ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58256— 2018

Защита информации

УПРАВЛЕНИЕ ПОТОКАМИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ. ФОРМАТ КЛАССИФИКАЦИОННЫХ МЕТОК

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Акционерным обществом «Научно-производственное объединение Русские базовые информационные технологии» (АО «НПО РусБИТех»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 октября 2018 г. № 849-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Применение средств защиты от несанкционированного доступа в информационных системах предполагает решение задачи обеспечения конфиденциальности, целостности и доступности информации при ее хранении, обработке и передаче. В целях реализации установленных в информационных системах правил разграничения доступа информация должна в обязательном порядке сопровождаться служебными атрибутами, содержащими сведения об уровне конфиденциальности, признаках классификации информации или иные необходимые сведения. Такими служебными атрибутами для применяемых в информационных системах средств защиты, осуществляющих мандатное управление доступом, являются классификационные метки.

Целью настоящего стандарта является определение единых правил формирования и передачи классификационных меток для обеспечения совместимости средств защиты при передаче информации с использованием протокола IP версии 4 (IPv4)[1)] в информационных системах, в которых реализовано мандатное управление доступом.

[1)] Протокол Интернета версии 4 (Internet Protocol version 4), определяемый международной спецификацией [1].

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УПРАВЛЕНИЕ ПОТОКАМИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ. ФОРМАТ КЛАССИФИКАЦИОННЫХ МЕТОК

Information protection. Management of information flows in information system. Interchange format of sensitivity labels

Дата введения — 2019—01—01

1 Область применения

Настоящий стандарт устанавливает общие требования к формату и правила установки классификационных меток в целях обеспечения совместимости средств защиты от несанкционированного доступа, осуществляющих мандатное управление доступом при передаче информации по протоколу IPv4.

Настоящий стандарт предназначен для разработчиков средств защиты от несанкционированного доступа, осуществляющих мандатное управление доступом.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1

конфиденциальность: Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

[ГОСТ Р ИСО/МЭК 27000—2012, пункт 2.9]

2.2 **классификационная метка**[1]**:** Служебный атрибут безопасности единицы информационного ресурса, представляющий собой комбинацию иерархических классификационных уровней (степеней секретности) и неиерархических классификационных признаков (категорий).

2.3

несанкционированный доступ: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа.

Примечания

1 Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

2 Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

[ГОСТ Р 53114—2008, статья 3.3.6]

2.4 **средство защиты от несанкционированного доступа** (средство защиты от НСД): Программное, аппаратное или программно-аппаратное средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

2.5 **система защиты информации от несанкционированного доступа:** Комплекс программно-аппаратных (в том числе криптографических) средств защиты от несанкционированного доступа и поддерживающих их организационных мер.

[1] Метка конфиденциальности по руководящему документу [2], метка безопасности согласно требованиям [3].

Издание официальное

2.6

совместимость: Способность продукта, системы или компонента обмениваться информацией с другими продуктами, системами или компонентами и/или выполнять требуемые функции при совместном использовании одних и тех же аппаратных средств или программной среды.

[ГОСТ Р ИСО/МЭК 25010—2015, пункт 4.2.3]

2.7 **субъект доступа;** субъект: Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.8 **объект доступа;** объект: Единица информационного ресурса, доступ к которой регламентируется правилами разграничения доступа.

2.9 **непривилегированный субъект доступа:** Субъект доступа, не имеющий полномочий по управлению средствами защиты от несанкционированного доступа.

2.10 **привилегированный субъект доступа:** Субъект доступа, имеющий полномочия по управлению средствами защиты от несанкционированного доступа.

2.11 **диспетчер доступа** (монитор обращений): Аппаратные и программные элементы средства защиты от несанкционированного доступа, осуществляющие контроль доступа субъектов к объектам.

2.12 **значение классификационной метки:** Совокупность значений, присваиваемых полям заголовка сетевых пакетов, при передаче информации по протоколу IPv4.

3 Общие положения

3.1 Настоящий стандарт определяет единые формат и правила установки классификационных меток в средствах защиты от несанкционированного доступа.

3.2 Соотнесение конкретных значений классификационных меток с уровнем конфиденциальности (степенью секретности) и признаками классификации информации осуществляется при проектировании информационной системы и не является предметом настоящего стандарта.

3.3 Соотнесение конкретных значений классификационных меток с уровнем конфиденциальности (степенью секретности) и признаками классификации информации при взаимодействии информационных систем осуществляется на основе соглашений об информационном взаимодействии и не является предметом настоящего стандарта.

3.4 При проектировании и разработке средств защиты от несанкционированного доступа необходимо руководствоваться: в части формата классификационных меток — положениями 4.1, а в части правил установки классификационных меток — положениями 4.2.

3.5 В случае применения аппаратных и программных средств передачи информации, а также средств криптографической защиты информации не должна быть нарушена целостность поля Опции[1)] в заголовке IP-пакета[2)], определенного в 4.1.2.

4 Формат и правила установки классификационных меток при сетевом взаимодействии

4.1 Формат классификационных меток

4.1.1 При передаче информации по протоколу IPv4 классификационные метки должны размещаться в каждом заголовке IP-пакета в поле Опции с типом Безопасность[3)].

Классификационная метка при передаче информации по протоколу IPv4 представляет собой совокупность полей, входящих в поле Опции заголовка IP-пакета.

При отсутствии поля Опции в составе заголовка IP-пакета следует считать, что данный пакет имеет метку с нулевым значением и не имеет категорий конфиденциальности.

4.1.2 Значения полей, входящих в поле Опции, совокупность которых определяет значение классификационной метки, устанавливаются в соответствии с таблицей 1.

---

1) Поле Options заголовка IP пакета.

2) Заголовок сетевого пакета в соответствии с [1].

3) Тип поля Опции — Security, используемого для обеспечения информационной безопасности в соответствии с международной спецификацией [4].

Таблица 1 — Значения полей, входящих в поле Опции[1)]

Поля, входящие в поле Опции	TYPE (8 бит)	LENGTH (8 бит)	CLASSIFICATION LEVEL (8 бит)	PROTECTION AUTHORITY FLAGS (11+ байт)
Значение поля	10000010	XXXXXXXX	10101011	AAAAAAA[1|0] AAAAAAA0

Значение поля TYPE равно 130 в десятичном представлении, что определяет тип поля Опции — Безопасность (Security).

Поле LENGTH содержит значение длины поля Опции в октетах. Минимальная длина поля Опции — 3 октета (байта), включая поля TYPE и LENGTH. Поле PROTECTION AUTHORITY FLAGS может отсутствовать. Значение поля LENGTH не должно превышать 40 октетов.

Значение поля LENGTH меньше 3 октетов должно обрабатываться как ошибка.

В поле CLASSIFICATION LEVEL всегда указывается значение 10101011 (Unclassified).

Поле PROTECTION AUTHORITY FLAGS имеет переменную длину. Младший бит каждого октета (байта) используется для индикации наличия следующего октета. Если бит равен 1, есть следующий октет, если бит равен 0 — октет последний. Ситуации, когда в соответствии со значением поля LENGTH октет является последним, но его младший бит не равен 0, либо октет не является последним, а младший бит равен 0, должны обрабатываться как ошибки.

Классификационная метка должна представлять собой структуру, которая включает 8 бит для кодирования уровня (беззнаковое целое число, 256 возможных значений) и до 251 бита для кодирования категорий. При этом кодирование категорий рекомендуется осуществлять с использованием 64-разрядной битовой маски, заканчивающейся младшим битом. Для увеличения числа категорий допускается применять комбинирование и группировку значений в пределах битовой маски.

Значение классификационной метки, равное нулю, соответствует информации, для которой не определены уровни конфиденциальности (степени секретности) и иные признаки классификации. Примером такой информации может являться общедоступная[2)] информация.

Структура должна быть упакована (полностью заполнена и выравнивание данных отключено). В поле PROTECTION AUTHORITY FLAGS классификационная метка записывается в виде последовательности бит. Начиная с младшего байта, вставляется младший бит признака продолжения со сдвигом остальных бит. Далее анализируются октеты с конца поля PROTECTION AUTHORITY FLAGS. В соответствии со спецификацией [4] те октеты, полезные 7 бит которых содержат 0, отбрасываются с корректировкой поля LENGTH.

Примеры

1 Общий вид заполнения поля PROTECTION AUTHORITY FLAGS битами значения уровня (L) и битовой маской категорий (C):

* *

LLLLLLL1 CCCCCCL1 CCCCCCC1 CCCCCCC1 CCCCCCC1 CCCCCCC1 CCCCCCC1 CCCCCCC1 CCCCCCC1 00000CC0

**** — указывает позицию младшего информационного бита для уровня и битовой маски категорий.***

2 Пошаговое кодирование классификационной метки с уровнем конфиденциальности 1 и категорией 0×11 с корректировкой поля длины и бита признака продолжения:

Исходные данные:

Уровень 1 — 00000001

Категория 3 — 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000011

Шаг 1: Исходная запись структуры:

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000011 00000001

Шаг 2: Деление на группы по 7 бит:

00 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000110 0000001

Шаг 3: Дополнение группы со старшими битами нулями до 7 бит:

0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000110 0000001

Шаг 4: Запись групп в обратном порядке:

0000001 0000110 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000

[1)] Наименования полей, входящих в поле Опции со значением поля TYPE, равным 130, в соответствии с международной спецификацией [4].

[2)] Термин используется в соответствии с Федеральным законом [5].

Шаг 5: Дополнение групп битом признака продолжения со сдвигом остальных бит в октете:
00000011 00001101 00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000000
Шаг 6: Отсечение заключительных октетов, 7 значащих бит которых равны 0, с корректировкой бита признака продолжения:
00000011 00001100
Результат: IPOPT_SEC[1],5,0×AB,0×03,0×0C.

4.1.3 Значение классификационной метки может быть равно нулю, кроме того, в классификационной метке могут отсутствовать категории.

Примеры
1 Кодирование нулевой классификационной метки:
IPOPT_SEC,3,0×AB.
Поле PROTECTION AUTHORITY FLAGS отсутствует.
2 Кодирование классификационной метки с уровнем конфиденциальности, равным 1:
IPOPT_SEC,4,0×AB,0×02.
Поле PROTECTION AUTHORITY FLAGS в виде битового списка:
00000010.
3 Кодирование классификационной метки с уровнем конфиденциальности, равным 2:
IPOPT_SEC,4,0×AB,0×04.
Поле PROTECTION AUTHORITY FLAGS в виде битового списка:
00000100.
4 Кодирование классификационной метки с уровнем конфиденциальности, равным 3:
IPOPT_SEC,4,0×AB,0×06.
Поле PROTECTION AUTHORITY FLAGS в виде битового списка:
00000110.

4.2 Правила установки классификационных меток

4.2.1 Все субъекты доступа, осуществляющие взаимодействие, делятся на привилегированные и непривилегированные субъекты доступа.

4.2.2 Взаимодействие между субъектами доступа должно осуществляться под контролем диспетчера доступа (монитора обращений).

4.2.3 Взаимодействие с использованием сетевых протоколов должно осуществляться через программный интерфейс объектов доступа, являющихся элементами межпроцессного и сетевого взаимодействия (например, сетевых сокетов), которые обеспечивают обмен данными, в том числе и с разными классификационными метками.

4.2.4 Изменять классификационную метку объекта доступа, являющегося элементом межпроцессного и сетевого взаимодействия (например, сетевых сокетов), может привилегированный субъект доступа.

---

[1] IPOPT_SEC — константное значение, численно равное 130 в десятичной системе исчисления, заданное для типа Безопасность.

Библиография

[1] RFC 791 Интернет-протокол. Программа интернета DARPA. Спецификация протокола [Internet protocol. DARPA internet program. Protocol specification, September 1981] доступен на https://tools.ietf.org/html/rfc791

[2] Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», Гостехкомиссия России, 1992

[3] «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», ФСТЭК России, 2013

[4] RFC 1108 Опция безопасности интернет-протокола [Security Options for the Internet Protocol, November 1991] доступен на https://tools.ietf.org/html/rfc1108

[5] Федеральный закон от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации

УДК 004:006.354 ОКС 35.020

Ключевые слова: защита информации, метка конфиденциальности, управление потоками информации, классификационная метка, формат, метка безопасности, средство защиты от несанкционированного доступа, система защиты информации от несанкционированного доступа, контроль доступа, защита информации, диспетчер доступа, монитор обращений

БЗ 11—2018/21

Редактор *Л.И. Нахимова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 29.10.2018. Подписано в печать 08.11.2018. Формат 60×84$^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,12.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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