ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56035— 2014

Системы охранные телевизионные

ЗАЩИТА ОЦИФРОВАННЫХ ВИДЕОДАННЫХ ОТ СЛУЧАЙНОГО И ПРЕДНАМЕРЕННОГО ИСКАЖЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Закрытым акционерным обществом «Нордавинд» и Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 234 «Системы тревожной сигнализации и противокриминальной защиты»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 июня 2014 г. № 527-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Сентябрь 2019 г.

*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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2015, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Введение

Системы охранные телевизионные предназначены для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты. Полученные оцифрованные видеоданные должны быть защищены от случайного и преднамеренного искажения. Настоящий стандарт позволяет упорядочить существующие и разрабатываемые методы защиты оцифрованных видеоданных, предназначенных для применения в составе систем противокриминальной защиты.

Выполнение методов защиты, указанных в настоящем стандарте, должно гарантировать подлинность оцифрованных видеоданных при передаче между частями охранных телевизионных систем и хранении.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системы охранные телевизионные

ЗАЩИТА ОЦИФРОВАННЫХ ВИДЕОДАННЫХ ОТ СЛУЧАЙНОГО И ПРЕДНАМЕРЕННОГО ИСКАЖЕНИЯ

Общие требования

Video surveillance systems.
Resistance for digital video data to accidental or deliberate distortion. General requirements

Дата введения — 2015—09—01

1 Область применения

Настоящий стандарт распространяется на цифровые системы охранные телевизионные (далее — ЦСОТ) и устанавливает общие технические требования к применению различных методов защиты оцифрованных видеоданных в ЦСОТ от случайного и преднамеренного искажения в процессе их передачи и хранения.

В настоящем стандарте не рассматриваются методы защиты от искажений, возникающих в результате нарушения способов подключения, настройки аппаратуры и других физических воздействий.

Настоящий стандарт следует применять совместно с ГОСТ Р 51558, ГОСТ Р 54830, ГОСТ Р 34.11 и ГОСТ Р ИСО/МЭК 27002.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 19.401 Единая система программной документации. Текст программы. Требования к содержанию и оформлению

ГОСТ 19.402 Единая система программной документации. Описание программы

ГОСТ 19.404 Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению

ГОСТ Р 34.10 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р 51558 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 54830 Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом ут-

Издание официальное

верждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **IP-адрес** (internet protocol address): Уникальный сетевой адрес узла (внешний или внутренний) в компьютерной сети, построенный по протоколу IP.

3.2 **RTSP** (real-time streaming protocol): Протокол потоков в реальном масштабе времени, представляющий собой протокол прикладного уровня, предназначенный для контроля доставки данных приложений реального времени.

3.3 **SDP** (session description protocol): Сетевой протокол, предназначенный для описания сессии передачи потоковых данных.

Примечание — SDP-сообщение может содержать адреса места назначения; номера UDP-портов для отправителя и получателя; медиа-форматы, которые могут применяться во время сессии; время старта и остановки.

3.4 **UDP-порт** (user datagram protocol): Программный адрес, используемый для взаимодействия различных конечных точек (сетевых устройств) в компьютерных сетях.

3.5 **UTC-время** (universal time, coordinated): Стандарт, по которому общество регулирует часы и время.

3.6

видеоданные (video data), **видеопоток** (video stream): Аналоговый сигнал, несущий информацию о пространственно-временных параметрах изображений.

[ГОСТ Р 54830—2011, статья 3.1]

3.7

видеокамера: Устройство для преобразования оптического изображения в электрический видеосигнал. Первичный источник видеосигнала в составе системы охранной сигнализации.

[ГОСТ Р 51558—2008, статья 3.3]

3.8 **видеоконтейнер** (video container): Формат файла или видеопотока, в котором сохраняются или передаются видеоряд и служебная информация, предназначенные для дальнейшей обработки/анализа видеоряда, либо составная часть иного файла и контейнера, предназначенная для хранения и передачи видеоряда и служебной информации.

Примечание — Спецификация видеоконтейнера описывает способ представления передаваемых данных, может накладывать ограничения на алгоритмы их кодирования.

3.9 **видеоряд** (video series): Последовательность кадров, поочередно заменяющих друг друга с высокой скоростью.

3.10 **группа кадров:** Определенное число последовательных кадров видеоданных.

3.11 **закрытый ключ** (private key): Секретная часть пары алгоритмов асимметричного шифрования, составляющая для ЭЦП уникальную последовательность символов, известную владельцу сертификата ключа подписи и предназначенную для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

3.12 **кадр** (frame): Элемент видеоряда, отдельное изображение.

3.13 **контрольная сумма** (check sum): Число, рассчитанное путем проведения определенных операций над входными данными, обычно используемое для проверки правильности передачи данных по каналам связи.

Примечание — В настоящем стандарте термин «контрольная сумма» используется для обозначения механизма некриптографического контроля информации.

3.14 **локальное время** (local time): Время, установленное на видеоисточнике.

3.15

несанкционированные действия; НСД: Преднамеренные действия, направленные на нарушение правильности функционирования системы.

[ГОСТ Р 51558—2008, статья 3.13]

3.16 **опорный кадр** (key frame): Кадры, в которых картинка в кадре существенно меняется.

3.17

оцифрованные видеоданные (digitized video data): Данные, полученные путем аналого-цифрового преобразования видеоданных, представляющие собой последовательность байтов в некотором формате (RGB, YUV или др.).

[ГОСТ Р 54830—2011, статья 3.2]

3.18 **подлинность видеоданных** (authenticity video data): Свойство системы сохранять неизменность или обнаруживать факт несанкционированного изменения информации и атрибутов, устанавливающих авторство.

3.19

система охранная телевизионная; СОТ: Телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты.

[ГОСТ Р 51558—2008, статья 3.20]

3.20 **служебная информация** (overhead information): Информация, добавляемая к кадру или группе кадров, содержащая нумерацию, дату и время передачи, а также другие данные, определяемые спецификой работы СОТ.

3.21 **сообщение** (message): Строка бит ограниченной длины.

3.22

техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

[ГОСТ Р 50922—2006, статья 2.2.2]

3.23

формат оцифрованных видеоданных (digitized video data format): Представление оцифрованных видеоданных, обеспечивающее их обработку цифровыми вычислительными средствами.

Примечание — Формат оцифрованных видеоданных включает в себя используемую цветовую модель и размерность (количество бит) представления каждого канала для используемой цветовой модели.

[ГОСТ Р 54830—2011, статья 3.3]

3.24 **фрагмент кадра** (frame fragment): Часть кадра, содержащая информацию об изображении.

3.25 **хеш-функция** (hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая установленным в настоящем стандарте свойствам.

3.26 **целостность видеоданных** (video data integrity): Обеспечение достоверности и полноты информации и методов ее обработки.

3.27

[электронная цифровая] подпись (signature), ЭЦП: Строка бит, полученная в результате процесса формирования подписи.

Примечания

1 Строка бит, являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

2 В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины «электронная подпись», «цифровая подпись» и «электронная цифровая подпись» являются синонимами.

[ГОСТ Р 34.10—2012, статья 3.1.15]

4 Общие положения

4.1 Хеш-функция должна удовлетворять следующим свойствам:

- по данному значению функции сложно вычислить исходные данные, отображаемые в этом значении;

- для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в этом значении,
- сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

4.2 Оцифрованные видеоданные могут иметь следующие виды искажений:
- подмену кадра или группы кадров;
- подмену фрагмента(ов) кадра или группы кадров;
- изменение порядка следования кадров или групп кадров;
- удаление кадра или групп кадров;
- потерю служебной информации, связанной с видеорядом;
- искажение служебной информации, связанной с видеорядом;
- удаление, добавление, изменение объектов, предметов, участков изображения внутри кадра;
- удаление, добавление, изменение числового и/или временного маркера (даты и времени);
- ухудшение качества изображения (перезапись, перекодирование).

Примечание — Указанные искажения могут появиться в результате случайного или преднамеренного воздействия.

4.3 В целях защиты информации устанавливают следующие уровни защиты оцифрованных видеоданных:
- уровень I — защита от случайных и преднамеренных искажений;
- уровень II — защита от случайных искажений.

Примечание — Назначение конкретного уровня защиты для оцифрованных видеоданных определяет владелец информации.

5 Общие требования

5.1 Методы защиты оцифрованных видеоданных от случайных или преднамеренных искажений должны быть разработаны (модернизированы) в соответствии с требованиями настоящего стандарта, нормативных документов (НД) и/или другой технической документации на СОТ конкретного типа.

5.2 Документация, подтверждающая применяемый уровень защиты оцифрованных видеоданных от случайных или преднамеренных искажений, должна соответствовать ГОСТ 19.401, ГОСТ 19.402, ГОСТ 19.404.

5.3 Обязательным для всех уровней защиты оцифрованных видеоданных от случайных и преднамеренных искажений является использование видеоформатов/видеоконтейнеров с возможностью ресинхронизации видеопотока при потере/повреждении заголовка, т. е. таких, заголовок которых начинается с маркера синхронизации, позволяющего однозначно определить следующий заголовок при повреждении предыдущего.

5.4 Требования к защите оцифрованных видеоданных уровня I

5.4.1 Уровень I защиты оцифрованных видеоданных реализуют добавлением информации к оцифрованным видеоданным и подписанием группы кадров электронной цифровой подписью (ЭЦП).

5.4.1.1 Добавляемая информация к оцифрованным видеоданным должна содержать нумерацию группы кадров, информацию о времени передачи и технические характеристики видеоисточника.

5.4.1.2 Требования к нумерации группы кадров:
- группы кадров следует нумеровать последовательно по возрастанию;
- нумерация должна начинаться с 1;
- шаг нумерации равен 1.

5.4.1.3 Информация о времени передачи должна содержать:
- время (часы, минуты);
- дату (день, месяц, год);
- разницу между UTC и локальным временем.

5.4.1.4 Информация к техническим характеристикам видеоисточника должна содержать:
- SDP-сообщение при передаче оцифрованных видеоданных протоколом RTSP (см. [1]);
- IP-адрес передающей видеокамеры при передаче оцифрованных видеоданных протоколом, отличным от RTSP;
- номер последнего опорного кадра для сжатых кадров.

5.4.2 Требования к ЭЦП:

- добавление ЭЦП для каждой группы кадров оцифрованных видеоданных является обязательным;
- ЭЦП должна генерироваться в режиме реального времени;
- расчет хеш-функции для ЭЦП должен выполняться после добавления информации в видеоданные;
- формирование и проверку ЭЦП следует осуществлять по ГОСТ Р 34.10;
- источники видеоинформации должны иметь техническую защиту, исключающую возможность съема и/или подмены закрытого ключа, согласно [2]. Организация этой технической защиты в настоящем стандарте не рассматривается.

5.5 Требования к защите оцифрованных видеоданных уровня II

5.5.1 Уровень II защиты оцифрованных видеоданных реализуют алгоритмом расчета контрольной суммы.

5.5.1.1 Требования к контрольной сумме:

- размер регистра для вычислений должен обеспечивать вероятность ошибки не более 2^{-32};
- алгоритм расчета контрольной суммы должен обеспечивать изменение в среднем 50 % битов контрольной суммы при изменении одного бита входных данных.

Рекомендуется использовать алгоритм CRC32 (см. [3]).

Библиография

[1] RFC 2326—1998 Потоковый протокол реального времени (Real time streaming protocol) [Электронный ресурс]. URL: gost.e-ecolog.ru (дата обращения: 20.05.2013)

[2] Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622)

[3] IEEE 802.3—2001 Циклический избыточный код (Cyclic redundant code) [Электронный ресурс]. URL: ttp://standards.ieee.org/about/get/802/802.3.html (дата обращения: 20.04.2013)

УДК 621.398:006.354 ОКС 13.320

Ключевые слова: системы охранные телевизионные, видеоданные, защита информации, электронная цифровая подпись, методы защиты видеоданных

Редактор *Е.И. Мосур*
Технические редакторы *В.Н. Прусакова, И.Е. Черепкова*
Корректор *Е.М. Поляченко*
Компьютерная верстка *Г.В. Струковой*

Сдано в набор 30.09.2019. Подписано в печать 20.10.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,00.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru stinfo.ru

gost.e-ecolog.ru