ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56102.2— 2015

СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ

Часть 2

Подсистема объектовая. Общие технические требования и методы испытаний

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным казенным учреждением «Научно-исследовательский центр «Охрана» Министерства внутренних дел Российской Федерации» (ФКУ НИЦ «Охрана» МВД России), Главным Управлением вневедомственной охраны Министерства внутренних дел Российской Федерации (ГУВО МВД России) 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 20 октября 2015 г. № 1591-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, 2016, 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

Технический комитет по стандартизации «Системы тревожной сигнализации и противокриминальной защиты» (ТК 234), функционирующий на базе ФКУ НИЦ «Охрана» МВД России, разрабатывает комплекс национальных стандартов Российской Федерации на системы централизованного наблюдения.

С 1 января 2016 года вводится в действие ГОСТ Р 56102.1—2014 «Системы централизованного наблюдения. Часть 1. Общие положения».

Настоящий стандарт является второй частью в указанном комплексе стандартов и устанавливает общие требования и методы испытаний к одной из трех подсистем, входящих в систему централизованного наблюдения, — к подсистеме объектовой.

Далее планируются к разработке национальные стандарты, регламентирующие общие технические требования и методы испытаний к подсистеме передачи информации и подсистеме пультовой, соответственно, третья и четвертая части комплекса стандартов на системы централизованного наблюдения.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ

Часть 2

Подсистема объектовая. Общие технические требования и методы испытаний

Centralized security monitoring systems. Part 2. Subsystem for mounting at protected facility. General technical requirements and test methods

Дата введения — 2017—01—01

1 Область применения

Настоящий стандарт распространяется на объектовые подсистемы и входящие в них технические средства и модули в составе вновь разрабатываемых и модернизируемых систем централизованного наблюдения (далее — СЦН) и устанавливает общие технические требования и методы испытаний к ним.

Настоящий стандарт не распространяется на системы оптико-электронного наблюдения и оценки обстановки технических средств физической защиты ядерно опасных объектов, а также на системы централизованного наблюдения специального назначения.

Настоящий стандарт следует применять совместно с ГОСТ Р 56102.1.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.601 Единая система конструкторской документации. Эксплуатационные документы

ГОСТ 2.610 Единая система конструкторской документации. Правила выполнения эксплуатационных документов

ГОСТ 12.1.006 Системы стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля

ГОСТ 32321 Извещатели охранные поверхностные ударно-контактные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний

ГОСТ Р 34025 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний

ГОСТ IEC 61142—2011 Обмен данными при считывании показаний счетчиков, тарификации и управлении нагрузкой. Обмен данными по локальной шине

ГОСТ Р 8.568 Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения

ГОСТ Р 12.1.019 Системы стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты

ГОСТ Р 15.301 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство

ГОСТ Р 50658—94 (МЭК 60839-2-4:1990) Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений

Издание официальное

ГОСТ Р 50659 Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний

ГОСТ Р 50777 Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний

ГОСТ Р 51241 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

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

ГОСТ Р 52434—2005 (МЭК 60839-2-3:1987) Извещатели охранные оптико-электронные активные. Общие технические требования и методы испытаний

ГОСТ Р 52436 Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний

ГОСТ Р 52650 Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний

ГОСТ Р 52651 Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний

ГОСТ Р 52933 Извещатели охранные поверхностные емкостные для помещений. Общие технические требования и методы испытаний

ГОСТ Р 53560 Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 53702 Извещатели охранные поверхностные вибрационные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний

ГОСТ Р 53704 Системы безопасности комплексные и интегрированные. Общие технические требования

ГОСТ Р 54126 Оповещатели охранные. Классификация. Общие технические требования и методы испытаний

ГОСТ Р 54455 Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам

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

ГОСТ Р 54832 Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний

ГОСТ Р 55150 Извещатели охранные комбинированные ультразвуковые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний

ГОСТ Р 56035 Системы охранные телевизионные. Защита оцифрованных видеоданных от случайного и преднамеренного искажения. Общие требования

ГОСТ Р 56047 Системы охранные телевизионные. Компрессия оцифрованных аудиоданных. Классификация. Общие требования и методы оценки алгоритмов

ГОСТ Р 56102.1 Системы централизованного наблюдения. Часть 1. Общие положения

ГОСТ Р ИСО 13373-1 Контроль состояния и диагностика машин. Вибрационный контроль состояния машин. Часть 1. Общие методы

ГОСТ Р ИСО/МЭК 7498-1 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

ГОСТ Р МЭК 60079-0 Взрывоопасные среды. Часть 0. Оборудование. Общие требования

ГОСТ Р МЭК 61511-1 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования

ГОСТ Р МЭК 61511-2 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1

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-

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 термины по ГОСТ Р 56102.1 и следующие термины с соответствующими определениями:

3.1

криминальная угроза: Угроза, связанная с несанкционированным проникновением на охраняемый объект (объект защиты) и/или совершением на его территории противоправных действий, в том числе террористических.

[ГОСТ Р 54126—2010, пункт 3.2]

3.2

(охранный) оповещатель: Техническое средство охранной сигнализации, предназначенное для оповещения людей о возникновении криминальной угрозы на охраняемом объекте.

[ГОСТ Р 54126—2010, пункт 3.3]

3.3

средства контроля и управления доступом (средства КУД): Механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

[ГОСТ Р 51241—2008, пункт 3.30]

3.4

средство охранного освещения: Осветительный прибор или устройство, предназначенное для освещения охраняемой зоны.

[ГОСТ Р 52551—2006, статья 2.7.113]

3.5 **верхний уровень интерфейса объектового:** Уровень представления и прикладной уровень, соответствующие модели по ГОСТ Р ИСО/МЭК 7498-1 и обеспечивающие представление и защиту информации от несанкционированных воздействий данных и доступ к информационным службам.

3.6 **нижний уровень интерфейса объектового:** Физический уровень, уровень звена данных, сетевой уровень, транспортный и сеансовый уровни, соответствующие модели по ГОСТ Р ИСО/МЭК 7498-1 и обеспечивающие арбитраж сети, определение начала и конца передачи, адресацию устройств в сети и контроль целостности передачи.

3.7 **протокол обмена информацией:** Техническая реализация, объединяющая интерфейс объектовый и интерфейс подсистемы передачи информации в составе системы централизованного наблюдения.

4 Общие технические требования

4.1 Общие требования

4.1.1 Объектовая подсистема должна обеспечивать возможность интеграции различных технических средств и модулей в единый аппаратно-программный комплекс СЦН.

4.1.2 Разработку и постановку на производство СЦН и компонентов, входящих в состав СЦН, следует осуществлять в соответствии с требованиями ГОСТ Р 15.201.

4.1.3 Конструкторскую документацию на СЦН и компоненты, входящие в состав СЦН, следует выполнять в соответствии с требованиями Единой системы конструкторской документации, а также ГОСТ 2.601 и ГОСТ 2.610.

4.1.4 Технические средства и модули, входящие в состав СЦН (далее — технические средства и модули), должны соответствовать требованиям пожарной безопасности по [1].

4.1.5 Объектовая подсистема СЦН должна состоять из одного или более центрального средства сбора и обработки информации (далее — ССОИ) и подключенных к нему технических средств и модулей.

4.2 Требования к объектовому интерфейсу

4.2.1 Объектовый интерфейс должен обеспечивать двустороннюю передачу информации между техническими средствами и модулями в составе объектовой подсистемы СЦН.

4.2.2 Объектовый интерфейс должен быть открытым и универсальным для обеспечения возможности включения в состав СЦН технических средств различных изготовителей.

4.2.3 Для физической реализации объектового интерфейса следует применять открытый стандарт связи физического уровня для проводных линий связи (далее — ЛС).

Примечание — В качестве открытого стандарта связи физического уровня для проводных ЛС рекомендуется использовать EIA RS-485 [2].

Для реализации объектового интерфейса допускается применять открытый стандарт связи физического уровня беспроводных линий.

4.2.4 Объектовый интерфейс должен обеспечивать подключение восьми или более устройств одновременно.

4.2.5 Объектовый интерфейс должен обеспечивать определение отсутствия связи с любым из устройств, входящих в состав объектовой подсистемы максимальной емкости, за время не более 10 с для проводных подсистем и 120 с — для беспроводных (радиоканальных).

4.2.6 Объектовый интерфейс должен обеспечивать прием тревожной информации от устройств, входящих в состав объектовой подсистемы максимальной емкости, с задержкой времени не более 10 с для проводных подсистем и 15 с — для беспроводных (радиоканальных).

4.2.7 Объектовый интерфейс должен обеспечивать порядок определения приоритета передачи информации, адресацию устройств в сети, определение начала и конца передачи, контроль целостности, представление информации и защиту ее от несанкционированных воздействий, доступ к информационным службам.

4.2.8 Объектовый интерфейс должен обеспечивать возможность приема, передачи и идентификации следующей информации: тревога, неисправность, саботаж работы устройства, внимание, взятие/снятие, обработка команд управления, связь, информационно-диагностические сообщения, телеметрия.

Перечень назначения используемых широковещательных и адресных функций, классов событий и их обозначения при передаче информации должны быть опубликованы в открытом доступе.

Примечание — Допускается поддержка объектовым интерфейсом передачи дополнительной информации.

4.2.9 Нижний уровень объектового интерфейса должен быть построен таким образом, чтобы устройство, реализующее его корректно, но не реализующее верхний (прикладной) уровень (или отдельные его функции), могло быть подключено по объектовому интерфейсу и начать корректно функционировать в объектовой подсистеме.

4.2.10 Объектовый интерфейс должен обеспечивать возможность идентификации всех технических средств и модулей при каждом сеансе информациионного обмена (передачи информации).

4.2.11 Нижний уровень объектового интерфейса должен обеспечивать контроль целостности передаваемых сообщений.

4.2.12 Верхний уровень объектового интерфейса должен поддерживать следующие форматы данных:

- незащищенное от несанкционированных воздействий (открытое) сообщение;
- защищенное от несанкционированных воздействий сообщение.

Примечание — Полный перечень форматов данных указывают в техническом описании объектового интерфейса или протокола обмена информацией.

4.2.13 Верхний уровень объектового интерфейса должен реализовывать алгоритм защиты, направленный на исключение подмены данных путем перехвата сообщений, подмены технических средств и модулей, несанкционированного управления техническими средствами и модулями объектовой подсистемы. В алгоритме следует применять закрытый ключ длиной не менее 128 бит.

Закрытый ключ следует использовать в модифицированном виде для исключения повторяемости одинаковых сообщений.

Примечание — Пример организации передачи данных по объектовому интерфейсу представлен на рисунке 1.

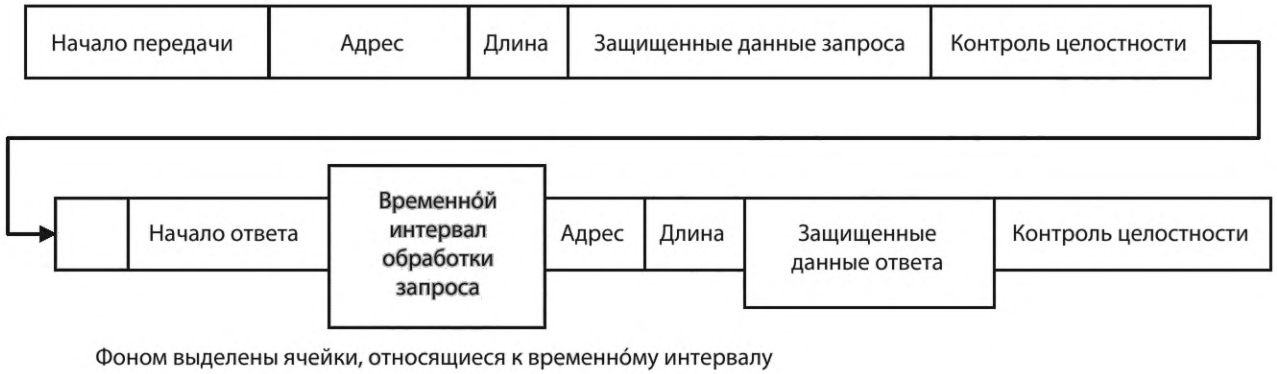


Рисунок 1 — Пример структуры обмена сообщениями в объектовом интерфейсе

4.2.14 Объектовый интерфейс должен обеспечивать:

- гарантированную доставку на ССОИ извещений обнаружения проникновения (попытки проникновения) в зоне охраны с указанием адреса (номера) зоны;
- передачу информации о состоянии технических средств, обеспечивающих контроль состояния зоны охраны и передачу извещений;
- управление техническими средствами и модулями объектовой подсистемы.

4.2.15 В объектовом интерфейсе на прикладном уровне должна быть предусмотрена поддержка команд, обеспечивающих функционирование аппаратных способов защиты от обрыва и короткого замыкания ЛС.

4.2.16 Для обеспечения контроля целостности данных необходимо использовать хэш-функции контроля целостности сообщений не ниже CRC16 по ГОСТ IEC 61142—2011 (приложение А).

4.2.17 Верхний уровень объектового интерфейса должен предоставлять доступ к информационным службам.

В техническом описании объектового интерфейса или протокола обмена информацией должны быть регламентированы правила ответа в случаях, когда технические средства и модули не поддерживают определенные функции или не обладают необходимой информацией для ответа.

4.2.18 Прикладной уровень объектового интерфейса должен поддерживать передачу следующих классов событий:

- «ТРЕВОГА» — тревожные сообщения, прямая опасность для жизни людей или сохранности имущества;
- «САБОТАЖ» — сообщения о вероятных действиях злоумышленника, направленных на вывод объектовой подсистемы из строя или нарушение ее функционирования;
- «НЕИСПРАВНОСТЬ» — сообщения о зарегистрированных неисправностях в технических средствах, модулях и линиях связи объектовой подсистемы, приводящих к сбоям в ее работе или потере заложенного функционала;
- «ВНИМАНИЕ» — сообщения о возможной, неподтвержденной опасности для жизни людей или сохранности имущества в тех случаях, когда требуется дополнительное подтверждение. Виды конкретных сообщений должны дублировать сообщения из категории «ТРЕВОГА»;
- «ОХРАНА» — сообщения о постановке на охрану или снятии с нее;
- «КОНТРОЛЬ» — сообщения об активных действиях пользователей или автоматических реакциях системы, изменяющих условия функционирования объектовой подсистемы;
- «ПИТАНИЕ» — сообщения об изменении условий электропитания технических средств и модулей, не приводящих к изменению в функционировании системы на данный момент времени;
- «СВЯЗЬ» — сообщения об изменениях состояния внутренних ЛС объектовой подсистемы, не приводящих к существенному изменению в функционировании системы на данный момент времени;
- «ИНФОРМАЦИЯ» — информационно-диагностические сообщения о состоянии детальной информации по техническим средствам и модулям.

Полный список классов сообщений и виды сообщений должен определять разработчик СЦН.

4.3 Требования к техническим средствам и модулям

4.3.1 Конструкция технических средств должна обеспечивать их подключение по линии связи по объектовому интерфейсу и возможность передачи информации на ССОИ.

Примечание — Допускается включать в состав СЦН по объектовому интерфейсу ССОИ интегрированных систем безопасности по ГОСТ Р 53704, работающих по закрытым проводным или беспроводным линиям связи, а также приемно-контрольный прибор по ГОСТ Р 52436.

4.3.2 Технические средства и модули должны соответствовать требованиям устойчивости к внешним воздействующим факторам по ГОСТ Р 54455.

4.3.3 Требования к средствам сбора и обработки информации

4.3.3.1 ССОИ в составе объектовой подсистемы должны обеспечивать функции приема и сбора информации от извещателей и других технических средств, включенных в ЛС по объектовому интерфейсу, контроля состояния подключенных технических средств и ЛС, формирования информации для последующей передачи на подсистему передачи информации.

4.3.3.2 ССОИ должны обеспечивать:

- оперативную передачу на ССОИ более высокого уровня объектовой подсистемы или на подсистему передачи информации данные о тревоге, саботаже или неисправности, а также другой информации о параметрах всех подключенных устройств и ССОИ;
- передачу полной информации о состоянии каждого из подключенных устройств и ССОИ по запросу на ССОИ более высокого уровня объектовой подсистемы или на подсистему передачи информации.

Примечание — Допускается отсутствие формирования тревожного извещения при срабатывании извещателей при его формировании в ССОИ на основе мажоритарной логики. Рекомендуется передача сообщения класса «ВНИМАНИЕ».

4.3.4 Требования к охранным извещателям

В зависимости от вида охранных извещателей, предназначенных для использования в составе объектовой подсистемы, что должно быть отражено в нормативно-технической документации (далее — НТД) на СЦН конкретного типа, охранные извещатели должны соответствовать требованиям ГОСТ 32321, ГОСТ 34025, ГОСТ Р 50658, ГОСТ Р 50659, ГОСТ Р 50777, ГОСТ Р 52434, ГОСТ Р 52650, ГОСТ Р 52651, ГОСТ Р 52933, ГОСТ Р 53702, ГОСТ Р 54832 и ГОСТ Р 55150.

4.3.5 Требования к модулям управления и индикации состояния

Модули управления и индикации состояния в составе объектовой подсистемы должны обеспечивать функции управления техническими средствами управления постановкой и снятием с охраны и соответствовать требованиям ГОСТ Р 52436.

4.3.6 Требования к средствам электропитания

4.3.6.1 Основное электропитание объектовой подсистемы следует осуществлять от сети переменного тока частотой 50 ±1 ГЦ и номинальным напряжением 220 В.

Средства электропитания должны обеспечивать работоспособность при допустимых отклонениях напряжения сети от минус 15 % до плюс 10 %.

Примечание — Допускается электропитание отдельных технических средств объектовой подсистемы, осуществляемое от источников с иными параметрами выходных напряжений, требования к которым устанавливают в НД на технические средства конкретного типа.

4.3.6.2 Источники электропитания в составе объектовой подсистемы должны соответствовать требованиям ГОСТ Р 53560.

4.3.7 Требования к охранным оповещателям

Охранные оповещатели, предназначенные для применения в составе объектовой подсистемы, должны соответствовать требованиям ГОСТ Р 54126.

4.3.8 Требования к средствам активной защиты

Средства активной защиты в составе объектовой подсистемы (средства искусственного задымления, звукового, светового воздействия и др.) должны обеспечивать психологическое и/или физическое воздействие на нарушителя.

Если в качестве создания в окружающем пространстве условий, препятствующих осуществлению противоправных действий и привлечения внимания к охраняемому объекту или предмету охраны, используют технические средства искусственного задымления, следует руководствоваться стандартом [3].

Технические средства активной защиты иных видов должны соответствовать требованиям, установленным в НД на СЦН конкретного типа.

4.3.9 Требования к охранным телевизионным средствам

4.3.9.1 Охранные телевизионные средства в составе объектовой подсистемы должны соответствовать требованиям ГОСТ Р 51558.

4.3.9.2 Охранные телевизионные средства в составе объектовой подсистемы должны обеспечивать выполнение алгоритмов компрессии видеоданных по ГОСТ Р 54830.

4.3.9.3 Охранные телевизионные средства в составе объектовой подсистемы должны обеспечивать защиту видеоданных от случайного или преднамеренного искажения по ГОСТ Р 56035.

4.3.9.4 Охранные телевизионные средства в составе объектовой подсистемы должны соответствовать требованиям компрессии аудиоданных по ГОСТ Р 56047.

4.3.10 Требования к средствам контроля и управления доступом

Средства контроля и управления доступом в составе объектовой подсистемы должны соответствовать требованиям ГОСТ Р 51241.

4.3.11 Требования к средствам охранного освещения

4.3.11.1 Средства охранного освещения в составе объектовой подсистемы должны обеспечивать необходимые условия видимости ограждения территории, периметра зданий, зон объекта, внешней территории, прилегающей к объекту, дорог и путей, предназначенных для организации охраны объекта, мест охраны.

К средствам охранного освещения относят осветительные приборы, кабельные и проводные сети, средства управления.

4.3.11.2 Средства охранного освещения должны состоять из основных средств и дополнительных (тревожное охранное освещение).

Основные средства охранного освещения должны обеспечивать требуемый уровень освещенности контролируемых зон.

Дополнительные средства охранного освещения предназначены для расширения возможности обзора контролируемых зон.

Примечание — При применении охранных телевизионных средств основные средства освещения должны обеспечивать необходимый уровень освещенности в зоне обзора камеры.

4.3.11.3 Основные средства охранного освещения должны обеспечивать непрерывную работу в темное время суток.

Дополнительные средства охранного освещения должны включаться при нарушении контролируемых зон в условиях недостаточной освещенности.

4.3.11.4 Средства охранного освещения должны обеспечивать:

- горизонтальную освещенность на уровне земли или вертикальную на плоскости ограждения, стены не менее 0,5 лк в темное время суток;
- равномерно освещенную сплошную полосу шириной не менее 3 м;
- возможность ручного и автоматического включения дополнительных источников света на отдельном участке (зоне) охраняемой территории (периметра) при срабатывании технических средств охранной сигнализации;
- ручное управление работой освещения из помещения охраны и на пункт централизованной охраны;
- совместимость с техническими средствами охранной сигнализации и охранного телевидения;
- непрерывность работы в помещении и на постах охраны.

4.3.11.5 Средства охранного освещения должны обеспечивать освещенность не менее 150 лк в местах проведения проверки документов.

4.3.11.6 Сеть охранного освещения по периметру объекта и на его территории должна быть выполнена отдельно от сети наружного освещения и разделена на самостоятельные участки в соответствии с участками охранной сигнализации периметра и/или охранного телевидения. Сеть охранного освещения должна быть подключена к отдельной группе щита освещения, расположенного в помещении охраны. Щит освещения должен быть закрыт на замок и оборудован охранной сигнализацией.

4.3.11.7 Лампы охранного освещения должны быть защищены от механических повреждений.

4.3.12 Требования к технологическим извещателям

В целях повышения защищенности объекта путем обнаружения техногенных угроз в состав объектовой подсистемы могут входить технологические извещатели для автоматического контроля различных параметров.

Технологические извещатели в составе объектовой подсистемы в зависимости от вида должны соответствовать требованиям ГОСТ Р МЭК 60079-0 и ГОСТ Р ИСО 13373-1, а также требованиям, установленным в НД на СЦН конкретного типа.

5 Методы испытаний

5.1 Общие положения

5.1.1 Испытания технических средств и модулей проводят методами, принятыми в соответствующих стандартах, а также по методикам испытаний, установленным в НД на СЦН конкретного типа.

Объем и последовательность испытаний следует устанавливать в НД на технические средства и модули конкретного типа.

5.1.2 Средства измерений, применяемые при проведении испытаний, должны быть поверены в установленном порядке, а оборудование аттестовано в соответствии с ГОСТ Р 8.568.

5.1.3 При проведении испытаний должны быть обеспечены требования техники безопасности.

Безопасность проведения работ, использования приборов, инструментов и оборудования должна быть обеспечена выполнением требований ГОСТ 12.1.006, ГОСТ Р 12.1.019.

Помещения для проведения испытаний должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование должны быть использованы в соответствии с инструкциями.

5.1.4 Образцы технических средств и модулей следует предъявлять на испытания с технической документацией в объеме, необходимом для проведения испытаний, и укомплектованными в соответствии с технической документацией.

5.1.5 Испытания технических средств и модулей на устойчивость к внешним воздействующим факторам по 4.3.2 следует проводить в соответствии с методами испытаний, установленными в ГОСТ Р 54455 и НД на технические средства и модули конкретного типа.

5.1.6 Технические средства и модули подвергают испытаниям следующих видов:

- приемо-сдаточным;
- периодическим;
- типовым;
- на надежность;
- на функциональную безопасность;
- эксплуатационным;
- квалификационным;
- на подтверждение соответствия.

5.1.7 Погрешность измерения параметров при проведении испытаний не должна превышать 5 %, если иные требования не установлены в методике испытаний.

5.1.8 Объем приемо-сдаточных испытаний и число испытуемых технических средств и модулей устанавливают в НД на технические средства и модули конкретного типа.

5.1.9 Технические средства и модули подвергают периодическим испытаниям в соответствии со сроками проведения, установленными в НД на технические средства и модули конкретного типа. Объем периодических испытаний и число испытуемых извещателей устанавливают в НД на извещатели конкретного типа.

5.1.10 Типовые испытания технических средств и модулей проводят по программе и методике, включающими обязательную проверку параметров, на которые могут повлиять изменения, внесенные в конструкцию, материалы или технологию изготовления технического средства или модуля.

5.1.11 Испытания на надежность технических средств и модулей, прошедших приемо-сдаточные испытания и принятых ОТК, проводит предприятие-изготовитель. Порядок испытаний на надежность в зависимости от вида технических средств и модулей установлен в соответствующих стандартах и НД на технические средства и модули конкретного типа.

5.1.12 Испытания на функциональную безопасность и оценку соответствия технологических извещателей следует проводить в соответствии с ГОСТ Р МЭК 61511-1 и ГОСТ Р МЭК 61511-2.

5.2 Проведение испытаний

5.2.1 Испытания технических средств и модулей

5.2.1.1 Испытания технических средств и модулей на соответствие требованиям 4.3.1 следует проводить с помощью доверенных эмулирующих программ, установленных на персональном компью-

тере, или специальных контрольных технических средств по методам, установленным в НД на технические средства и модули конкретного типа.

5.2.1.2 Испытания технических средств и модулей на устойчивость к внешним воздействующим факторам (см. 4.3.2) следует проводить по ГОСТ Р 54455.

5.2.2 Испытания средств сбора и обработки информации (см. 4.3.3) следует проводить в соответствии с ГОСТ Р 52436 и НД на средства сбора и обработки информации конкретного типа.

5.2.3 Испытания охранных извещателей (см. 4.3.4) в зависимости от типов следует проводить в соответствии с ГОСТ 32321, ГОСТ 34025, ГОСТ Р 50658, ГОСТ Р 50659, ГОСТ Р 50777, ГОСТ Р 52434, ГОСТ Р 52650, ГОСТ Р 52651, ГОСТ Р 52933, ГОСТ Р 53702, ГОСТ Р 54832, ГОСТ Р 55150 и НД на извещатели конкретного типа.

5.2.4 Испытания модулей управления и индикации состояния (см. 4.3.5) следует проводить в соответствии с ГОСТ Р 52436 и НД на модули управления и индикации состояния конкретного типа.

5.2.5 Испытания средств электропитания (см. 4.3.6) следует проводить по ГОСТ Р 53560 и НД на средства обеспечения электропитания конкретного типа.

5.2.6 Испытания охранных оповещателей (см. 4.3.7) следует проводить в соответствии с ГОСТ Р 54126 и НД на оповещатели конкретного типа.

5.2.7 Испытания средств активной защиты (см. 4.3.8) следует проводить в соответствии с [3] и НД на средства активной защиты конкретного типа.

5.2.8 Испытания охранных телевизионных средств (см. 4.3.9) следует проводить по ГОСТ Р 51558.

Алгоритмы компрессии видеоданных оценивают по ГОСТ Р 54830.

Алгоритмы компрессии аудиоданных оценивают по ГОСТ Р 56047.

Уровни защиты видеоданных от случайных и/или преднамеренных искажений рассчитывают по ГОСТ Р 56035.

5.2.9 Испытания средств контроля и управления доступом (см. 4.3.10) следует проводить в соответствии с ГОСТ Р 51241 и НД на средства контроля и управления доступом конкретного типа.

5.2.10 Испытания средств охранного освещения (см. 4.3.11) следует проводить в соответствии с методами, установленными в НД на средства охранного освещения конкретного типа.

5.2.11 Испытания технологических извещателей (см. 4.3.12) следует проводить по методам испытаний, установленным в НД на технологические извещатели конкретного типа.

Библиография

[1] Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности»

[2] IEA RS-485:2003 Рекомендованный стандарт передачи данных по двухпроводному полудуплексному многоточечному последовательному каналу связи. Электрические характеристики генераторов и приемников для использования в балансных многоточечных системах (Recommended Standard 485 Electrical Characteristics of Generator and Receivers for Use in Balanced Multipoint Systems)

[3] МЭК 62642-8:2011 Системы тревожной сигнализации. Системы охранной сигнализации. Часть 8. Системы/технические средства защиты искусственного задымления (Alarm systems — Intrusion and hold-up systems — Part 8: Security fog device/systems)

УДК 621.398:006.354 ОКС 13.320

Ключевые слова: система централизованного наблюдения, объектовая подсистема, средства сбора и обработки информации, охранный оповещатель, средства контроля и управления доступом, охранные телевизионные средства, технологические извещатели, средства активной защиты, средства охранного освещения

Редактор *Н.Е. Рагузина*
Технические редакторы *В.Н. Прусакова, И.Е. Черепкова*
Корректор *Е.Ю. Каболова*
Компьютерная верстка *Л.В. Софейчук*

Сдано в набор 30.09.2019. Подписано в печать 03.10.2019. Формат $60 \times 84^1/_8$. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

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 gost.e-ecolog.ru

gost.e-ecolog.ru