ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71895.1— 2025

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

Интеллектуальная система предотвращения несанкционированного копирования информации с рабочих мест операторов автоматизированных информационных систем

Часть 1

Общие требования

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

1 РАЗРАБОТАН Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») и Акционерным обществом «ЭЛВИС-НеоТек»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Киберфизические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 июня 2025 г. № 596-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.rst.gov.ru)

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

Интеллектуальная система предотвращения несанкционированного копирования информации с рабочих мест операторов автоматизированных информационных систем

Часть 1

Общие требования

Cyberphysical systems.
An intelligent system to prevent unauthorized copying of information from the workplaces of operators of automated information systems.
Part 1. General requirements

Дата введения — 2025—08—01

1 Область применения

Настоящий стандарт устанавливает требования:

- к интеллектуальной системе предотвращения несанкционированного копирования информации (ИСПНКИ) с рабочих мест операторов автоматизированных информационных систем общего вида;
- основным компонентам ИСПНКИ;
- размещению и установке ИСПНКИ;
- типовым примерам применения ИСПНКИ.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 12.2.007.01 Система стандартов безопасности труда. Машины электрические вращающиеся. Требования безопасности

ГОСТ 14254 Степени защиты, обеспечиваемые оболочками (Код IP)

ГОСТ 15150 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

ГОСТ Р 50267.0 (МЭК 601-1—88) Изделия медицинские электрические. Часть 1. Общие требования безопасности

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

Издание официальное

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 предотвращения несанкционированного копирования информации с рабочих мест операторов автоматизированных информационных систем;** ИСПНКИ: Система, фиксирующая попытки несанкционированного копирования информации с рабочих мест операторов автоматизированных информационных систем и осуществляющая оперативные действия по пресечению этих попыток.

3.2 **несанкционированное копирование информации:** Копирование защищаемой информации с нарушением установленных прав и (или) правил доступа путем съемки визуальной информации средствами фото/видеофиксации.

3.3 **предотвращение утечки данных:** Предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание — Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

АИС — автоматизированная информационная система, копирование данных из которой предотвращается ИСПНКИ;

АРМ — автоматизированное рабочее место;

НСД — несанкционированный съем данных;

ПУД — предотвращение утечки данных;

СБ — служба безопасности;

СНК — средства несанкционированного копирования;

ТСО — технические средства охраны;

LAN — локальная сеть.

5 Устройство и работа ИСПНКИ

5.1 Общие требования к ИСПНКИ

В общем случае система предотвращения несанкционированного копирования информации включает в свой состав следующие модули:

- контроллер управления рабочим местом оператора АИС;
- широкоформатный сканер средств фото/видеосъемки;
- программное обеспечение ситуационного центра.

На рабочем месте оператора АИС устанавливаются сканеры средств фото/видеосъемки и контроллер управления рабочим местом оператора. Данные с видеокамер(ы) обрабатываются в системе, и в случае обнаружения атаки включаются меры противодействия (если рабочее место ими оснащено). Данные инцидента передаются на АРМ сотрудника безопасности.

На рисунке 1 показана схема работы ИСПНКИ.

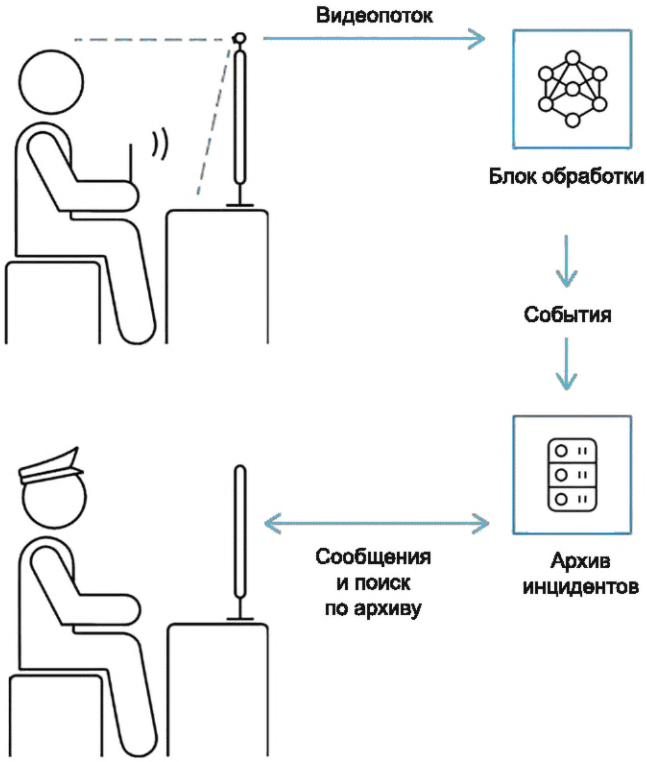

Рисунок 1 — Схема работы ИСПНКИ

Функционально все элементы системы разделены на следующие категории:

- сервер;
- АРМ оператора СБ;
- подсистема обнаружения СНК;
- подсистема подавления СНК;
- подсистема управления.

Система должна удовлетворять следующим техническим требованиям:

1) наличие одновременного контроля одним ответственным сотрудником большого количества рабочих мест сотрудников;

2) возможность просмотра списка всех зафиксированных событий;

3) возможность просмотра видеозаписи, на которой зафиксирован факт нарушения;

4) возможность экспорта фрагмента видеозаписи или стоп-кадров;

5) возможность детектирования любых моделей мобильных устройств разных производителей;

6) формирование информационного сообщения ответственному сотруднику о срабатывании системы;

7) возможность автоматической идентификации неисправности или некорректного изображения (например, закрытия/загораживания камеры сторонним предметом) с установленных видеокамер;

8) видеокамеры, установленные на рабочем месте сотрудника, должны обеспечивать качество записи, позволяющее однозначно идентифицировать действия сотрудника;

9) возможность хранения видеозаписей по журналу событий в течение определенного периода времени;

10) возможность масштабирования системы;

11) видеокамера не должна выдавать свою активность;

12) формирование и экспорт данных по зафиксированным событиям, видеозаписям с указанием даты, времени, продолжительности, рабочего места оператора АИС и т. д.;

13) возможность разграничения прав доступа в системе к информации/воспроизведению информации, отчетности.

ИСПНКИ должна соответствовать:

- по типу защиты от поражения электрическим током — изделию класса I, питаемому от внешнего источника электрической энергии по ГОСТ Р 50267.0;
- способу защиты человека от поражения электрическим током — классу 0I по ГОСТ 12.2.007.01;
- степени защиты от проникновения воды для корпуса прибора — классу IPX1 по ГОСТ 14254;
- категории исполнения — категории 4 по ГОСТ 15150.

5.2 Компоненты системы

5.2.1 Центральный сервер

Центральный сервер АРМ выполняет следующие функции:

- фиксация места нарушения (расположение на плане помещения);
- фиксация даты и времени нарушения с привязкой к видеозаписи;
- фиксация обстоятельств нарушения посредством видеозаписи с видеокамер, расположенных на рабочих местах сотрудников, а также при необходимости с обзорных видеокамер, расположенных в помещениях с рабочими местами сотрудников;
- фиксация записей видеокамеры, контролирующей сотрудника, а также обзорных видеокамер, смотрящих на рабочее место сотрудника;
- информирование о факте несанкционированного съема информации на АРМ операторов СБ.

В общем случае центральный сервер ИСПНКИ с рабочих мест операторов АИС содержит: блок подключения внешних датчиков, совместно реализующих функцию мультиспектральной съемки в различных диапазонах электромагнитных волн; блок обработки данных с внешних датчиков, состоящий из одного или более высокопроизводительных графических процессорных устройств для обработки мультиспектральных данных с внешних датчиков; блок подключения внешних устройств, реализующих функцию подавления канала утечки данных за счет отключения устройства для вывода визуальной информации или формирования помех (засветок) в одном из диапазонов электромагнитного излучения с целью нарушить условия фото/видеосъемки; блок подключения АРМ оператора СБ и АРМ начальника смены СБ; предустановленное прикладное ПО, в состав которого входят следующие модули: модуль обнаружения СНК, модуль захвата и предварительной обработки данных с мультиспектральных датчиков, модуль фиксации места, даты и времени нарушения, модуль фиксации обстоятельств нарушения с привязкой к видеозаписи с камер, установленных на рабочих местах сотрудников, модуль настройки пользовательских параметров и сценариев, модуль управления входящими в устройство и внешними подключаемыми модулями, модуль формирования тревожного сигнала, предупреждающего об обнаружении факта несанкционированного съема информации на АРМ оператора СБ; модуль управления, обеспечивающий функционирование ИСПНКИ в части взаимодействия с рабочим местом оператора АИС, модуль идентификации рабочего места оператора АИС, модуль обеспечения передачи видеопотока с рабочего места на сервер, модуль передачи сообщений о фиксации фактов НСД, модуль выполнения команды оператора СБ на блокировку доступа к АРМ оператора АИС, модуль управления устройством подавления СНК, модуль предоставления доступа к данным с датчиков в режиме реального времени, модуль предоставления доступа к архивным данным; блок управления и хранения данных, включающий центральный процессор, оперативное и постоянное запоминающее устройства; сетевой контроллер.

5.2.2 АРМ оператора СБ

АРМ оператора СБ выполняет следующие функции:

- предоставляет доступ к видеопотоку реального времени с видеокамер, расположенных на рабочих местах сотрудников, посредством древовидного списка и планов помещений;
- уведомляет оператора в реальном времени о фактах фиксации НСД с возможностью принятия оператором решения о блокировке соответствующего АРМ оператора АИС;
- предоставляет доступ к архивным данным для организации разбора фактов НСД.

5.2.3 Подсистема обнаружения СНК

Подсистема обнаружения СНК служит для фиксации фактов НСД. Для повышения вероятности обнаружения НСД, а также снижения числа ложных срабатываний; в подсистеме может быть заложено несколько методик обнаружения, основанных на различных физических принципах. Подсистема обнаружения строится на базе нейросетевых алгоритмов и должна иметь возможность дообучения алгоритмов по определению мобильных устройств для повышения качества распознания угроз.

В зависимости от конечной цели применения различные аспекты и факторы должны быть приняты во внимание для того, чтобы выбрать наиболее адекватный метод обнаружения СНК:

- точность выравнивания и разрешения облака точек. Определяются аппаратными средствами (датчиком) и программным обеспечением (выполняющим обработку изображения);
- диапазон датчика. Рабочее расстояние определяется радиусом действия и размером датчика;
- вес датчика. Если датчик установлен на манипуляторе, то его вес не должен превышать максимальной нагрузки, чтобы обеспечить его полную динамику;
- вопросы безопасности. Система может работать во взаимодействии с человеком, поэтому датчики не должны содержать лазеров высокой мощности;
- время обработки. Время обработки может иметь решающее значение для определения, подходит ли система для определенного применения;
- влияние окружающей среды. Условия освещения, вибрации, движения камеры и так далее могут вызвать помехи и снизить качество изображения;
- аппаратные средства и программное обеспечение интеграции с другими системами.

Блок сканера средств фото/видеосъемки позволяет осуществлять контроль действий оператора АИС. Блок сканера средств фото/видеосъемки состоит из модуля видеорегистрации и модуля подсветки.

Основным является модуль видеорегистрации, предназначенный для регистрации и записи видеопоследовательности, отображающей действия оператора АИС. Блок видеорегистрации выполняется по монокулярной или бинокулярной схеме. Алгоритмический модуль работает с видеопотоком со стационарной видеокамеры, закрепленной на кромке монитора. Базовый вариант: камера, закрепленная посередине сверху. При камере, закрепленной сбоку или снизу, показатели качества могут несколько отличаться. В поле зрения камеры должны попадать точки, из которых возможна съемка экрана. Если охватить их все одной камерой невозможно, устанавливается несколько камер на один монитор или камера с высоким разрешением, на разных участках изображения с которой запускается несколько экземпляров алгоритма. Изображение должно быть хорошего качества: резкое, стабильное (без сбоев и сильной тряски).

Модуль подсветки предназначен для создания минимально необходимого уровня освещения независимо от наличия внешних источников света и формирования точечных бликов за счет отражений от оптики устройств фото/видеофиксации. Для блока подсветки рекомендуется использовать излучение ближнего ИК диапазона, поскольку оно обладает следующими преимуществами:

- излучение не видимо для человека, не отвлекает внимание пользователя и не вызывает расширение зрачка;
- излучение данного диапазона не вызывает деградации и разрушения рецепторного аппарата глаза человека;
- регистрируется теми же инструментами, что и видимое излучение;
- применение ИК излучения позволяет отделить полезную информацию от внешних засветок, приходящихся на видимую часть спектра.

Чтобы сфотографировать экран рабочего места, сотрудник обычно располагается относительно монитора определенным образом: находится перед монитором рабочего места, держит в руках мобильный телефон и направляет объектив его видеокамеры в сторону монитора. Ракурс съемки при классическом расположении WEB-камер на мониторе позволяет определить момент появления телефона в руках сотрудника и факт съемки. Одновременно с этим видеокамера, направленная на сотрудника, может снизить количество противоправных действий из-за опасения быть пойманным в момент правонарушения.

5.2.4 Подсистема подавления СНК

Подсистема подавления СНК служит для предотвращения фактов НСД. В общем случае в подсистеме может быть заложено несколько методик подавления, основанных на различных физических принципах.

В качестве устройств подавления СНК могут применяться программно-аппаратные средства: автоматического отключения экрана рабочего места оператора АИС; блокировки вывода информации на экран монитора рабочего места оператора АИС; формирования засветки светочувствительного элемента СНК некогерентным широкоугольным излучением ближнего ИК-спектра; формирования засветки светочувствительного элемента СНК узконаправленным когерентным излучением ближнего ИК-спектра; формирования помех в радиочастотном диапазоне.

5.2.5 Подсистема управления

Подсистема управления служит для обеспечения бизнес-логики функционирования ИСПНКИ в части взаимодействия с рабочим местом оператора АИС и выполняет следующие функции:

- идентификацию рабочего места оператора АИС;
- (опционально) идентификацию сотрудника по лицу с возможностью проверки соответствия АРМ АИС распознанному работнику предприятия;
- обеспечение передачи видеопотока с рабочего места на сервер;
- передачу сообщений о фиксации фактов НСД;
- выполнение команды оператора СБ на блокировку доступа к АРМ оператора АИС;
- управление подсистемой подавления СНК.

6 Варианты реализации ИСПНКИ

Существует три базовые реализации ИСПНКИ для конечных пользователей, различающиеся необходимостью или отсутствием необходимости использовать внешний сервер. При этом для всех базовых вариантов предусмотрено опциональное подключение дополнительных элементов.

6.1 Вариант реализации ИСПНКИ № 1

На рисунке 2 показан первый вариант реализации ИСПНКИ, использующей в качестве вычислителя внешний центральный сервер.

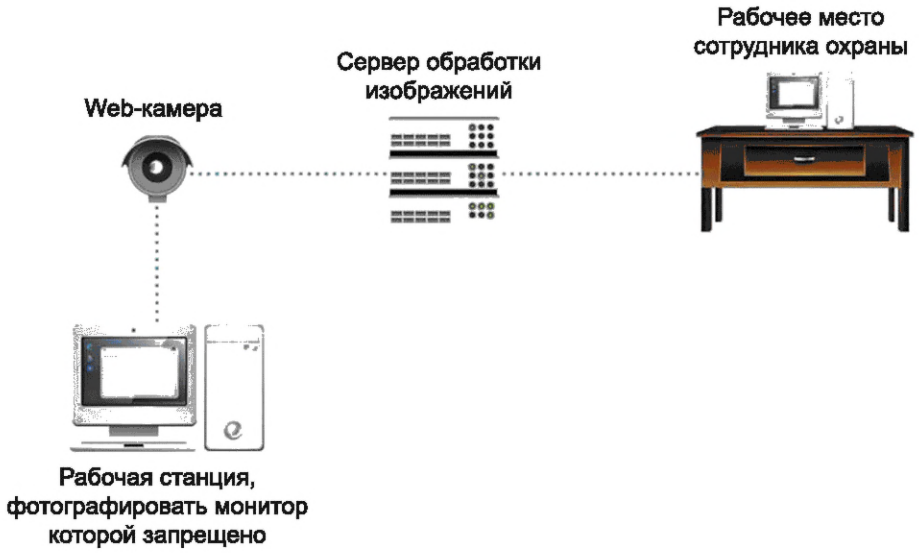

Рисунок 2 — Вариант реализации ИСПНКИ № 1

На рисунке 3 показана структурная схема рассматриваемой реализации.

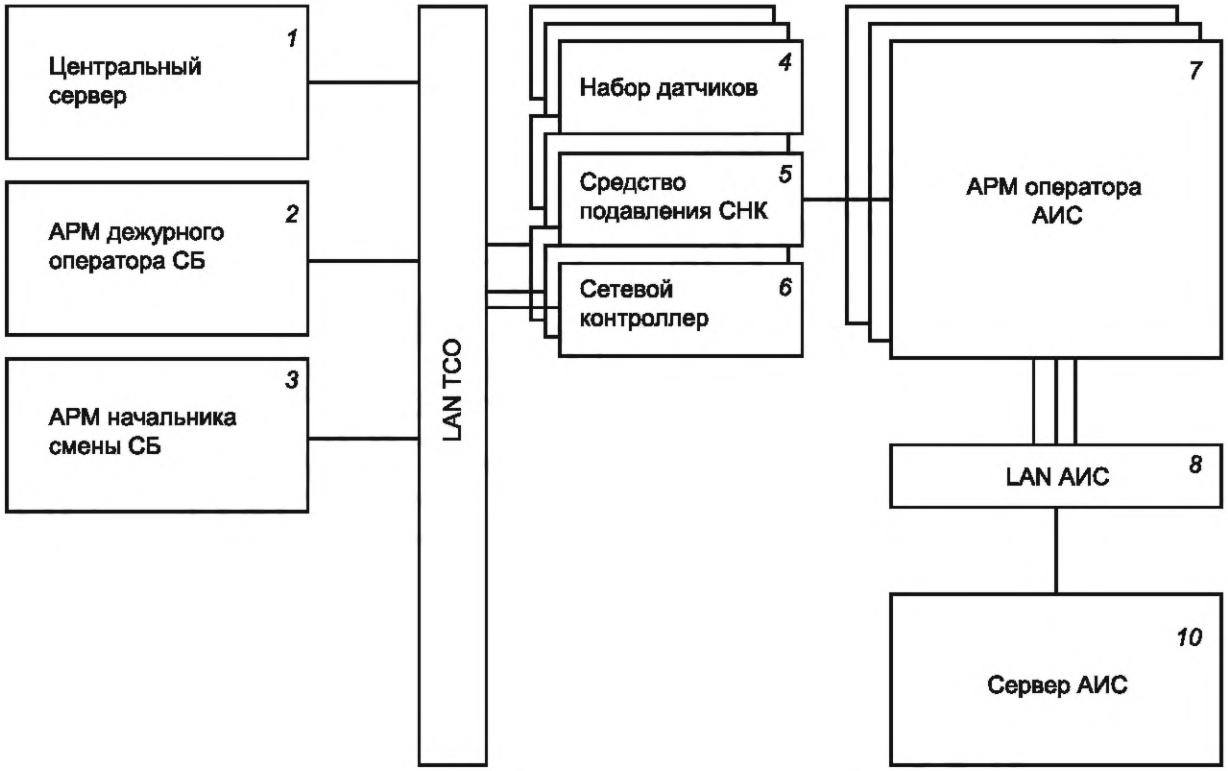

Рисунок 3 — Структурная схема реализации 1

Система включает в себя специализированный сервер *1* с установленным ПО, содержащий необходимое количество графических адаптеров для обеспечения работы блока обнаружения СНК.

Блок обнаружения СНК *4* представляет собой набор программных модулей, устанавливаемых на сервере устройства и реализующих функцию захвата и последующей обработки данных с мультиспектральных датчиков в режиме реального времени с целью обнаружения признаков наличия СНК.

Подключаемый к устройству блок подавления СНК *5*, подключенный к устройству через локальную сеть, позволяет выполнять отключение питания устройства вывода визуальной информации по команде с сервера.

К устройству подключается АРМ дежурного оператора СБ *2*, а также АРМ начальника смены СБ *3*.

Блок управления *6* выполняет следующие функции:

- идентификация рабочего места оператора АИС *7*, подключенного к локальной вычислительной сети автоматизированной информационной системы предприятия (*8*);
- обеспечение передачи видеопотока с рабочего места на сервер;
- передача сообщений о фиксации фактов НСД;
- выполнение команды оператора СБ на блокировку доступа к АРМ оператора АИС;
- управление подсистемой подавления СНК.

В рассматриваемом варианте реализации сервер ИСПНКИ *1* устройства получает через локальную сеть ТСО *9* видеопоток с цифровых стереокамер наблюдения, транслирующих изображения оператора АИС. Видеопоток разбивается на кадры, каждому из которых присваивается метка времени. После этого блок обнаружения СНК *4* обрабатывает каждый кадр, выполняя поиск устройств фото/видеофиксации, и в случае обнаружения блок управления *6* формирует управляющий сигнал, который также через локальную сеть *9* передается на блок подавления СНК *5*, АРМ дежурного оператора СБ *2*, АРМ начальника смены СБ *3*. После этого блок подавления *5* отключает питание монитора, на АРМ дежурного оператора СБ *2* и АРМ начальника смены СБ *3* формируется сообщение о попытке несанкционированного съема данных, а сервер ИСПНКИ *1* формирует коллаж, содержащий кадры, на которых зафиксировано нарушение, идентификатор рабочего места, на котором произошло нарушение, а также время нарушения, и передает коллаж в электронный архив инцидентов.

6.2 Вариант реализации ИСПНКИ № 2

Во втором варианте реализации, так же как и в первом, в качестве вычислителя используется внешний центральный сервер. На рабочем месте оператора АИС устанавливаются сканеры средств фото/видеосъемки и контроллер управления рабочим местом оператора. Данные с видеокамер(ы) попадают непосредственно в одноплатный компьютер, который создает шифрованный канал с сервером обработки изображений и транслирует видеоданные в него для последующей обработки. Сервер обнаруживает атаку, включает меры противодействия (если рабочее место ими оснащено) и передает инцидент по общей, выделенной проводной или беспроводной (Wi-Fi) сети на АРМ сотрудника безопасности.

Второй вариант реализации ИСПНКИ показан на рисунке 4.

Рисунок 4 — Вариант реализации ИСПНКИ № 2

6.3 Вариант реализации ИСПНКИ № 3

В третьем варианте реализации, в отличие от первого и второго варианта реализации, внешний вычислитель отсутствует. На рабочем месте оператора АИС устанавливаются сканеры средств фото/видеосъемки и контроллер управления рабочим местом оператора. Данные с видеокамер(ы) попадают непосредственно в одноплатный компьютер, который с помощью встроенного ПО обнаруживает атаку, включает меры противодействия (если рабочее место ими оснащено) и передает инцидент на АРМ сотрудника безопасности по общей, выделенной проводной или беспроводной (Wi-Fi) сети.

Третий вариант реализации показан на рисунке 5.

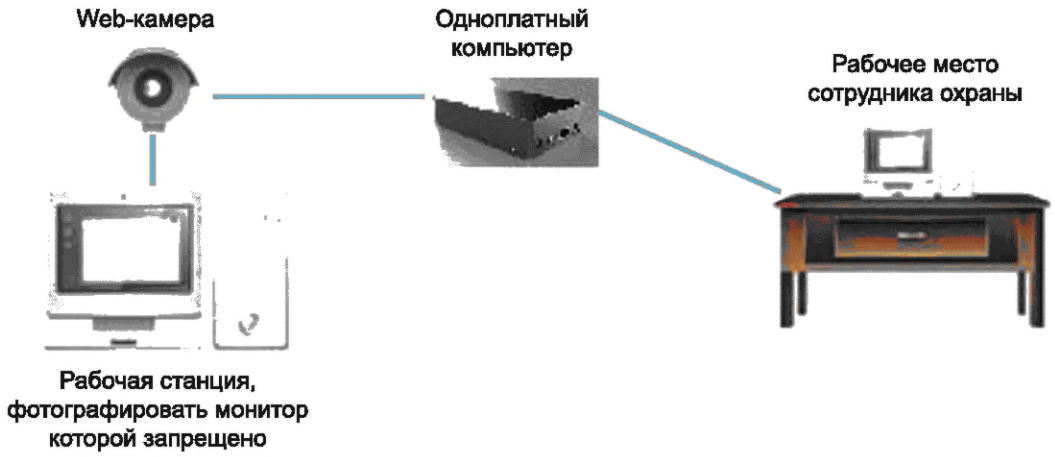

Рисунок 5 — Третий вариант реализации 3 ИСПНКИ

6.4 Краткие выводы

Все три реализации имеют возможность интеграции с существующими системами видеонаблюдения и охранного телевидения, развернутыми в помещениях контролируемого объекта, возможность масштабирования за счет подключения дополнительных графических процессорных устройств сервера для подключения дополнительных контролируемых рабочих мест оператора АИС; интеграции с системой контроля доступа; возможность подключения в качестве дополнительного устройства к рабочему месту оператора СБ; позволяют осуществлять разграничение прав доступа в системе к информации/воспроизведению информации, отчетности.

Приложение А
(справочное)

Пример внешнего вида реализации системы

А.1 Внешний вид реализации рабочего места оператора АИС

Для регистрации и записи видеопоследовательности, отображающей действия оператора АИС, на корпусе монитора оператора АИС при помощи крепежа размещаются видеокамеры (рисунок А.1).

Примечание — Использование двух камер для регистрации изображения одной и той же области позволяет снизить требуемую частоту кадров камеры в два раза, что уменьшает стоимость отдельной камеры. Для этого матрицы работают в режиме попеременной регистрации, что обеспечивается выбором соответствующего режима синхронизации. Еще одним преимуществом такого решения является увеличение надежности блока видеорегистрации за счет возможности сохранения работоспособности изделия при выходе из строя одного из регистрирующих каналов. В этом случае контроль действий оператора будет осуществляться по данным с одной из видеокамер. В таком режиме изделие будет оставаться работоспособным при потере качества по ряду показателей.

Рисунок А.1 — Пример 1 внешнего вида реализации рабочего места оператора АИС

А.2 Внешний вид реализации рабочего места сотрудника СБ

Внешний вид реализации рабочего места сотрудника СБ показан на рисунке А.2.

Рисунок А.2 — Внешний вид реализации рабочего места сотрудника СБ

А.3 Информационно-функциональная панель интерфейса

При возникновении инцидента система оповещает сотрудника службы охраны и передает ему изображение с камеры, на которой было обнаружено мобильное устройство, с указанием названия и расположения видеокамеры, чтобы быстро определить место нарушения, дату и время фиксации нарушения, список всех зафиксированных событий. Интуитивно понятный интерфейс позволяет быстро найти и посмотреть видеозапись нарушения, легко переходить к просмотру других обзорных камер, расположенных в помещении, в котором было зафиксировано нарушение, оперативно экспортировать фрагмент видеозаписи или стоп-кадр для предъявления доказательств нарушителю.

Клиентское приложение включает следующие элементы интерфейса: основное меню, информационно-функциональную панель.

Информационно-функциональная панель приложения содержит имя пользователя, и текущее время в формате «чч:мм». При наведении на область отображения времени появляется окно с текущим временем в формате «чч:мм:сс», датой и днем недели.

Пример информационно-функциональной панели интерфейса показан на рисунке А.3.

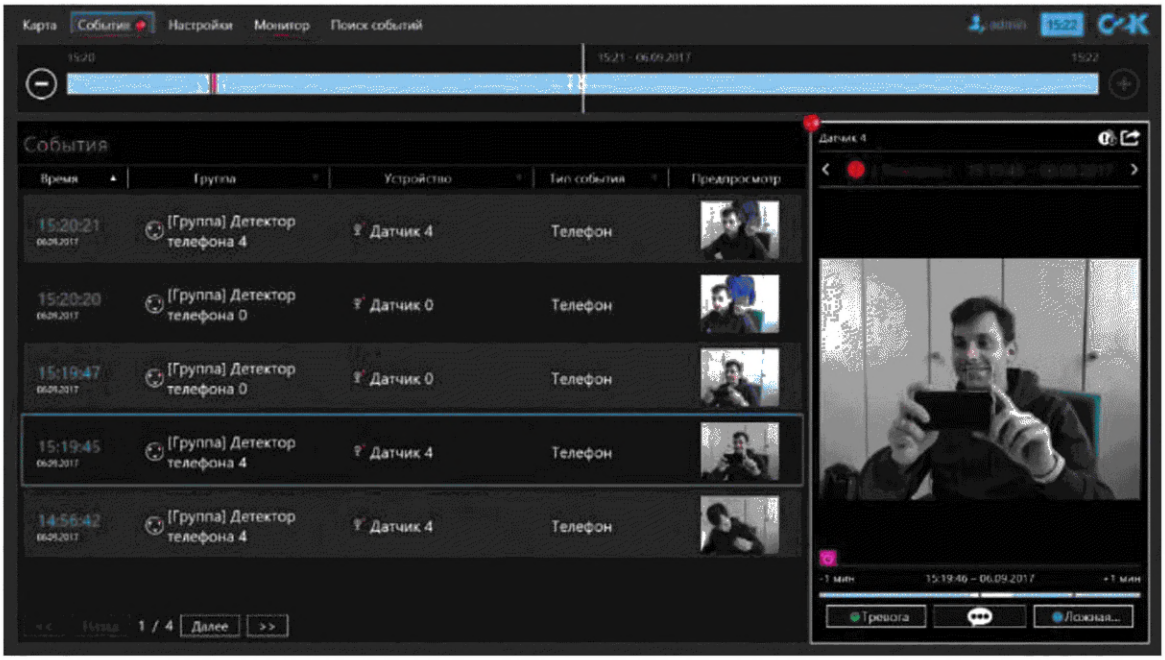

Рисунок А.3 — Информационно-функциональная панель интерфейса

А.4 Основное меню интерфейса

Список групп и устройств предназначен для отображения групп с добавленными устройствами, а также для информирования о типах устройств и их состояниях. Над списком групп и устройств расположено поле для поиска устройства или группы в списке. Для групп и устройств в списке отображаются иконки с их состояниями. Помимо групп, созданных администратором, список содержит группу «Избранное». Устройства в данную группу добавляются оператором либо администратором системы. В группе «Несгруппированные» содержатся устройства, которые не были добавлены администратором ни в одну из созданных групп.

Также при помощи списка групп и устройств выполняются следующие действия: открытие окна свойств с информацией об устройстве/группе и функциями управления; открытие группы или устройства в отдельной вкладке; добавление окон просмотра для видеокамеры/группы устройств в раскладку; добавление устройства без видеоизображения.

Внешний вид основного меню интерфейса показан на рисунке А.4.

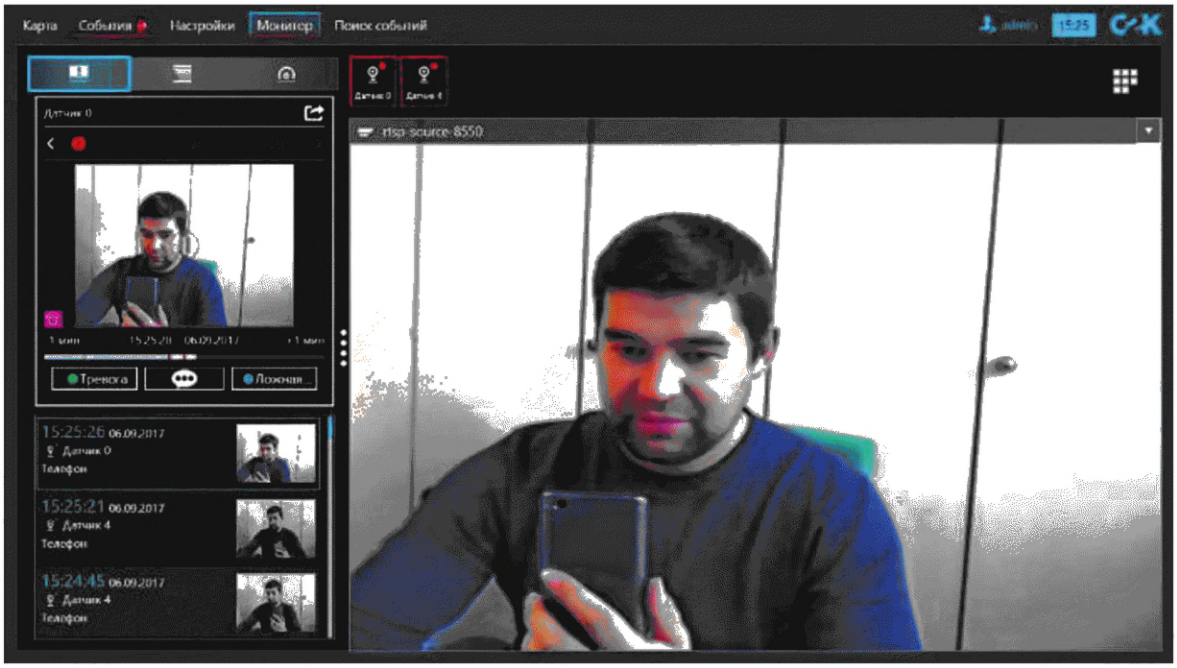

Рисунок А.4 — Основное меню интерфейса

А.5 Дополнительные элементы интерфейса

Помимо основных элементов интерфейса есть дополнительные, которые отображаются в результате определенных действий или событий. К таким элементам относятся, например, окно свойств, окно просмотра и обработки тревожного события, а также изменения интерфейса при регистрации тревожных событий.

Пример дополнительных элементов интерфейса показан на рисунке А.5.

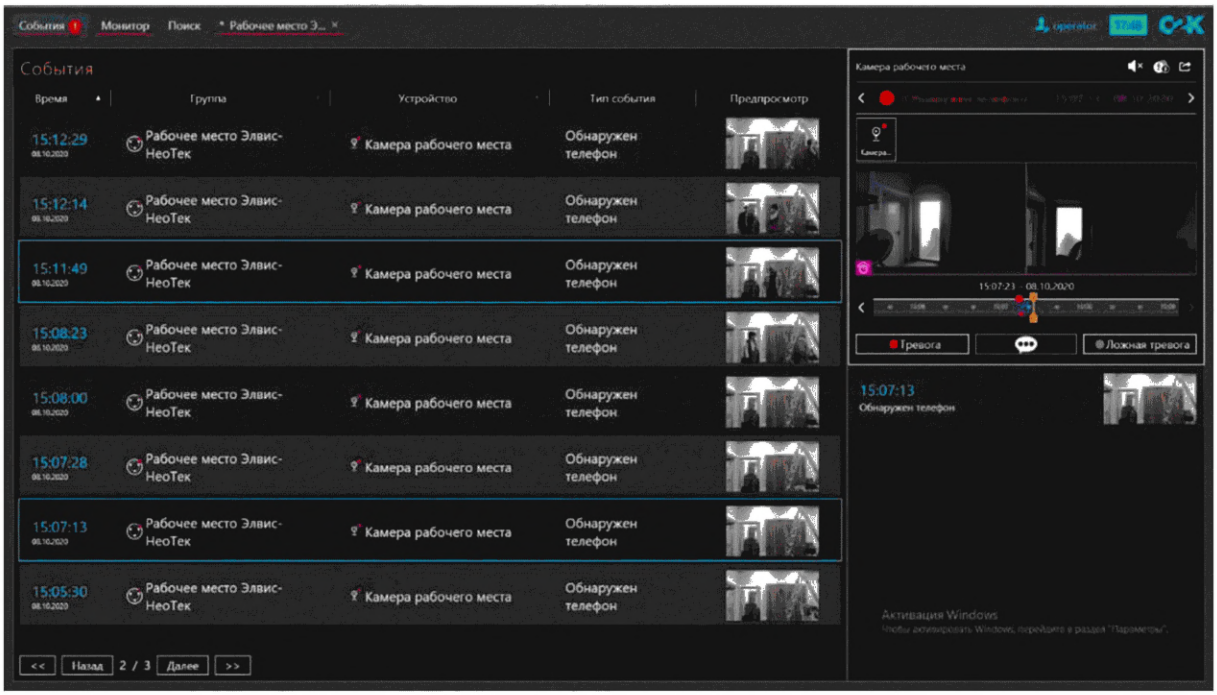

Рисунок А.5 — Дополнительные элементы интерфейса

А.6 Работа с событиями

Пункт меню «События» предназначен для просмотра списка необработанных инцидентов и относящихся к ним тревожных событий (рисунок А.6).

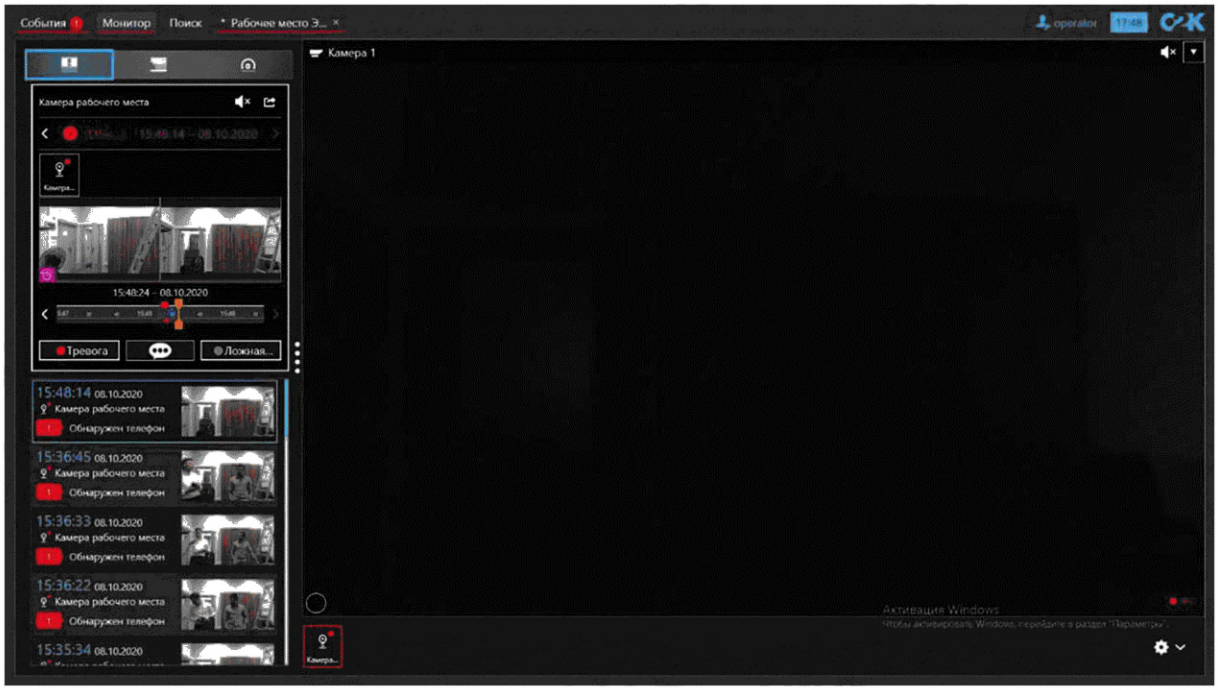

Рисунок А.6 — Работа с событиями

Инциденты в списке можно отфильтровать по следующим параметрам: «Время», «Группа», «Устройство» и «Тип события» (рисунок А.7).

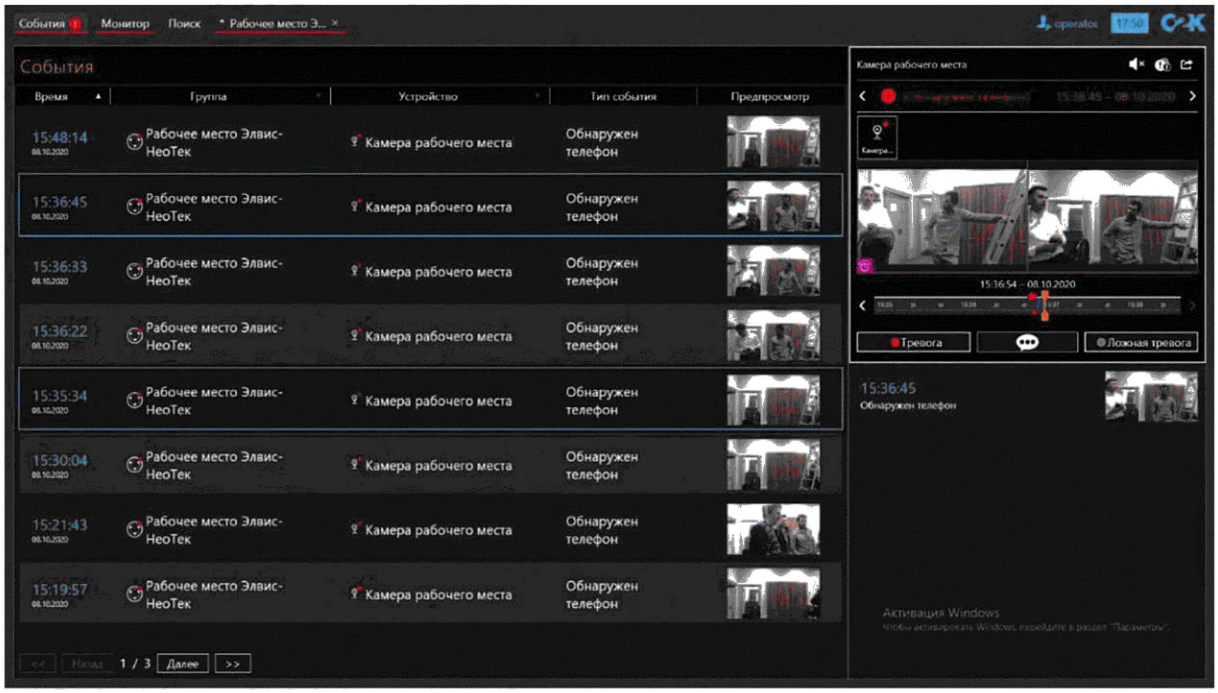

Рисунок А.7 — Работа с инцидентами

Тревожные события, зарегистрированные в одной зоне регистрации тревожных событий, группируются в инциденты. Оператор обрабатывает сразу все события, входящие в инцидент.

При группировке тревожных событий в инциденты соблюдаются следующие правила: в течение определенного времени от начала инцидента все события, возникающие в зоне регистрации, группируются в этот инцидент. По истечении данного промежутка времени события группируются в следующий инцидент; по истечении времени максимальной продолжительности инцидента он закрывается и новые тревожные события группируются в следующий инцидент; если объект, вызвавший тревожное событие, по истечении времени максимальной продолжительности инцидента продолжает существовать, то формируется новый инцидент, в который попадает данный объект; оператору будет доступна обработка инцидента по истечении установленного промежутка времени после начала инцидента; в случае если оператор не обработал инцидент в течение заданного времени, то инцидент будет обработан автоматически.

Для группировки событий используются временные параметры, которые настраиваются администратором системы.

Возникновение нового инцидента в системе сопровождается: звуковым оповещением; появлением красной линии под названием некоторых вкладок; появлением красной точки рядом с устройством в списке устройств; появлением красной рамки вокруг окна просмотра видеоизображения; появлением окна просмотра и обработки тревожного события.

Оператору доступны следующие действия: просмотр инцидента и входящих в него тревожных событий; обработка инцидентов; вызов пользовательской тревоги; добавление комментария к инциденту; экспорт видеоархива.

В окне просмотра и обработки тревожного события воспроизводится видеоархив с тревожным событием и содержится следующая информация:

- название устройства;
- тип тревожного события;
- дата и время возникновения тревожного события;
- дата и время начала инцидента.

В окне просмотра и обработки тревожных событий осуществляется обработка сразу всех событий, которые относятся к выбранному инциденту. Для обработки инцидента необходимо:

- определить тип тревоги: тревога или ложная тревога;
- добавить комментарий к инциденту: нажать тревожную кнопку и в появившемся поле ввести текст комментария. Комментарий появится у каждого события, относящегося к инциденту;
- подтвердить тип тревоги путем нажатия кнопки «Тревога» или «Ложная тревога».

Видеоархив предназначен для поиска и просмотра видеофайлов с событиями, уточнения деталей и дополнительных сведений о событиях, произошедших на подконтрольной территории. Работа с видеоархивом включает в себя следующие действия: поиск видеозаписей и кадров; просмотр видеозаписи на разной скорости, в том числе по кадрам; экспорт выбранной видеозаписи, кадра или его части.

Приложение Б
(справочное)

Типовые примеры применения ИСПНКИ

Сферы применения ИСПНКИ с рабочих мест операторов АИС:

- защита персональных данных, финансовых сведений, сведений о счетах и движении денежных средств от несанкционированного копирования и передачи третьим лицам в банковской финансовой сфере;
- защита информации о состоянии здоровья пациента, диагнозе, результатах обследования, самом факте обращения за медицинской помощью и сведения о личной жизни, полученных при обследовании и лечении с целью обеспечения врачебной тайны;
- защита информации с грифами «особой важности», «совершенно секретно», «секретно», относящихся к сведениям в военной области, в области науки и техники, внешней политики и экономики, в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты в государственных органах власти и силовых структурах;
- предотвращение копирования и передачи информации третьим лицам, например средствам массовой информации, операторами систем видеонаблюдения и охранного телевидения;
- предотвращение копирования информации, представляющей коммерческую тайну, содержащую данные о ноу-хау, секретах производства и технологиях в коммерческих организациях, конструкторских бюро, научно-исследовательских институтах.

УДК 004.93′1:006.354 ОКС 35.020

Ключевые слова: системы киберфизические, интеллектуальная система предотвращения несанкционированного копирования информации с рабочих мест операторов автоматизированных информационных систем, общие требования

Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 24.06.2025. Подписано в печать 02.07.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

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