ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 819— 2023

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Системы с разделением доменов. Термины и определения

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 РАЗРАБОТАН Акционерным обществом «Лаборатория Касперского» (АО «Лаборатория Касперского»)

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 13 марта 2023 г. № 14-пнст

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: 121205 Москва, Инновационный центр Сколково, улица Нобеля, 1, e-mail: info@tc194.ru и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

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.rst.gov.ru)

Содержание

1 Область применения 1
2 Термины и определения 1
Алфавитный указатель терминов на русском языке 5

Введение

Установленные в настоящем стандарте термины расположены в систематизированном порядке, отражающем систему понятий данной области знания.

Для каждого понятия установлен один стандартизованный термин.

В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Системы с разделением доменов. Термины и определения

Information technology. Internet of things. Domain shared systems. Terms and definitions

Срок действия — с 2023—03—31
до 2026—03—31

1 Область применения

Настоящий стандарт устанавливает термины и определения в области интернета вещей, использующих подход с разделением доменов.

2 Термины и определения

1 **авторизация:** Процесс предоставления прав доступа субъекта к объекту.

2 **архитектура POSIX:** Набор стандартов, описывающих интерфейсы между операционной системой и прикладной программой (системный API), библиотеку языка С и набор приложений и их интерфейсов.

3 **архитектура политики:** Описание семейства политик безопасности в системе интернета вещей.

Примечание — Графически может быть представлено в виде направленного графа, узлы которого описывают домены, направленные дуги которых описывают связь между доменами.

4

безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

[ГОСТ Р 53114—2008, статья 3.1.1]

5 **временное разделение:** Тип разделения, который разделяет системные ресурсы во времени путем планирования обработки запросов к этим ресурсам от разделенных доменов в разные промежутки времени.

6 **декомпозиция в проектировании программного обеспечения;** декомпозиция ПО: Подход к разработке программного обеспечения, состоящий в разбиении сложной программной системы на множество простых с целью уменьшения сложности ее понимания, верификации, сертификации и поддержки.

Примечания

1 Декомпозиция вертикальная — метод декомпозиции, при котором сложная система представляется в соответствии с модулями и иерархическими уровнями функциональности, когда модули более высокого уровня реализуются с использованием модулей низкого уровня.

Издание официальное

2 Декомпозиция горизонтальная — метод декомпозиции сложной системы на модули, при котором модуль содержит функции, имеющие схожее назначение. Интерфейс межмодульных взаимодействий должен быть четко определен и, по возможности, минимизирован.

7 **домен:** Функциональная изолированная единица разделения системы, выделенная таким образом, чтобы в этой системе можно было реализовать заданную политику безопасности.

8 **доступ:** Возможность получения информации, в том числе хранимой в системе интернета вещей, и использования этой информации.

Примечание — Доступ порождает поток информации.

9 **интерфейс прикладного программирования системы с разделением доменов:** Соглашение о взаимодействии с системой разделения доменов.

10 **контроль потоков информации:** Проверка соответствия потоков информации в системе установленным требованиям политики безопасности.

11 **модуль:** Независимая и функционально законченная часть программы, оформленная в виде самостоятельного фрагмента кода, упакованная в отдельный файл или обособленная другим способом.

12 **монитор пересылок:** Компонент, который проверяет все запросы субъектов на доступ к объектам и гарантирует, что эти запросы, а также формируемые в результате осуществления доступа потоки данных, удовлетворяют определенной политике безопасности.

13 **объект:** Именованная сущность.

Примечание — В системе интернета вещей доступ к объекту может быть ограничен в соответствии с правами доступа.

14 **окружение домена:** Множество доменов интернета вещей, на которые может повлиять данный домен.

15 **политика безопасности в системе интернета вещей:** Набор правил и ограничений, формально определяющих, какие потоки данных разрешены (и/или запрещены), какие свойства безопасности, определяемые на атрибутах потоков данных, должны поддерживаться для конкретной системы интернета вещей.

Примечание — Формализованная политика безопасности иногда называется моделью безопасности.

16 **политика взаимодействий:** Политика безопасности, описывающая разрешенную связь между доменами.

17 **пользовательские процессы:** Процессы, которые запускаются из исполняемого (бинарного) файла пользователем и могут выполняться в интерактивном или фоновом режимах с привилегиями пользователя.

18 **поток информации:** Некоторый объем информации, разделяемый между объектами/субъектами в процессе осуществления доступа.

19 **предположение безопасности:** Условие или требование, которое считается выполненным для системы и которое каким-либо образом определяет или ограничивает достижение целей безопасности для этой системы.

Примечание — Предположение безопасности может касаться контекста использования системы интернета вещей, факторов, касающихся ее проектирования, разработки, сопровождения и вывода системы из эксплуатации, а также доверия к отдельным аппаратным или программным компонентам этой системы, алгоритмам, протоколам взаимодействия и технологиям.

20

прикладная программа (приложение): Программа, предназначенная для решения задачи или класса задач в определенной области применения системы интернета вещей.

[Адаптировано из ГОСТ 19781—90, статья 7]

21 **принцип безопасных сбоев:** Изоляция и обработка отказов для повышения надежности системы за счет обеспечения ее отказоустойчивого исполнения.

22 **принцип наименьших привилегий:** Разделение функций между доменами для минимизации необходимого домену множества операций взаимодействия с другими доменами, в том числе операций доступа к ресурсам.

Примечание — Использование данного принципа позволяет упростить проверку выполнения политики безопасности за счет декомпозиции сложных политик безопасности.

23 **промежуточное программное обеспечение** (**middleware**): Программное обеспечение, реализующее сервисные и вспомогательные функции, предназначенные для совместного использования прикладными программами и не составляющие часть ОС, необходимую для ее нормального функционирования

24 **пространственное разделение:** Тип разделения, который разделяет системные ресурсы путем их логического разделения, например путем разделения адресного пространства данных, а также реализует управление информационным потоком с учетом этого разделения и изоляцию отказов.

25 **процесс в операционной системе:** Выполнение пассивных инструкций компьютерной программы на процессоре ЭВМ.

Примечание — Всегда имеется процесс, соответствующий операционной системе (ОС).

26 **разделение доменов:** Системная архитектура, основанная на организации взаимодействия доменов, между которыми нет передачи управления и потоков информации кроме явно разрешенных политикой безопасности.

27 **связь между доменами:** Возможность сообщения доменов, организации доступа, порождающей в случае осуществления доступа поток информации между доменами.

28

система интернета вещей: Комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей обработки информации о физическом и виртуальном мире и реагирования на нее.

[Адаптировано из ГОСТ Р 57193—2016, пункт 4.1.44]

Примечания

1 Системный элемент является отдельной частью системы, которая может быть создана для полного выполнения заданных требований.

2 Элемент системы также может представлять собой систему.

29 **система с разделением доменов:** Система, реализующая подход с разделением доменов, на основе одной или нескольких архитектур политик.

30 **скрытый канал:** Непредусмотренный канал передачи информации или управляющего сигнала между доменами, который не был предназначен для организации связи между доменами и который не является контролируемым.

31 **средства безопасности:** Совокупность механизмов защиты в компьютерной системе, включая аппаратное и микропрограммное обеспечение и программное обеспечение, комбинация которых отвечает за реализацию политики безопасности.

32 **субъект:** Именованная активная сущность.

Примечание — В системе интернета вещей субъекту может быть назначен домен и предоставлена авторизация.

33

функциональная безопасность: Часть общей безопасности, обусловленная применением управляемого оборудования и системы управления управляемого оборудования и зависящая от правильности функционирования электрических и/или электронных, и/или программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска.

[ГОСТ Р МЭК 61508-4—2012, статья 3.1.12]

34 **цель безопасности:** Условие или требование, относящееся к системе в целом, которое должно выполняться для этой системы в любой момент времени на протяжении ее жизненного цикла и которое определяет в каком-либо аспекте безопасность этой системы относительно использования ее ресурсов или взаимодействия с окружающей средой.

Примечание — Набор целей безопасности, утвержденный для системы интернета вещей, определяет задачу обеспечения безопасности этой системы.

35 **ядерная архитектура безопасности операционной системы:** Архитектура, основанная на едином центральном доверенном компоненте, ядре безопасности, которое может перехватывать и контролировать системные операции для реализации политики безопасности.

36 **ядро безопасности операционной системы:** Тип ядра, реализующий в дополнение к базовым функциям ядра концепцию монитора пересылок.

Примечание — Ядро безопасности должно контролировать все доступы, быть защищенным от изменений и быть достаточно простым для возможности его верификации.

37 **ядро операционной системы:** Модуль операционной системы, обеспечивающий выполнение базовых функций по управлению ресурсами операционной системы и системы в целом.

38 **ядро разделения операционной системы:** Особый тип ядра безопасности, который ограничивается применением политик изоляции доменов и управления потоками информации между доменами, чтобы создать среду, которая не отличается от среды, предоставляемой физически распределенной системой.

Примечание — Основной механизм для реализации систем с разделением доменов. Базовая функциональность ядра разделения включает в себя: изоляцию доменов, связь между доменами, поддержку политики безопасности, управление памятью, планирование, обработку периодов, минимальное обслуживание прерываний, передачу прерываний по объектам, минимальное управление примитивами синхронизации, таймеры, сторожа и инструментацию.

Алфавитный указатель терминов на русском языке

авторизация 1
архитектура безопасности операционной системы ядерная 35
архитектура POSIX 2
архитектура политики 3
безопасность информации 4
безопасность данных 4
безопасность функциональная 33
декомпозиция в проектировании программного обеспечения 6
декомпозиция ПО 6
домен 7
доступ 8
интерфейс прикладного программирования системы с разделением доменов 9
канал скрытый 30
контроль потоков информации 10
модуль 11
монитор пересылок 12
обеспечение промежуточное программное (middleware) 23
объект 13
окружение домена 14
политика безопасности в системе интернета вещей 15
политика взаимодействий 16
поток информации 18
предположение безопасности 19
приложение прикладное 20
принцип безопасных сбоев 21
принцип наименьших привилегий 22
программа прикладная 20
процесс в операционной системе 25
процессы пользовательские 17
разделение временное 5
разделение доменов 26
разделение пространственное 24
связь между доменами 27
система интернета вещей 28
система с разделением доменов 29
средства безопасности 31
субъект 32
цель безопасности 34
ядро безопасности операционной системы 36
ядро операционной системы 37
ядро разделения операционной системы 38

УДК 004.738:006.354 ОКС 35.110

Ключевые слова: системы с разделением доменов, интернет вещей, термины и определения

Редактор *В.Н. Шмельков*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 15.03.2023. Подписано в печать 16.03.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации» для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru