (risk identification)**:** Процесс (см.3.102) нахождения, составления перечня и описания элементов риска (см.3.105).

Примечания

1 – Идентификация риска включает в себя идентификацию источников риска, событий (см.3.117), их причин и потенциальных последствий.

2 – Идентификация риска может включать исторические данные, теоретический анализ, информированные и экспертные мнения и потребности заинтересованных сторон (см.3.42).

[24]

3.47 **идентичность** (identity)**:** Неотъемлемое свойство экземпляра, которое отличает его от всех других экземпляров.

[29]

3.48 **интерес (системы)** (concern)**:** Польза или проблемы в системе, относящиеся к одной или нескольким заинтересованным сторонам.

Примечание – Интерес относится к любому воздействию на систему в ее окружающей среде (см.3.80), включая воздействия разработки, технологические, деловые, эксплуатационные, организационные, политические, экономические, юридические, регулирующие, экологические и социальные воздействия.

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.49 **интерфейс** (interface)**:** Именованный набор операций, который характеризует поведение сущности (см.3.122).

[35]

3.50 **информационные технологии, ИТ** (information technology, IT)**:** Спектр технологий для обработки информации (см.3.52), включая программное обеспечение, оборудование, технологии связи и соответствующие службы.

Примечание − Хотя ИТ используются в ОТ (см.3.81), ИТ традиционно считаются отличными от ОТ из-за различного набора требований и интересов (см.3.48).

[36]

3.51 **информационный домен** (information domain)**:** Функциональный домен (см.3.140) для управления и обработки данных (см.3.30).

3.52 **информация** (information)**:** Данные (см.3.30), которые в определенном контексте имеют особое значение.

[на основе [21]]

3.53 **инфраструктура открытых ключей, ИОК** (public key infrastructure, PKI)**:** Инфраструктура, включающая в себя аппаратное и программное обеспечение, людей, процессы и политики, которая использует технологию электронной подписи для предоставления доверяющим сторонам проверяемой ассоциации, установленной между открытым компонентом (см.3.59) пары асимметричных ключей и конкретным субъектом.

[ГОСТ Р ИСО 21091-2017]

3.54 **инфраструктурная служба** (infrastructure service)**:** Служба (см.3.116), необходимая для корректной работы любой реализации IoT.

Примечание − Инфраструктурные службы обеспечивают поддержку основных функций IoT.

[35]

3.55 **инцидент информационной безопасности** (information security incident)**:** Одно или несколько нежелательных или неожиданных событий (см.3.117) информационной безопасности (см.3.16), которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

[ГОСТ Р ИСО/МЭК 27000-2012]

3.56 **исполнительное устройство IoT** (IoT actuator)**:** Устройство IoT (см.3.131),

которое меняет свойство физической сущности (см. 3.135) в ответ на входной сигнал.

3.57 **коллаборация** (collaboration)**:** Тип композиции (см.3.58), элементы (см.3.149) которой взаимодействуют децентрализованным образом, каждый из них согласно своему плану и целям без предопределенного шаблона поведения.

[ГОСТ Р ИСО/МЭК 18384-1-2017]

3.58 **композиция** (composition)**:** Результат сборки набора элементов (см.3.149) для конкретной цели.

[ГОСТ Р ИСО/МЭК 18384-1-2017]

3.59 **компонент** (component)**:** Модульная, развертываемая и заменяемая часть системы, которая инкапсулирует реализацию и предоставляет набор интерфейсов (см.3.49).

[16]

3.60 **компонуемость** (composability)**:** Способность компонента (см.3.59) взаимодействовать с другими компонентами рекомбинантным способом для удовлетворения требований, основанных на ожидании поведения взаимодействующих сторон.

3.61 **конвергенция ИТ и ОТ** (IT/OT convergence)**:** Процесс совмещения информационных технологий (см.3.50) и операционных технологий (см.3.81) для создания систем промышленного Интернета вещей (IIoT) (см.3.113).

3.62 **конечная точка** (endpoint)**:** Компонент (см.3.59), который имеет вычислительные возможности и подключение по сети (см.3.111).

3.63 **конечная точка связности** (connectivity endpoint)**:** Интерфейс (см.3.49), который обеспечивает связность (см.3.109).

3.64 **контрмера** (countermeasure)**:** Действие, устройство, процедура, методика или другая мера, предназначенная для минимизации уязвимости (см.3.133).

[21]

3.65 **контроль безопасности** (security controls)**:** Управленческий, операционный и технический контроль (т.е. меры предосторожности или контрмеры (см.3.64)), предписанные системе информации для защиты конфиденциальности (см.3.67), целостности (см.3.144) и доступности (см.3.40) системы и ее информации.

[14]

3.66 **контроль доступа** (access control)**:** Обеспечение того, чтобы доступ к активам (см.3.3) был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и требованиями безопасности (см.3.16).

Примечание − Контроль доступа требует как аутентификации (см.3.13), так и авторизации (см.3.2).

[ГОСТ Р ИСО/МЭК 27000-2012]

3.67 **конфиденциальность** (confidentiality)**:** Свойство информации (см.3.52) быть недоступной или закрытой для неавторизованных лиц, сущностей (см.3.122) или процессов.

[ГОСТ Р ИСО/МЭК 27000-2012]

3.68 **корни доверия** (roots of trust)**:** Базис, включающий оборудование, программное обеспечение, людей и организационные процессы (см.3.102) для установления доверия к системе.

3.69 **критичность** (criticality)**:** Мера степени, в которой организация зависит от сущности (см.3.122) для достижения миссии или бизнес-функции.

[32*]

3.70 **криптография** (cryptography)**:** Дисциплина, которая воплощает принципы, средства и механизмы для преобразования данных, чтобы скрыть содержание информации (см.3.52), предотвратить их скрытое изменение и / или предотвратить их несанкционированное использование.

[18]

3.71 **менеджмент риска** (risk management)**:** Скоординированные действия по руководству и управлению организацией в отношении риска (см.3.105).

[ГОСТ Р ИСО/МЭК 27000-2012]

3.72 **минимальная привилегия** (least privilege)**:** Принцип, согласно которому архитектура (см.3.8) безопасности (см.3.16) должна быть спроектирована таким образом, чтобы каждой сущности (см.3.122) предоставлялись минимальные системные ресурсы и авторизации (см.3.2), необходимые для выполнения ее функции.

[32]

3.73 **моделирование угроз** (threat modeling)**:** Структурированный анализ для выявления, количественной оценки и устранения рисков информационной безопасности (см.3.106), связанных с приложением или системой.

3.74 **мультиаренда** (multi-tenancy)**:** Распределение физических или

---

* *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

виртуальных ресурсов, таким образом, что несколько арендаторов и их вычисления и данные (см.3.30) изолированы друг от друга и недоступны друг другу.

[ГОСТ ISO/IEC 17788-2016]

3.75 **надежность** (reliability)**:** Способность системы или компонента (см.3.59) выполнять свои требуемые функции в указанных условиях в течение определенного периода времени.

[26]

3.76 **нарушитель** (attacker)**:** Любое лицо, преднамеренно использующее уязвимости (см.3.133) технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей (см.3.111), или снижения доступности (см.3.40) ресурсов информационной системы и сетевых ресурсов для законных пользователей.

[ГОСТ Р ИСО/МЭК 27033-1-2011]

3.77 **неотказуемость** (non-repudiation)**:** Способность удостоверять возникновение заявленного события (см.3.117) или действия и их объектов.

[24]

3.78 **нефункциональное требование** (non-functional requirement)**:** Требование, которое определяет общие качества или атрибуты (см.3.11) получаемой системы.

Примечание − Нефункциональные требования накладывают ограничения на разрабатываемую систему, процесс разработки и определяют внешние ограничения, которым должна соответствовать система.

3.79 **облачные вычисления** (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.

Примечание − Примеры ресурсов включают серверы, операционные системы, сети, программное обеспечение, приложения и оборудование для хранения данных.

[ГОСТ ISO/IEC 17788-2016]

3.80 **окружающая среда (системы)** (environment)**:** Контекст, определяющий параметры и обстоятельства всех воздействий на систему.

Примечание − Окружающая среда системы включает воздействия разработки, технологические, деловые, эксплуатационные, организационные, политические, экономические, юридические, регулирующие, экологические и социальные воздействия.

[ГОСТ Р 57100-2016 /ISO/IEC/IEEE 42010:2011*]

3.81 **операционные технологии, ОТ** (operational technology, OT)**:** Аппаратное и программное обеспечение, которое обнаруживает или вызывает изменение посредством прямого мониторинга и / или контроля физических устройств, процессов и событий (см.3.117) на предприятии.

[36]

3.82 **операционный домен** (operations domain)**:** Функциональный домен (см.3.138) для управления и работы в домене управления (см.3.38).

3.83 **описание архитектуры** (architecture description)**:** Рабочий продукт, используемый для выражения архитектуры (см.3.8).

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.84 **оркестровка** (orchestration)**:** Тип композиции (см.3.58), где один определенный элемент (см.3.149) используется для наблюдения за другими элементами и управления ими.

Примечание − Элемент, который управляет оркестровкой, сам не является частью оркестровки.

[ГОСТ Р ИСО/МЭК 18384-1-2017]

3.85 **осведомленность о ситуации** (situational awareness)**:** Понимание состояния безопасности (см.3.16) предприятия и его окружающей среды угроз (см.3.127) в определенном объеме времени и пространства; понимание / подразумевание обоих рисков (см.3.105); и проекция их статуса на ближайшее будущее.

[32]

3.86 **отказ в обслуживании** (denial of service, DoS)**:** Прекращение санкционированного доступа к ресурсам системы или задержка операций и функций системы, приводящее в итоге к потере доступности для авторизованных пользователей.

[ГОСТ Р ИСО/МЭК 27033-1-2011]

3.87 **оценивание риска** (risk evaluation)**:** Процесс (см.3.102) сравнения результатов анализа риска (см.3.5) с критериями риска (см.3.105) для определения, является ли величина приемлемой или допустимой.

Примечание − Оценивание риска способствует принятию решения об обработке риска.

[24]

3.88 **оценка риска** (risk assessment)**:** Общий процесс (см.3.102) идентификации риска (см.3.46), анализа риска (см.3.5) и оценивания риска (см.3.87).

[24]

3.89 **оценка риска обеспечения приватности** (privacy risk assessment)**:** Общий процесс (см.3.102) идентификации риска (см.3.46), анализа риска (см.3.5) и оценивания риска (см.3.87) в отношении обработки ПИИ (см.3.91).

Примечание − Этот процесс известен также как оценка влияния на приватность (см.3.95).

[ГОСТ Р ИСО/МЭК 29100-2013]

3.90 **оценка уязвимости безопасности** (security vulnerability assessment)**:** Систематическое исследование информационной системы или продукта для определения адекватности мер безопасности (см.3.16), выявления недостатков безопасности, предоставления данных (см.3.30), из которых можно прогнозировать эффективность предлагаемых мер безопасности, и подтверждения адекватности таких мер после реализации.

[32]

3.91 **персональная идентификационная информация, ПИИ** (personally identifiable information, PII)**:** Любая информация (см.3.52):

- которая идентифицирует или может быть использована для идентификации, контакта или определения местонахождения лица, к которому относится такая информация;
- из которой может быть получена идентификационная или контактная информация о физическом лице;
- которая прямо или косвенно связана или может быть связана с физическим лицом.

[22]

3.92 **поверхность атаки** (attack surface)**:** Элементы (см.3.149) и взаимодействия системы, которые уязвимы для атаки.

3.93 **подтверждение соответствия** (attestation)**:** Выдача заявления, основанного на демонстрации выполнения определенных требований.

[ГОСТ Р ИСО/МЭК 29109-1-2012]

3.94 **политика безопасности** (security policy)**:** Правила, директивы и

рекомендации по управлению, защите и распределению активов (см.3.3) внутри организации и ее систем, включая конфиденциальную информацию (см.3.52) и влияющие на систему активы и связанные с ними элементы (см.3.149).

[32]

3.95 **приватность** (privacy)**:** Право отдельных лиц контролировать или влиять на то, какая информация (см.3.52), связанная с ними, может быть собрана и сохранена, а также кем и кому эта информация может быть раскрыта.

[30]

3.96 **привилегия** (privilege)**:** Право, предоставленное человеку, программе или процессу (см.3.102).

[37]

3.97 **программируемый логический контроллер, ПЛК** (programmable logic controller, PLC)**:** Электронное устройство, предназначенное для контроля логической последовательности событий (см.3.117).

[15]

3.98 **программное обеспечение как услуга, SaaS** (software as a service, SaaS)**:** Категория служб (см. 3.116) облачных вычислений, в которой потребителю службы облачных вычислений предоставляется следующий тип возможностей облака: тип возможностей приложений.

[ГОСТ ISO/IEC 17788-2016]

3.99 **производное поведение** (emergent behavior)**:** Поведение системы, реализуемое взаимодействием ее компонентов (см.3.59).

3.100 **промышленная система управления, ICS** (industrial control system, ICS)**:** Комбинация компонентов (см.3.59) управления, которые действуют вместе для осуществления контроля в физическом мире.

3.101 **промышленный интернет** (industrial internet)**:** Интернет вещей, машин, компьютеров и людей, обеспечивающий интеллектуальные производственные операции с использованием расширенной аналитики (см.3.7) данных (см.3.30) для качественно новых результатов бизнеса.

3.102 **процесс** (process)**:** Тип композиции (см.3.58), элементы (см.3.149) которой составлены в последовательность или поток действий и взаимодействий с целью выполнения определенной работы.

Примечание − Процесс также может быть коллаборацией (см.3.57), хореографией (см.3.143) или оркестровкой (см.3.84).

[ГОСТ Р ИСО/МЭК 18384-1-2017]

3.103 **реакция на риск** (risk response)**:** Принятие, уклонение, смягчение, разделение или передача риска (см.3.105) организационным операциям (т.е. миссии, функциям, имиджу или репутации), активам (см.3.3) организации, индивидуумам, другим организациям или стране.

[32]

3.104 **реакция на инцидент / реакция на вторжение** (incident response / intrusion response)**:** Действия, предпринятые для защиты и восстановления нормальных условий работы информационных систем и информации (см.3.52), хранящейся в них, когда происходит атака или вторжение.

[25]

3.105 **риск** (risk)**:** Влияние неопределенности на цели.

Примечания

1 – Влиянием является положительное или отрицательное отклонение от ожидаемого результата.

2 – Неопределенность – это состояние недостатка информации (см.3.52), связанной с пониманием или знанием события (см.3.117), его последствия или вероятности.

3 – Риск можно характеризовать потенциальными событиями и последствиями или их совокупностью.

4 – Риск можно выражать в терминах совокупности последствий события (включая изменение обстоятельств) и связанной вероятности возникновения.

5 – В контексте систем управления информационной безопасностью риски информационной безопасности (см.3.106) могут быть выражены как влияние неопределенности на цели информационной безопасности.

6 – Риск информационной безопасности (см.3.106) связан с возможностью, что угрозы (см.3.127) будут использовать уязвимости (см.3.133) актива (см.3.3) информации (см.3.52) или группы активов информации и тем самым нанести ущерб организации.

[24]

3.106 **риск информационной безопасности** (information security risk)**:** Возможность того, что данная угроза (см.3.127) сможет воспользоваться уязвимостью (см.3.133) актива (см.3.3) или группы активов и тем самым нанесет ущерб организации.

[ГОСТ Р ИСО/МЭК 27005-2010]

3.107 **робастность** (robustness)**:** Способность системы или компонента (см.3.59) корректно функционировать при наличии недопустимых входных данных или стрессовых условий окружающей среды (см.3.80).

3.108 **роль** (role)**:** Набор возможностей использования (см.3.23).

Примечания

1 – Роль – это абстракция сущности (см.3.122), которая выполняет набор деятельностей (см.3.35).

2 – Роли выполняются или принимаются сторонами (см.3.120).

3.109 **связность** (connectivity)**:** Способность системы или приложения взаимодействовать с другими системами или приложениями через сеть (-и) (см.3.111).

3.110 **семантическая функциональная совместимость** (semantic interoperability)**:** Функциональная совместимость (см.3.138), обеспечивающая понимание участвующими системами смысла передаваемой информации (см.3.52).

3.111 **сеть** (network)**:** Совокупность взаимодействующих конечных точек (см.3.62).

3.112 **синтаксическая функциональная совместимость** (syntactic interoperability)**:** Функциональная совместимость (см.3.138), обеспечивающая понимание участвующими системами форматов передаваемой информации (см.3.52).

[20]

3.113 **система промышленного Интернета вещей** (industrial internet of things system, IIoT)**:** Система, которая связывает и интегрирует промышленные системы управления (см.3.100) с корпоративными системами, бизнес-процессами и аналитикой (см.3.7).

Примечания

1 – Промышленные системы управления (см.3.100) содержат датчики и исполнительные устройства.

2 – Как правило, это большие и сложные системы.

3.114 **сквозная функция** (cross-cutting function)**:** Функция, применяется и реализуется в нескольких функциональных доменах (см.3.140) архитектуры (см.3.8)

для работы со сквозными интересами (3.115).

3.115 **сквозной интерес** (cross-cutting concern)**:** Интерес (см.3.48), который затрагивает всю систему и, следовательно, влияет на несколько точек зрения на архитектуру (см.3.123).

3.116 **служба** (service)**:** Отдельная часть функциональности, которая предоставляется сущностью (см.3.122) через интерфейсы (см.3.49).

[28]

3.117 **событие** (event)**:** Любое наблюдаемое явление в системе и / или сети (см.3.111).

[33]

3.118 **событие угрозы** (threat event)**:** Событие (см.3.117) или ситуация, которая может вызвать нежелательные последствия или воздействие.

[32]

3.119 **способность к восстановлению** (resilience)**:** Способность системы или компонента (см.3.59) поддерживать приемлемый уровень обслуживания в условиях сбоя.

3.120 **сторона** (party)**:** Сущность (см.3.122), физическое лицо или логическая сущность (например, администратор, юридическое лицо, агент), обладающая некоторой автономностью (3.1), интересом и ответственностью при выполнении деятельности (см.3.35).

Примечание − Сторона (см.3.120) может выполнять более одной роли (см.3.108), и роль может выполняться несколькими сторонами (т.е. любой из них).

3.121 **структура архитектуры** (architecture framework)**:** Условности, принципы и практики для описания архитектур (см.3.8), установленные в пределах заданной области применения и/или объединения заинтересованных сторон (см.3.42).

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.122 **сущность** (entity)**:** Предмет, который имеет отличительное узнаваемое присутствие.

Примечание − Например, человек, организация, устройство, подсистема или группа таких предметов.

[23*]

3.123 **точка зрения на архитектуру** (architecture viewpoint)**:** Рабочий продукт, устанавливающий условности конструирования, интерпретации и использования архитектурного представления (см.3.9) для структуризации определенных системных интересов (см.3.48).

[ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011]

3.124 **точка зрения на бизнес** (business viewpoint)**:** Точка зрения на архитектуру (см.3.123), которая отражает видение, ценности и цели заинтересованных сторон (см.3.42) в создании системы промышленного Интернета вещей (см.3.113) в деловом и нормативном контексте.

3.125 **точка зрения на использование** (usage viewpoint)**:** Точка зрения на архитектуру (см.3.123), которая отражает интересы (см.3.48), связанные с использованием системы промышленного Интернета вещей (см.3.113).

3.126 **точка зрения на реализацию** (implementation viewpoint)**:** Точка зрения на архитектуру (см.3.123), которая отражает интересы (см.3.48), связанные с реализацией возможностей и структуры системы промышленного Интернета вещей (см.3.113).

3.127 **угроза** (threat)**:** Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

[ГОСТ Р ИСО/МЭК 27000-2012]

3.128 **управление идентичностью** (identity management)**:** Процессы и политики, участвующие в управлении жизненным циклом, значением, типом и необязательными метаданными атрибутов (см.3.11) в идентичности (см.3.47), известных в определенном домене идентичности (см.3.36).

[23]

3.129 **уровень архитектуры** (architecture layer)**:** Логическое разбиение архитектуры (см.3.8).

3.130 **устойчивость к риску** (risk tolerance)**:** Уровень риска (см.3.105), допускаемый сущностью (см.3.122) для достижения потенциального ожидаемого результата.

[32]

3.131 **устройство IoT** (IoT device)**:** Конечная точка (см.3.62), которая

---

* *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

взаимодействует с физическим миром посредством восприятия или воздействия.

3.132 **учетные данные** (credential)**:** Доказательства или свидетельства, которые подтверждают заявление идентичности (см.3.47) или утверждение атрибута (см.3.11) и обычно предназначены для использования более одного раза.

[37]

3.133 **уязвимость** (vulnerability)**:** Слабое место актива (см.3.3) или контроля безопасности (см.3.65) , которые могут быть использованы угрозой (см.3.127).

[24*]

3.134 **физическая защита** (physical security)**:** Средства, используемые для обеспечения физической защиты ресурсов от преднамеренной или случайной угрозы (см.3.127).

[ГОСТ Р ИСО 7498-2-99]

3.135 **физическая сущность** (physical entity)**:** Сущность (см.3.122), которая является субъектом мониторинга и контроля действий.

3.136 **функциональная структура** (functional framework)**:** Набор абстрактных многократно используемых функциональных компонентов (см.3.141), которые могут быть расширены / настроены и применены к нескольким приложениям в определенной области.

3.137 **функциональная безопасность** (safety)**:** Состояние работающей системы, не приводящее к неприемлемому риску (см.3.105) получения телесных повреждений или ущерба здоровью людей, прямо или косвенно в результате нанесения ущерба имуществу или окружающей среде (см.3.80).

[31]

3.138 **функциональная совместимость (интероперабельность)** (interoperability)**:** Способность двух или более систем обмениваться информацией (см.3.52) и использовать эту информацию.

[ГОСТ ISO/IEC 17788-2016]

3.139 **функциональная точка зрения** (functional viewpoint)**:** Точка зрения на архитектуру (см.3.123), которая отражает интересы (см.3.48), связанные с функциональными возможностями и структурой системы промышленного Интернета вещей (см.3.113) и ее компонентов (см.3.59).

3.140 **функциональный домен** (functional domain)**:** Набор функций,

---

* *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

составляющих систему.

3.141 **функциональный компонент** (functional component)**:** Функциональный строительный блок, необходимый для участия в деятельности (см.3.35), осуществляемой реализацией.

[17]

3.142 **функция безопасности** (security function)**:** Криптографические алгоритмы с режимами работы, утвержденные ИСО/МЭК или уполномоченным органом, такие как блочные шифры, потоковые шифры, алгоритмы симметричного или асимметричного ключа, коды аутентификации сообщений, хэш-функции или другие функции безопасности, генераторы случайных битов, аутентификация объектов, а также генерация и установление SSP*.

[19**]

3.143 **хореография** (choreography)**:** Тип композиции (см.3.58), элементы (см.3.149) которой взаимодействуют децентрализованным образом с каждой автономной частью, зная определенный заранее шаблон поведения для всей (глобальной) композиции и следуя ему.

Примечания

1 – Хореография не требует полного или точного знания шаблона поведения.

2 – См. ИСО/МЭК 18384-3:2016, 8.3.

[ГОСТ Р ИСО/МЭК 18384-1-2017]

3.144 **целостность** (integrity)**:** Свойство сохранения правильности и полноты активов.

[ГОСТ Р ИСО/МЭК 27000-2012]

3.145 **целостность данных** (data integrity)**:** Свойство данных, что они не были изменены или уничтожены несанкционированным способом.

[26]

3.146 **цифровое представление** (digital representation)**:** Элемент (см.3.149) данных (см.3.30), представляющий набор свойств физической сущности (см.3.135).

3.147 **шина данных** (databus)**:** Технология обмена информацией (см.3.52),

---

* *SSP – чувствительные параметры безопасности (Sensitive security parameters)*

** *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

ориентированная на данные и реализующая виртуальное глобальное пространство данных, где приложения обмениваются данными.

Примечание – Ключевыми характеристиками шины данных являются:

- приложения напрямую взаимодействуют с оперативными данными через интерфейс (см.3.49);
- реализация шины данных интерпретирует и выборочно фильтрует данные (см.3.30);
- реализация шины данных предписывает правила и управляет параметрами качества обслуживания (Quality of service, QoS), такими как скорость, надежность (см.3.75) и безопасность (см.3.16) потока данных (см.3.32).

3.148 **шифрование** (encryption)**:** Обратимая операция с использованием криптографического алгоритма, преобразующего данные (см.3.32) в зашифрованный текст для сокрытия информационного содержания данных.

[27]

3.149 **элемент** (element)**:** Сущность (см.3.122), неделимая на данном уровне абстракции и имеющая четко определенную границу.

[ГОСТ Р ИСО/МЭК 18384-1-2017*]

---

* *Формулировка определения из соответствующего источника изменена для согласованности с другими определениями*

Алфавитный указатель терминов на русском языке

	ПНСТ
корни доверия	3.68
критичность	3.69
криптография	3.70
менеджмент риска	3.71
минимальная привилегия	3.72
моделирование угроз	3.73
мультиаренда	3.74
надежность	3.75
нарушитель	3.76
неотказуемость	3.77
нефункциональное требование	3.78
облачные вычисления	3.79
окружающая среда (системы)	3.80
операционные технологии, ОТ	3.81
операционный домен	3.82
описание архитектуры	3.83
оркестровка	3.84
осведомленность о ситуации	3.85
отказ в обслуживании	3.86
оценивание риска	3.87
оценка риска	3.88
оценка риска обеспечения приватности	3.89
оценка уязвимости безопасности	3.90
персональная идентификационная информация, ПИИ	3.91
поверхность атаки	3.92
подтверждение соответствия	3.93
политика безопасности	3.94
приватность	3.95
привилегия	3.96
программируемый логический контроллер, ПЛК	3.97
программное обеспечение как услуга, SaaS	3.98
производное поведение	3.99
промышленная система управления, ICS	3.100
промышленный интернет	3.101

процесс	3.102
реакция на риск	3.103
реакция на инцидент / реакция на вторжение	3.104
риск	3.105
риск информационной безопасности	3.106
робастность	3.107
роль	3.108
связность	3.109
семантическая функциональная совместимость	3.110
сеть	3.111
синтаксическая функциональная совместимость	3.112
система промышленного Интернета вещей, IIoT	3.113
сквозная функция	3.114
сквозной интерес	3.115
служба	3.116
событие	3.117
событие угрозы	3.118
способность к восстановлению	3.119
сторона	3.120
структура архитектуры	3.121
сущность	3.122
точка зрения на архитектуру	3.123
точка зрения на бизнес	3.124
точка зрения на использование	3.125
точка зрения на реализацию	3.126
угроза	3.127
управление идентичностью	3.128
уровень архитектуры	3.129
устойчивость к риску	3.130
устройство IoT	3.131
учетные данные	3.132
уязвимость	3.133
физическая защита	3.134
физическая сущность	3.135

функциональная структура	3.136
функциональная безопасность	3.137
функциональная совместимость (интероперабельность)	3.138
функциональная точка зрения	3.139
функциональный домен	3.140
функциональный компонент	3.141
функция безопасности	3.142
хореография	3.143
целостность	3.144
целостность данных	3.145
цифровое представление	3.146
шина данных	3.147
шифрование	3.148
элемент	3.149

Алфавитный указатель терминов на английском языке

ПНСТ

	ПНСТ
orchestration	3.84
party	3.120
personally identifiable information, PII	3.91
physical entity	3.135
physical security	3.134
public key infrastructure, PKI	3.53
privacy	3.95
privacy risk assessment	3.89
privilege	3.96
process	3.102
programmable logic controller, PLC	3.97
reliability	3.75
resilience	3.119
risk	3.105
risk analysis	3.5
risk assessment	3.88
risk evaluation	3.87
risk identification	3.46
risk management	3.71
risk response	3.103
risk tolerance	3.130
robustness	3.107
role	3.108
roots of trust	3.68
software as a service, SaaS	3.98
safety	3.137
security	3.16
security controls	3.65
security function	3.142
security policy	3.94
security vulnerability assessment	3.90
semantic interoperability	3.110
service	3.116
situational awareness	3.85

ПНСТ

Библиография

[1] ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры

[2] ГОСТ Р ИСО 21091-2017 Информатизация здоровья. Службы каталога поставщиков и субъектов медицинской помощи и других сущностей

[3] ГОСТ Р ИСО 7498-2-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации

[4] ГОСТ Р ИСО/МЭК 15026-1-2016 Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 1. Понятия и словарь

[5] ГОСТ Р ИСО/МЭК 18384-1-2017 Информационные технологии (ИТ). Эталонная архитектура для сервис-ориентированной архитектуры (SOA RA). Часть 1. Терминология и концепции SOA

[6] ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

[7] ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

[8] ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

[9] ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции

[10] ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Основы обеспечения приватности

[11] ГОСТ Р ИСО/МЭК 29109-1-2012 Информационные технологии (ИТ). Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщенная методология испытаний на соответствие

[12] ГОСТ ISO/IEC 17788-2016 Информационные технологии (ИТ). Облачные вычисления. Общие положения и терминология

[13] ИСО 7498-2:1989 Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты (ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basis reference model – Part 2: Security architecture)

[14] ИСО 12812-1:2017 Банковская система. Мобильные финансовые услуги. Часть 1. Общая структура (ISO 12812-1:2017 Core banking – Mobile financial services – Part 1: General framework)

[15] ИСО 13577-4:2014 Печи промышленные и связанное с ними технологическое оборудование. Безопасность. Часть 4. Защитные системы (ISO 13577-4:2014 Industrial furnace and associated processing equipment – Safety – Part 4: Protective systems)

[16] ИСО 14813-5:2010 Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспортных систем. Часть 5. Требования к описанию архитектуры в стандартах ITS (ISO 14813-5:2010 Intelligent transport systems -- Reference model architecture(s) for the ITS sector -- Part 5: Requirements for architecture description in ITS standards)

[17] ИСО/МЭК 17789:2014 Информационные технологии. Облачные вычисления. Эталонная архитектура (ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture)

[18] ИСО/МЭК 18014-2:2019 Информационная технология. Методы и средства обеспечения безопасности. Услуги по созданию метки даты/времени. Часть 2. Механизмы создания независимых маркеров (ISO/IEC 18014-2:2019 Information technology. Security techniques. Time-stamping services. Part 2. Mechanisms producing independent tokens)

[19] ИСО/МЭК 19790:2012 Информационная технология. Методы обеспечения защиты. Требования к защите применительно к криптографическим модулям (ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules)

[20] ИСО/МЭК 19941:2017 Информационная технология. Облачные вычисления. Интероперабельность и переносимость (ISO/IEC 19941:2017 Information technology -- Cloud computing -- Interoperability and portability)

[21] ИСО/МЭК 2382:2015 Информационная технология. Словарь (ISO/IEC 2382:2015

Information technology – Vocabulary)

[22] ИСО/МЭК 24745:2011 Информационные технологии. Техника безопасности. Защита биометрической информации (ISO/IEC 24745:2011 Information technology -- Security techniques -- Biometric information protection)

[23] ИСО/МЭК 24760-1:2011 Информационная технология. Методы обеспечения защиты. Схема управления идентичностью. Часть 1. Терминология и понятия (ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts)

[24] ИСО/МЭК 27000:2016 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь (ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary)

[25] ИСО/МЭК 27039:2015 Информационная технология. Методы защиты. Выбор, применение и операции систем обнаружения вторжений (IDPS) (ISO/IEC 27039:2015 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems (IDPS))

[26] ИСО/МЭК 27040:2015 Информационная технология. Методы обеспечения безопасности. Безопасность хранения (ISO/IEC 27040:2015 Information technology -- Security techniques -- Storage security)

[27] ИСО/МЭК 9798-1:2010 Информационные технологии. Методы защиты. Аутентификация объектов. Часть 1. Общие положения (ISO/IEC 9798-1:2010 Information technology -- Security techniques -- Entity authentication -- Part 1: General)

[28] ИСО/МЭК ТО 14252:1996 Информационные технологии. Руководство для среды открытой системы POSIX (ISO/IEC TR 14252:1996 Information technology - Guide to the POSIX Open System Environment (OSE))

[29] ИСО/МЭК/IEEE 31320-2:2012 Информационные технологии. Языки моделирования. Часть 2. Синтаксис и семантика для IDEF1X97 (IDEFobject) (ISO/IEC/IEEE 31320-2:2012 Information technology -- Modeling Languages -- Part 2: Syntax and Semantics for IDEF1X97 (IDEFobject))

[30] ИСО/ТУ 17574:2009 Электронный сбор денег. Руководящие указания по защитным профилям безопасности (ISO/TS 17574:2009 Electronic fee collection - Guidelines for security protection profiles)

ПНСТ

[31] Руководство ИСО/МЭК 51 Аспекты безопасности и их применение в стандартах (ISO/IEC Guide 51, Safety aspects - Guidelines for their inclusion in standards)

[32] Глоссарий основных терминов по информационной безопасности НИСТ*, версия 2 (NIST IR 7298 Glossary of Key Information Security Terms, revision 2)

[33] Специальная публикация НИСТ* 800-61 «Руководство по обработке инцидентов компьютерной безопасности», версия 2 (NIST SP 800-61 Computer Security Incident Handling Guide, revision 2)

[34] Межведомственная публикация НИСТ 8401-1 «Концепция NIST интероперабельности больших данных. Том 1: Определения» (NIST IP 8401-1 DRAFT NIST Big Data Interoperability Framework: Volume 1, Definitions)

[35] VDI/VDE Innovation+Technik GmbH: Интернет вещей. Архитектура: терминология. (Internet of Things – Architecture: Terminology, VDI/VDE Innovation+Technik GmbH)

[36] Gartner: Глоссарий IT-терминов (Gartner: IT Glossary)

[37] Комитет по национальным системам безопасности (CNSS): 4009. Глоссарий (Committee on National Security Systems (CNSS): CNSSI No. 4009: Glossary)

* *НИСТ – Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST), США*

УДК 004.738 ОКС 35.020, 35.110

Ключевые слова: информационные технологии, промышленный интернет вещей, словарь, термины и определения