ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72355.1— 2026

Системы киберфизические

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ КОНТРОЛЯ СРЕДСТВ ИНДИВИДУАЛЬНОЙ ЗАЩИТЫ

Часть 1

Общие технические требования

Издание официальное

Москва
Российский институт стандартизации
2026

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество»)

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 20 января 2026 г. № 13-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 (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2026

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системы киберфизические

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ КОНТРОЛЯ СРЕДСТВ ИНДИВИДУАЛЬНОЙ ЗАЩИТЫ

Часть 1

Общие технические требования

Cyber-physical systems. Smart control systems for personal protective equipment.
Part 1. General technical requirements

Дата введения — 2026—06—30

1 Область применения

Настоящий стандарт устанавливает требования:

- к интеллектуальной системе контроля средств индивидуальной защиты общего вида;
- основным компонентам интеллектуальной системы контроля средств индивидуальной защиты;
- объектам распознавания интеллектуальной системы контроля средств индивидуальной защиты.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 59123—2020 Система стандартов безопасности труда. Средства индивидуальной защиты. Общие требования и классификация

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 утверждения (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 **интеллектуальная система контроля средств индивидуальной защиты;** ИСКСИЗ: Система, определяющая и фиксирующая признаки нарушения в ношении средств индивидуальной защиты.

3.2 **средства индивидуальной защиты;** СИЗ: Носимое на человеке средство индивидуального пользования для предотвращения или уменьшения воздействия на человека вредных и/или опасных факторов, а также для защиты от загрязнения.

Издание официальное

3.3 **детекция:** Процесс автоматического обнаружения и распознавания объектов в видеопотоке с использованием алгоритмов компьютерного зрения и нейронных сетей.

4 Сокращения

В настоящем стандарте применены следующие сокращения:
АРМ — автоматизированное рабочее место;
КСПД — корпоративная сеть передачи данных;
ОТ — охрана труда;
ПБ — промышленная безопасность;
ПО — программное обеспечение;
ТБ — техника безопасности;
API — прикладной программный интерфейс (application programming interface);
IP — интернет-протокол (internet protocol).

5 Устройство и работа интеллектуальной системы контроля средств индивидуальной защиты

5.1 Общие требования к интеллектуальной системе контроля средств индивидуальной защиты

ИСКСИЗ должна обеспечивать выполнение следующих функций:
- распознавания надетых СИЗ и правильности их ношения;
- распознавания цвета СИЗ (при необходимости);
- контроля полноты комплекта СИЗ;
- фиксации признаков нарушения ТБ и ПБ и реакции на признаки нарушения;
- интеграции с турникетами, замками, сигнальными устройствами, приборами контроля электростатики;
- мониторинга процесса в режиме реального времени;
- интеграции с базами данных персонала (при необходимости);
- самостоятельной настройки типов видеоаналитики, отчетности и уведомлений (при необходимости);
- возможности прямой интеграции с системами видеонаблюдения;
- возможности настройки для камер статических и динамических зон (в т. ч. активируемых внешними сигналами), в которых будет проконтролировано присутствие человека и/или наличие СИЗ;
- возможности формирования аннотированных описаний зафиксированных признаков нарушения (при необходимости).

В ИСКСИЗ дополнительно может быть доступен пользовательский интерфейс для дообучения моделей распознавания уникальных объектов и событий, а также API для интеграции с внешней системой, выполняющей функции локального ситуационного центра.

5.2 Функциональные элементы интеллектуальной системы контроля средств индивидуальной защиты

5.2.1 Общие положения

В общем случае ИСКСИЗ включает в себя:
- подсистему видеоаналитики;
- подсистему статистики;
- подсистему хранения данных;
- подсистему мониторинга;
- подсистему интерфейса и API.

Схема ИСКСИЗ общего вида представлена на рисунке 1.

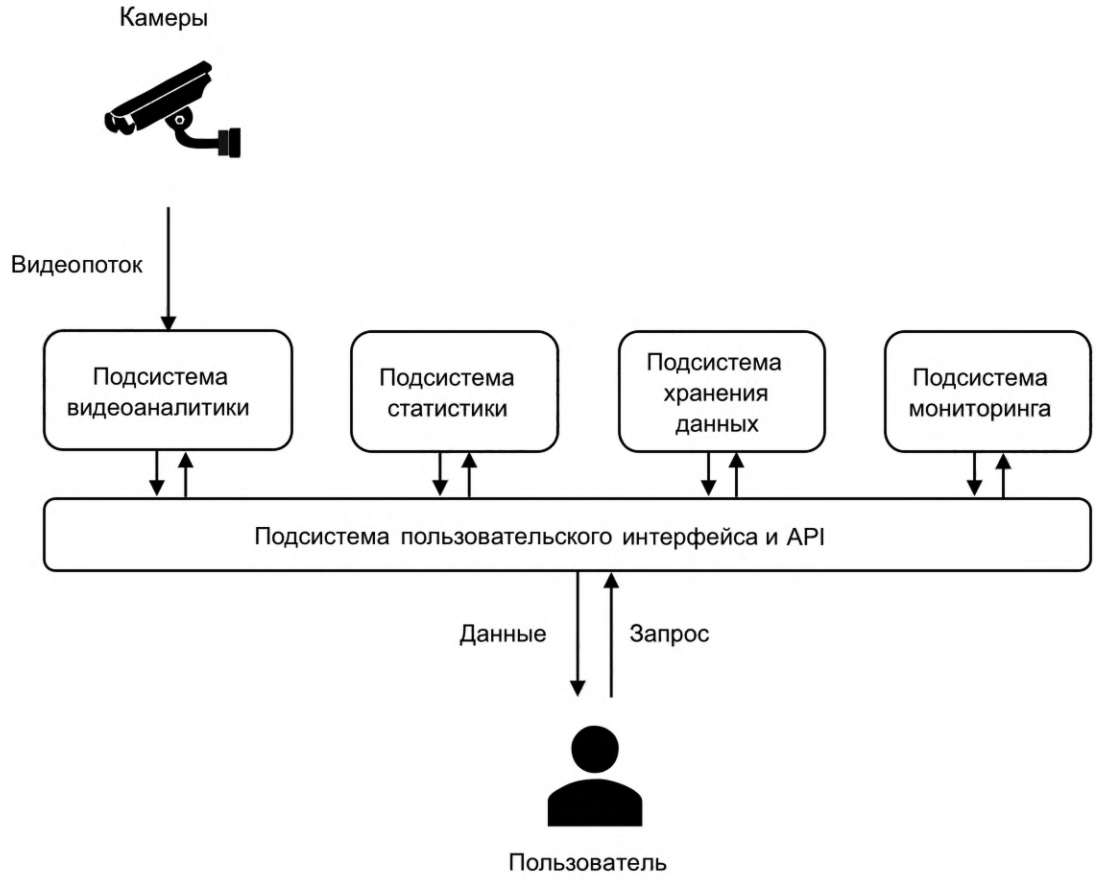

Рисунок 1 — Схема ИСКСИЗ общего вида

Примечание — Настоящий стандарт не устанавливает требования к техническим характеристикам видеопотока и камер, с которых ИСКСИЗ получает данный видеопоток, так как данные характеристики зависят от конкретного предприятия, в котором развернута ИСКСИЗ, и в общем случае их изменение невозможно.

5.2.2 Подсистема видеоаналитики

5.2.2.1 Общие положения

Подсистема видеоаналитики предназначена для сбора видеоданных, детектирования особых случаев (событий, признаков нарушения) и передачи первичных результатов по ним для дальнейшей обработки ИСКСИЗ.

В состав подсистемы видеоаналитики могут входить следующие функциональные элементы:

- модуль мониторинга;
- модуль балансировки нагрузки;
- модуль идентификации признаков нарушения ТБ;
- модуль разработки сценариев обработки видеопотоков;
- база данных.

5.2.2.2 Модуль мониторинга

Модуль мониторинга обеспечивает мониторинг работоспособности компонентов ИСКСИЗ: с заданной периодичностью получает информацию о работе камер (частота кадров, разрешение) и в случае отсутствия сообщений о работе камеры отправляет уведомление на перезапуск камеры.

5.2.2.3 Модуль балансировки

Модуль балансировки нагрузки обеспечивает распределение (балансировку) видеопотоков по физическим серверам и в случае выхода из строя одного из физических серверов перераспределяет ресурсы.

5.2.2.4 Модуль идентификации признаков нарушения техники безопасности

Модуль идентификации признаков нарушения ТБ обеспечивает сбор и анализ видеопотоков с различных камер, детектирование признаков нарушения ТБ и ПБ, формирование видеопотока для просмотра видео.

5.2.2.5 Модуль разработки сценариев обработки видеопотоков

Модуль разработки сценариев обработки видеопотоков обеспечивает возможность пользователю создавать собственные цепочки обработки видеопотока с применением выбранных моделей и логических блоков.

5.2.2.6 Хранилище данных

Хранилище данных обеспечивает хранение ПО для распознавания (например, моделей распознавания, необходимых библиотек и т. п.).

5.2.3 Подсистема статистики

5.2.3.1 Общие положения

Подсистема статистики предназначена для осуществления пользовательской обработки обнаруженных событий (особых случаев), сбора и хранения данных об обнаруженных событиях.

В состав подсистемы статистики могут входить следующие модули:

- описание камер;
- обработка событий;
- хранение событий;
- уведомления;
- хранение счетчиков.

5.2.3.2 Модуль описания камер

Модуль описания камер обеспечивает хранение сведений о камерах (IP, названия, настройки, параметры зон и т. п.) и права доступа для пользователей, принимает от пользователя запрос на добавление новых камер и передает информацию о новых камерах в модуль обработки событий и домен инференса.

5.2.3.3 Модуль обработки событий

Модуль обработки событий обеспечивает обработку и фиксацию признаков нарушения в ИСКСИЗ с применением фильтрации по заданным критериям.

5.2.3.4 Модуль хранения событий

Модуль хранения событий обеспечивает хранение информации по всем детектированным событиям в системе: получает от модулей информацию о событиях и передает ее в домен хранения данных.

Примечание — Модуль хранения событий обеспечивает возможность последующего просмотра, анализа и аннотирования детектированных событий оператором для формирования обратной связи и разрешения спорных ситуаций.

5.2.3.5 Модуль уведомлений

Модуль уведомлений обеспечивает передачу сообщений оператору о фиксации признака нарушения.

5.2.3.6 Модуль хранения счетчиков

Модуль хранения счетчиков обеспечивает хранение информации по числу людей в кадре/зоне (счетчики).

5.2.4 Подсистема хранения данных

Подсистема хранения данных предназначена для хранения статических медиафайлов (фотографий, видеофрагментов).

Подсистема хранения данных обладает структурой, которая базируется на файловой системе сервера.

5.2.5 Подсистема мониторинга

5.2.5.1 Общие положения

Подсистема мониторинга обеспечивает сбор служебной информации о функционировании ИСКСИЗ, сбор и визуализацию статистических данных, лог-сообщений о работе сервисов. Мониторинг осуществляют путем установки агентов мониторинга на серверах размещения ИСКСИЗ.

В состав подсистемы мониторинга могут входить следующие функциональные элементы:

- сервер;
- программное приложение;
- доставщик лог-сообщений;
- модуль поиска, анализа и хранения данных;
- программная панель визуализации данных.

5.2.5.2 Сервер

Сервер принимает запросы от пользователя на отображение данных мониторинга.

5.2.5.3 Программное приложение

Программное приложение используют для мониторинга событий и оповещения о событиях.

5.2.5.4 Доставщик лог-сообщений

Доставщик лог-сообщений осуществляет мониторинг и сбор лог-сообщений из различных лог-файлов и пересылку их в модуль поиска, анализа и хранения данных.

5.2.5.5 Модуль поиска, анализа и хранения данных

Модуль поиска, анализа и хранения данных используют для хранения логов.

5.2.5.6 Программная панель визуализации данных

Программная панель визуализации данных иллюстрирует пользователю данные от модуля поиска, анализа и хранения данных.

5.2.6 Подсистема пользовательского интерфейса и API

5.2.6.1 Общие положения

Подсистема пользовательского интерфейса и API предоставляет человеко-машинный интерфейс для взаимодействия с ИСКСИЗ: администрирования, отображения аналитических отчетов, редактирования конфигурации системы.

В состав подсистемы пользовательского интерфейса и API могут входить следующие функциональные элементы:

- сервер;
- библиотека для программирования пользовательских интерфейсов;
- конвертер;
- сервис аутентификации.

5.2.6.2 Сервер

Сервер принимает запросы от пользователя на отображение или изменение данных, отправляет их в необходимые сервисы и выдает пользователю веб-страницу.

5.2.6.3 Библиотека для программирования пользовательских интерфейсов

Библиотека для программирования пользовательских интерфейсов предоставляет статичные файлы, необходимые для создания интерфейса.

5.2.6.4 Конвертер

Конвертер принимает запрос на предоставление различных данных для отображения их на веб-странице (списки камер, изображения с камер, авторизация и т. п.), отправляет запросы другим сервисам системы и возвращает полученную от других сервисов информацию для отображения на странице веб-интерфейса пользователю.

5.2.6.5 Сервис аутентификации

Сервис аутентификации принимает запрос от пользователя на изменение каких-либо прав доступа.

5.2.7 Подсистема идентификации сотрудников

5.2.7.1 Общие положения

В состав ИСКСИЗ может входить подсистема идентификации сотрудников. Она предназначена для идентификации сотрудников: хранения и изменения заранее заложенной информации (фото сотрудника, личные данные), последующего распознавания сотрудника по фото-видеофрагменту и фиксации события распознавания.

В состав подсистемы идентификации сотрудников могут входить следующие функциональные элементы:

- база данных сотрудников;
- модуль детектирования сотрудников.

5.2.7.2 База данных сотрудников

База данных сотрудников позволяет добавлять, обновлять и удалять данные сотрудников.

5.2.7.3 Модуль детектирования сотрудников

Модуль детектирования сотрудников предназначен для обнаружения и идентификации сотрудников.

Обработка биометрических данных (медиафайлов) для идентификации сотрудников должна проходить в строгом соответствии с законодательством Российской Федерации с обязательным получением согласия субъекта или при наличии иного основания, предусмотренного законом.

5.3 Двухуровневая архитектура интеллектуальной системы контроля средств индивидуальной защиты

В случае необходимости сбора и анализа данных с нескольких территориальных единиц (объектов) предприятия может быть развернута двухуровневая архитектура ИСКСИЗ (см. рисунок 2), в которой детекция и обработка событий происходят на уровне территориальных единиц (объектов) во избежание перегрузки каналов передачи данных видеопотоками с камер, а информация по детектированным и обработанным событиям передается в систему, установленную в центральной диспетчерской. При такой реализации ИСКСИЗ на каждом из предприятий видеопоток с камер передается из выделенной сети видеонаблюдения в расположенный в КСПД предприятия сервер видеоаналитики, на котором выполняют обработку видео. Через КСПД предприятия на АРМ пользователей передается доступ к ИСКСИЗ на предприятии: доступ к видеопотоку с подключенных к системе камер в режиме реального времени, возможность получать от ИСКСИЗ оповещения о детектированных событиях.

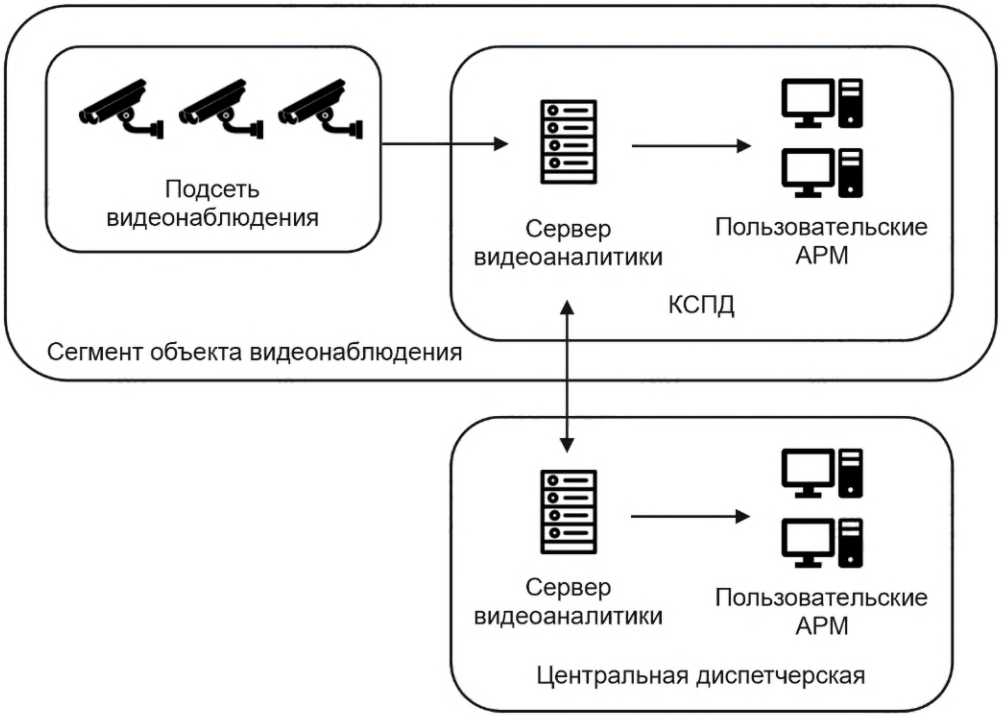

Рисунок 2 — Двухуровневая архитектура ИСКСИЗ

Данные по событиям, детектированным ИСКСИЗ, передаются из локальных серверов видеоаналитики каждого из объектов на сервер видеоаналитики, установленный в центральной диспетчерской предприятия. В центральной диспетчерской пользователь (например, оператор или администратор) может просматривать информацию по детектированным и обработанным признакам нарушения, формировать и выгружать из системы отчеты по признакам нарушения ПБ и ОТ. Для корректной работы ИСКСИЗ вместе с событиями должна быть также передана информация о структуре объекта, включая информацию о предприятии, его подразделениях, камерах и сотрудниках.

6 Объекты распознавания интеллектуальной системы контроля средств индивидуальной защиты

ИСКСИЗ должна осуществлять распознавание СИЗ одного и более назначений в соответствии с классификацией по назначению, установленной ГОСТ Р 59123—2020 (пункт 5.1).

Приложение А
(справочное)

Примеры реализации интеллектуальной системы контроля средств индивидуальной защиты

Примеры реализации ИСКСИЗ представлены на рисунках А.1 и А.2.

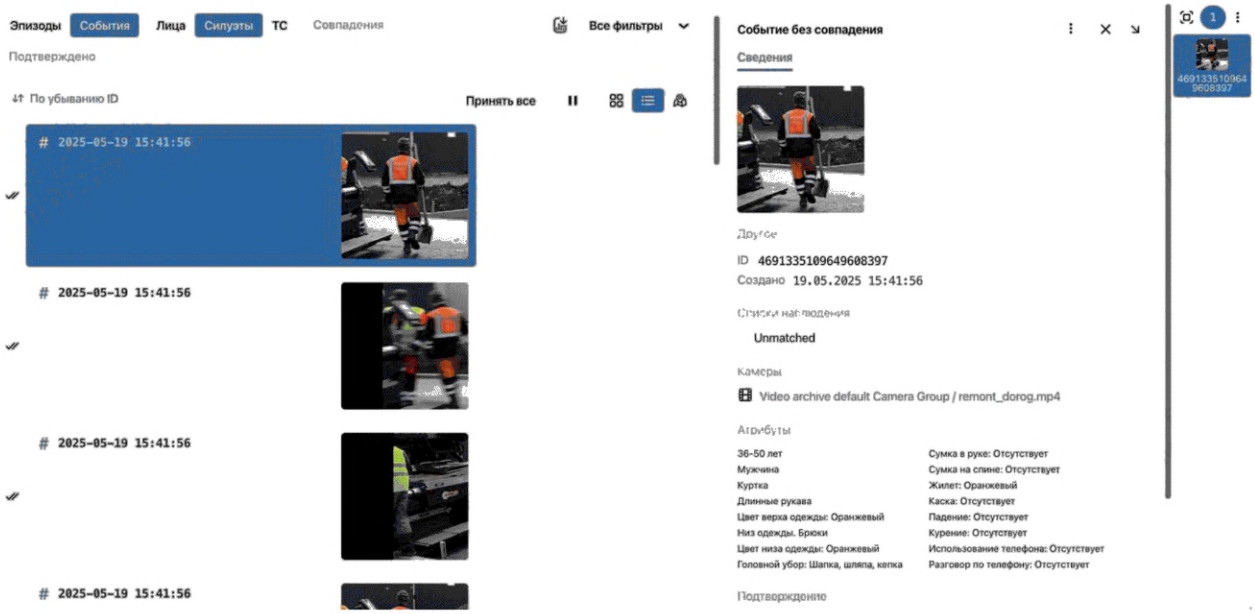

Рисунок А.1 — Пример реализации ИСКСИЗ 1

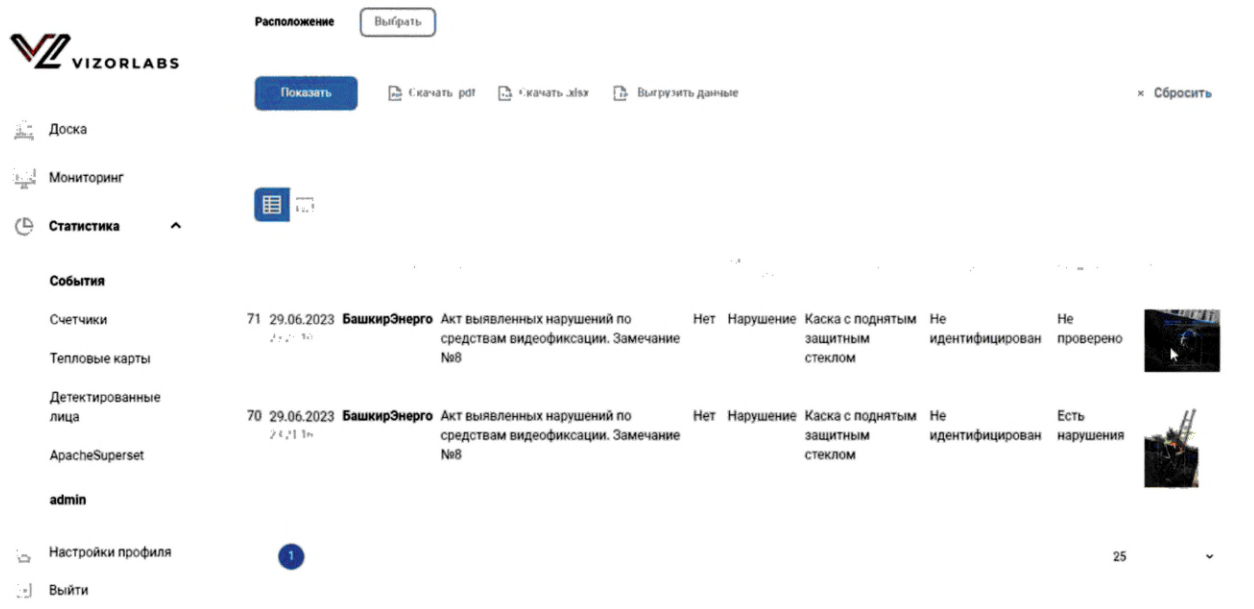

Рисунок А.2 — Пример реализации ИСКСИЗ 2

УДК 004.93'1:006.354 ОКС 35.240.99

Ключевые слова: системы киберфизические, интеллектуальная система, контроль, средства индивидуальной защиты, общие технические требования

Редактор *М.В. Митрофанова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 22.01.2026. Подписано в печать 16.02.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,18.

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.
gost.e-ecolog.ru gost.e-ecolog.ru