ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71844— 2024

Аэродромы гражданские. Искусственные покрытия

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРИ РАСПОЗНАВАНИИ ДЕФЕКТОВ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации»), Обществом с ограниченной ответственностью «А-Я эксперт» (ООО «А-Я эксперт»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 164 «Искусственный интеллект»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2024 г. № 1812-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», 2024

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 6
5 Общие требования 7
6 Требования к конфигурации 9
7 Рекомендации и требования к обучению модели искусственного интеллекта 10
8 Требования к методам тестирования 11
9 Требования к обеспечению информационной безопасности 12
Библиография 14

Введение

Настоящий стандарт разработан в целях обеспечения единых требований к разработке автоматизированных систем, использующих в составе своего математического и (или) программного обеспечения частные алгоритмы искусственного интеллекта для распознавания дефектов на искусственных покрытиях гражданских аэродромов. При этом модальность и источники данных для функционирования таких частных алгоритмов искусственного интеллекта не имеют значения и определяются требованиями к соответствующей автоматизированной системе.

Настоящий стандарт входит в комплекс национальных стандартов, регламентирующих применение технологий искусственного интеллекта, и относится к стандартам для частных алгоритмов искусственного интеллекта.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аэродромы гражданские.
Искусственные покрытия

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРИ РАСПОЗНАВАНИИ ДЕФЕКТОВ

Общие положения

Civil aerodromes. Artificial coatings. Artificial intelligence in defect recognition. General provisions

Дата введения — 2025—02—01

1 Область применения

Настоящий стандарт распространяется на процессы жизненного цикла автоматизированных систем, в составе программного обеспечения которых реализованы частные алгоритмы искусственного интеллекта, применяемые для распознавания дефектов на искусственных покрытиях гражданских аэродромов, и устанавливает общие положения по реализации и применению этих алгоритмов.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы:

ГОСТ 19.301 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению

ГОСТ 19.402 Единая система программной документации. Описание программы

ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 56546 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 57657 (ИСО 19131:2007) Пространственные данные. Спецификация информационного продукта

ГОСТ Р 57773 (ИСО 19157:2013) Пространственные данные. Качество данных

ГОСТ Р 58412 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения

ГОСТ Р 58833 Защита информации. Идентификация и аутентификация. Общие положения

ГОСТ Р 58973 Оценка соответствия. Правила к оформлению протоколов испытаний

ГОСТ Р 59547 Защита информации. Мониторинг информационной безопасности. Общие положения

ГОСТ Р 59793 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ Р 59898 Оценка качества систем искусственного интеллекта. Общие положения

ГОСТ Р 70252 Системы искусственного интеллекта на автомобильном транспорте. Системы управления движением транспортным средством. Требования к испытанию алгоритмов низкоуровневого слияния данных

Издание официальное

ГОСТ Р 70462.1/ISO/IEC TR 24029-1—2021 Информационные технологии. Интеллект искусственный. Оценка робастности нейронных сетей. Часть 1. Обзор

ГОСТ Р 71207 Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования

ГОСТ Р 71533—2024 Системы искусственного интеллекта на автомобильном транспорте. Системы управления движением транспортным средством. Требования к испытанию алгоритмов обнаружения и распознавания дорожной разметки

СП 491.1325800.2020 Аэродромы. Правила обследования технического состояния

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов (сводов правил) 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 документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку. Сведения о действии сводов правил можно проверить в Федеральном информационном фонде стандартов.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

автоматизированная система; АС: Система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.

Примечания

1 В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.

2 В зависимости от вида управляемого объекта (процесса) АСУ подразделяют, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т. д.

[ГОСТ Р 59853—2021, статья 2]

3.2

алгоритм искусственного интеллекта: Алгоритм, при реализации которого используются подходы, модели, методы, технологии искусственного интеллекта.

[ГОСТ Р 70981—2023, пункт 3.4]

3.3 **атака искажением данных:** Атака на модель машинного обучения, при которой злоумышленник вводит вредоносные или искаженные данные в обучающий набор данных, при этом целью атаки является изменение поведения модели, ухудшение ее производительности или создание уязвимостей, которые могут быть использованы в дальнейшем.

Примечание — Также используется термин «атака отравлением данных», в том числе см. [1] (УБИ.221).

3.4

атака подмены модели машинного обучения: Применение состязательного примера путем подачи его на вход системы искусственного интеллекта с целью отказа системы искусственного интеллекта.

Примечания

1 Обычно применяется к моделям искусственного интеллекта в форме нейронной сети.

2 См. [2], пункт 3.1.6.

[Адаптировано из ГОСТ Р 59921.7—2022, пункт 3.12]

3.5 **атака с внедрением вредоносного кода:** Атака на информационную систему, при которой злоумышленник вводит вредоносный код или команды в системы через уязвимые точки ввода данных с целью изменения ее поведения и получения несанкционированного доступа к данным или ресурсам системы.

Примечание — Основные виды инъекционных атак включают SQL-инъекции, инъекции команд операционной системы и инъекции скриптов. Также используется термин «инъекционная атака», в том числе см. [1] (УБИ.006).

3.6

аугментация данных: Процесс создания дополнительного набора данных из имеющегося набора данных.

Примечание — Применяется для увеличения обучающего набора данных путем модификации существующего набора данных.

[ГОСТ Р 59898—2021, пункт 3.2]

3.7

аэродром: Участок земли или поверхности воды с расположенными на нем зданиями, сооружениями и оборудованием, предназначенный для взлета, посадки, рулежки и стоянки воздушных судов.

[ГОСТ Р 55584—2013, статья 5]

3.8

вредоносный код: Программы или код, написанные с целью получения информации о системах или пользователях, уничтожения системных данных, создания благоприятных условий для дальнейшего несанкционированного проникновения в систему, фальсификации системных данных и отчетов, а также внесения путаницы в системные процессы и доставления длительных хлопот обслуживающему персоналу.

Примечание 1 — Вредоносные коды, используемые в ходе атак, могут принимать форму вирусов, червей, троянских коней или других автоматических программ, использующих уязвимости в системе.

Примечание 2 — Вредоносный код часто называют вредоносными программами.

[ГОСТ Р 56205—2014, пункт 3.2.70]

3.9

гиперпараметры (в машинном обучении): Параметры системы искусственного интеллекта, значения которых задаются до начала обучения и не изменяются в процессе обучения.

Примечание — У системы искусственного интеллекта может не быть гиперпараметров.

[ГОСТ Р 59900—2021, пункт 2.2]

3.10

гражданская авиация: Авиация, используемая в целях обеспечения потребностей граждан и экономики.

[Адаптировано из [2], статья 21.1]

3.11

гражданский аэродром: Аэродром, используемый для целей гражданской авиации.
[Адаптировано из [2], статья 40]

3.12

дефект: Отдельное несоответствие конструкции аэродромного покрытия параметрам, установленным нормативными документами.
[ГОСТ Р 71270—2024, пункт 3.1.9]

3.13 **дефектометрия:** Измерение геометрических размеров дефектов и определение их местоположения в объекте контроля.

3.14 **дефектоскопия:** Выявление дефектов объекта контроля.

3.15

жизненный цикл автоматизированной системы; жизненный цикл АС: Совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС.
[ГОСТ Р 59853—2021, статья 19]

3.16

искусственное покрытие: Конструкция, воспринимающая нагрузки и воздействия от воздушных судов, эксплуатационных и природных факторов.
[Адаптировано из СП 121.13330.2019, пункт 3.2]

3.17

искусственный интеллект; ИИ: Способность технической системы имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.
[ГОСТ Р 59276—2020, пункт 3.6]

3.18 **истинно положительный результат;** TP: Результат бинарной классификации, когда модель правильно классифицирует положительный класс как положительный.

3.19

качество: Совокупность характеристик и свойств системы ИИ, обусловливающих ее способность удовлетворять установленным или предполагаемым требованиям в соответствии с ее назначением.
[ГОСТ Р 59898—2021, пункт 3.9]

3.20

критерий оценки качества: Набор определенных и задокументированных правил и условий, которые используются для решения о приемлемости общего качества конкретной системы ИИ.
[ГОСТ Р 59898—2021, пункт 3.10]

3.21 **ложноотрицательный результат;** FN: Результат бинарной классификации, когда модель неправильно классифицирует положительный класс как отрицательный (ошибка второго рода).

3.22 **ложноположительный результат;** FP: Результат бинарной классификации, когда модель неправильно классифицирует отрицательный класс как положительный (ошибка первого рода).

3.23

метрика: Материальная мера некоторых аспектов характеристик качества.
[ГОСТ Р 59898—2021, пункт 3.12]

3.24 **метрика F1:** Метрика для оценки качества алгоритма классификации, которая учитывает обе метрики — точность (precision) и полноту (recall).

Примечания

1) Метрика F1 рассчитывается по формуле

$$F1\text{-score} = 2 \cdot (precision \cdot recall) / (precision + recall). \quad (1)$$

2) Значения метрики F1 находятся в диапазоне от 0 до 1 (или от 0 % до 100 %). Чем ближе значение метрики F1 к 1, тем лучше модель справляется с задачей классификации. Если значение метрики F1 равно 0, то это означает, что модель полностью не справляется с задачей классификации.

3.25 **модальность данных:** Характеристика набора данных, определяющая источник, формат и структуру данных, которые могут быть использованы для анализа, обработки и хранения в информационных системах.

3.26

обучающие данные: Подмножество доступных данных, используемых для обучения модели машинного обучения.

[ГОСТ Р 59895—2021, пункт 2.1.10]

3.27

онтология: Совокупность терминов (3.7), выражений отношения (3.6) и связанных с ними определений на естественном языке (3.8) вместе с одной или несколькими формальными теориями (3.11), предназначенными для отражения заданных интерпретаций этих определений.

[ГОСТ Р ИСО/МЭК 21838-1—2021, пункт 3.14]

3.28

перекрестная валидация: Статистический метод оценки и проверки устойчивости математических моделей.

Примечание — Перекрестная валидация особенно применяется в задачах машинного обучения и искусственного интеллекта, что включает в себя деление выборки данных на подвыборки, одна из которых используется для проверки модели, а оставшиеся — для ее обучения. Такой подход позволяет оценить то, как модель машинного обучения будет справляться с новыми данными, и провести проверку на переобучение.

[ГОСТ Р 71538—2024, пункт 3.12]

3.29 **полнота:** Метрика для оценки качества алгоритма классификации, которая показывает долю правильно классифицированных объектов среди всех объектов классификации и рассчитывается по формуле

$$recall = TP / (TP + FN), \quad (2)$$

где TP — истинно положительный результат;

FN — ложноотрицательный результат.

3.30 **положительный класс:** Класс в задаче классификации, который распознается (идентифицируется) моделью классификации.

Примечание — В задаче распознавания дефектов искусственных покрытий гражданских аэродромов положительным классом является наличие дефекта. Если модель распознает дефект в то время, как он в действительности имеется, это является истинно положительным результатом (TP). Если модель не распознает дефекта в то время, как он в действительности имеется, это является ложноотрицательным результатом (FN). Если модель распознает дефект в то время, как его в действительности нет, это является ложноположительным результатом (FP).

3.31

программное обеспечение: Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

[ГОСТ Р 56939—2016, пункт 3.11]

3.32

робастность: Способность системы ИИ поддерживать качество работы алгоритмов машинного обучения при любых условиях.

Примечание — В настоящем стандарте главным образом описываются условия, связанные со входными данными, такими как их спектр и характеристики. Но это определение представлено более широко, чтобы не исключать аппаратный сбой и другие виды условий.

[ГОСТ Р 70462.1—2022, пункт 3.6]

3.33

состязательный пример: Входные данные для модели искусственного интеллекта, созданные путем добавления универсального случайного возмущения к примеру входных данных, что приводит к тому, что система искусственного интеллекта выдает неверный результат с высокой степенью достоверности.

Примечания

1 Обычно применяется к моделям искусственного интеллекта в форме нейронной сети.

2 См. [2], пункт 3.1.7.

[ГОСТ Р 59921.7—2022, пункт 3.13]

3.34

строгая аутентификация: Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.

[ГОСТ Р 58833—2020, пункт 3.54]

3.35

существенный фактор эксплуатации: Важный входной параметр для алгоритма искусственного интеллекта, который относится к решаемой задаче и изменение значения которого существенно влияет на результат работы алгоритма.

[ГОСТ Р 70983—2023, пункт 3.15]

3.36 **точность:** Метрика для оценки качества алгоритма классификации, которая показывает долю правильно классифицированных объектов среди всех классифицированных объектов и рассчитывается по формуле

$$\text{precision} = TP / (TP + FP). \quad (3)$$

3.37 **частный алгоритм искусственного интеллекта;** ЧАИИ: алгоритм искусственного интеллекта, реализующий решение конкретной задачи.

Примечание — Для целей настоящего стандарта под ЧАИИ понимается алгоритм искусственного интеллекта для распознавания дефектов на искусственных покрытиях гражданских аэродромов.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИВПП — искусственная взлетно-посадочная полоса;

ПАГ — плита аэродромная гладкая;

ПИБ — подсистема информационной безопасности;

ПО — программное обеспечение;

ПС — программное средство;

СКЗИ — средство криптографической защиты информации;

СМС — служба коротких сообщений (англ. SMS — short message service);

СФЭ — существенный фактор эксплуатации;

ТЗ — техническое задание;

ЧТЗ — частное техническое задание;

CSV — значения, разделенные запятыми (comma-separated values);

FTP — протокол передачи файлов (file transfer protocol);

HTTP — протокол передачи гипертекста (hypertext transfer protocol);

IP — интернет-протокол (internet protocol);

JSON — описание объектов на синтаксисе языка программирования JavaScript (JavaScript object notation);

PDF — переносимый формат документа (portable document format);

SQL — язык структурированных запросов (structured query language);

SSH — протокол туннелирования TCP-соединений (secure shell);

TCP — протокол управления передачей (transmission control protocol);

XML — расширяемый язык разметки (extensible markup language).

5 Общие требования

5.1 Применимость требований к стадиям создания автоматизированных систем

5.1.1 Стадии создания АС определяют по ГОСТ Р 59793.

5.1.2 В таблице 1 приведено указание по применимости требований настоящего стандарта на стадиях создания АС.

Таблица 1 — Применимость требований на стадиях создания АС

Структурный элемент	Требования	Стадии создания АС, на которых применяются требования
5.2	Общие требования к ЧАИИ распознавания дефектов	1 Формирование требований к АС; 2 Разработка концепции АС; 3 ТЗ; 4 Эскизный проект; 5 Технический проект; 6 Рабочая документация
6	Требования к конфигурации	5 Технический проект; 6 Рабочая документация; 7 Ввод в действие
7	Рекомендации и требования к обучению модели ИИ	3 ТЗ; 4 Эскизный проект; 5 Технический проект; 6 Рабочая документация
8	Требования к методам тестирования	6 Рабочая документация; 7 Ввод в действие; 8 Сопровождение АС
9	Требования к обеспечению информационной безопасности	Все стадии создания АС

5.2 Общие требования к частному алгоритму искусственного интеллекта распознавания дефектов

5.2.1 ЧАИИ для распознавания дефектов искусственных покрытий гражданских аэродромов реализуется ПС из состава ПО АС в программно-аппаратном комплексе или ином изделии, используемом в целях обследования технического состояния искусственных покрытий гражданских аэродромов.

5.2.2 Классификация дефектов искусственных покрытий гражданских аэродромов и оценка их размеров должна охватывать дефекты, перечисленные в СП 491.1325800.2020 (приложение А). Распознаваемые классы дефектов необходимо перечислить в эксплуатационной документации на ПС, реализующее ЧАИИ, при этом для перечисления рекомендуется пользоваться следующим перечнем:

а) дефекты на жестких типах аэродромных покрытий (цементобетон, железобетон, ПАГ):

1) трещины, м,
2) сколы углов и кромок плит, м^2,
3) шелушение (поверхностное, глубокое), м^2,
4) сетка трещин, м^2,
5) уступы кромок плит, шт.,
6) просадка плит, шт.,
7) раковины, шт.,
8) выбоины, м^2,
9) нарушение герметизации швов, м,
10) разрушенные плиты, шт.;

б) дефекты на нежестких и смешанных типах аэродромных покрытий с верхним слоем из асфальтобетона:

1) продольные трещины, м (для расчета сигнальной оценки ИВПП),
2) поперечные трещины, м (для расчета сигнальной оценки ИВПП),
3) трещины, м,
4) сетка трещин (крокодиловая кожа), м^2,
5) эрозия (поверхностная, глубокая), м^2,
6) выбоины, м^2,
7) колееобразование (колея), м^2,
8) просадка, м^2,
9) пучение, м^2,
10) нарушение герметизации швов, м.

5.2.3 В ТЗ на ПО, в составе которого разработаны ПС, реализующие ЧАИИ, необходимо определить требования к режиму работы ПО.

5.2.4 Оценку робастности ЧАИИ осуществляют в соответствии с ГОСТ Р 70462.1.

5.2.5 В случае применения ПС, реализующего ЧАИИ, в системах, функционирующих в критически важных процессах обеспечения безопасности, эксплуатирующая организация должна разработать и внедрить систему мониторинга погрешности результата. Отклонение от заявленной в эксплуатационной документации погрешности результата, выдаваемого ЧАИИ, не должно превышать установленных требований.

5.2.6 Все составные части ПС, реализующего ЧАИИ, включая наборы данных для обучения и тестирования, должны быть доступны для аудита.

5.2.7 Критерии оценки качества модели ИИ, лежащей в основе ЧАИИ, приведенные в эксплуатационной документации, должны включать, как минимум, значения следующих показателей:

- точность и полноту распознавания дефектов либо метрику F1 для дефектоскопии;
- уровень ошибок первого рода (ложноположительных результатов);
- уровень ошибок второго рода (ложноотрицательных результатов);
- погрешность результатов дефектометрии.

Примечание — В ТЗ или ЧТЗ на ЧАИИ могут быть определены дополнительные критерии оценки качества модели ИИ и самого ЧАИИ в соответствии с требованиями ГОСТ Р 59898.

5.2.8 Критерии эффективности ПС, реализующего ЧАИИ, приведенные в эксплуатационной документации, должны включать, как минимум, значения следующих показателей:

- скорость обработки и анализа данных, время, затрачиваемое на обнаружение и классификацию дефектов при дефектоскосии, а также на дефектометрию обнаруженных дефектов;

- устойчивость ЧАИИ к вариативности условий эксплуатации (например, освещенность, погодные условия и др.), включая перечисления возможных интервалов значений характеристик условий эксплуатации.

5.2.9 В случае присоединения организации — разработчика ПС ЧАИИ к системе добровольной сертификации, направленной на обеспечение качества ПО, либо в случае требования заказчика ПО, реализующее ЧАИИ, а также все его модификации и обновления должны проходить процедуру сертификации для подтверждения соответствия установленным требованиям.

6 Требования к конфигурации

6.1 Оборудование, на котором выполняются ПС ЧАИИ для распознавания дефектов на искусственных покрытиях аэродромов, должно:

- быть оснащено вычислительными устройствами, технические характеристики которых достаточны для выполнения ЧАИИ без обращения к облачным вычислительным ресурсам;
- быть оснащено постоянными запоминающими устройствами (накопителями данных) для долговременного хранения результатов, объем которых достаточен для хранения результатов обработки площадей покрытия гражданских аэродромов, на которых эксплуатируется ЧАИИ;
- иметь аппаратные интерфейсы высокоскоростной передачи данных со скоростью передачи данных не менее 10 Гб/с.

6.2 Оборудование, на котором исполняется ПС ЧАИИ, должно обеспечивать функционирование моделей машинного обучения, лежащих в основе ЧАИИ.

6.3 В ТЗ или ЧТЗ на реализацию ПС ЧАИИ необходимо отразить требования к следующим показателям назначения:

- критерии оценки качества модели ИИ в соответствии с 5.2.7;
- скорость обработки входных данных;
- объем обрабатываемых входных данных;
- распознавание дефектов с заявленной точностью при изменении погодных условий или уровня освещенности, при этом допустимые условия и уровни необходимо перечислить в ТЗ или ЧТЗ;
- возможность отображения результатов анализа на экране оператора с выделением обнаруженных дефектов;
- наличие интуитивно понятного и эргономичного интерфейса пользователя;
- автоматическое ведение ведомости всех обнаруженных дефектов по СП 491.1325800.2020 и обеспечение возможности формирования отчетов за определенные периоды времени;
- масштабируемость для обработки увеличивающихся объемов данных и интеграции новых функциональных модулей без значительных доработок.

Примечание — В ТЗ или ЧТЗ на ЧАИИ могут быть определены требования к значениям перечисленных показателей качества для каждого класса дефектов в соответствии с 5.2.2.

6.4 В части интеграции в аэродромную программную и информационную инфраструктуру ПС ЧАИИ должно:

- быть совместимо с уже имеющимися информационными системами аэродрома, включая системы мониторинга состояния аэродромной инфраструктуры (при наличии);
- поддерживать стандартные форматы представления и обмена данных, (например, но не ограничиваясь, JSON, XML), а в случае использования технологий лазерного сканирования — форматы LAS и (или) LAZ;
- поддерживать стандартные протоколы обмена информацией, (например, но не ограничиваясь TCP/IP, FTP, HTTP, SSH);
- реализовывать механизмы оповещения и уведомления для операторов в случае обнаружения дефектов с возможностью отправки сводных уведомлений через различные каналы связи, а именно СМС, электронную почту, внутренние уведомления в системе и др.

6.5 В случае использования пространственных данных при разработке, обучении и функционировании ЧАИИ требования к ним определяют по ГОСТ Р 57657. Оценку качества таких данных осуществляют по ГОСТ Р 57773.

6.6 Если для распознавания дефектов искусственных покрытий аэродромов используются методы низкоуровневого слияния данных, следует применять положения ГОСТ Р 70252.

7 Рекомендации и требования к обучению модели искусственного интеллекта

7.1 Для обучения модели ИИ, которая может использоваться в составе ЧАИИ, рекомендуется подготовить обучающий набор размеченных данных.

7.2 В ТЗ или ЧТЗ на ПО, в составе которого разработаны ПС, реализующие ЧАИИ, должны быть:

- определены и перечислены источники данных, используемых для обучения модели ИИ и для функционирования ПС;
- определены требования к форматам входящей обрабатываемой информации и формату выходных результатов работы ЧАИИ;
- определены требования по совместимости с геоинформационными системами и системами управления базами данных.

7.3 В случае применения для реализации ЧАИИ машинного обучения с учителем рекомендуется разработать онтологию СФЭ и их значений для обучения персонала, участвующего в разметке данных, и возможной верификации результатов работы ЧАИИ людьми-экспертами.

7.4 Порядок составления онтологии СФЭ ЧАИИ для отражения всех вариаций значений характеристик распознаваемых типов дефектов:

а) определение основных понятий, таких как типы дефектов, их характеристики и характеристики воспринимаемой сцены в целом;

б) построение иерархической структуры, в которой должны быть сформированы общие и специализированные типы дефектов, перечислены значения характеристик дефектов и воспринимаемой сцены;

в) определение вариативных диапазонов для характеристик дефектов и воспринимаемой сцены в целом.

7.5 В ТЗ или ЧТЗ на ПО, в составе которого разработаны ПС, реализующие ЧАИИ, рекомендуется определить требования к возможности адаптации семантической онтологии под специфические условия эксплуатации, а также к возможности расширения семантической онтологии для учета новых типов дефектов, новых СФЭ, новых значений характеристик.

7.6 Данные из обучающего набора должны проходить проверку на наличие ошибочных и недостоверных элементов перед подачей на обучение модели.

7.7 Обучающему набору данных рекомендуется:

- покрывать полный спектр возможных дефектов, различных по типу, размеру и форме для обеспечения универсальности модели;
- включать варианты из разных географических и климатических регионов для повышения адаптивности модели;
- содержать выборки как истинно положительных размеченных данных, так и примеры ложноположительных данных, схожих с классифицируемыми дефектами (пример — трещины, залитые герметиком);
- содержать данные, которые корректно аннотированы для указания типов и характеристик распознаваемых дефектов и характеристик воспринимаемой сцены в целом при помощи семантической онтологии;
- быть сбалансированным по типам дефектов в соответствии с наблюдаемым соотношением типов для предотвращения переобучения модели на один из типов;
- быть поделенным на тренировочные и тестовые выборки для перекрестной валидации результатов обучения модели (рекомендуемое соотношение — 80 % для обучения и 20 % для тестирования), при этом разделение должно быть случайным, но каждый тип дефектов должен быть представлен в обеих выборках.

7.8 В случае необходимости применяют техники аугментации данных для увеличения объема и качества обучающих данных.

7.9 Все стадии подготовки данных, включая сбор, создание семантической онтологии (в случае применения), аннотирование и обработку данных, следует документировать. Документирование рекомендуется осуществлять в соответствии с требованиями, изложенными в ГОСТ Р 71533—2024 (раздел 7).

7.10 В ТЗ или ЧТЗ на ПО должны быть определены требования к процессу обучения модели ИИ на собранном обучающем наборе размеченных данных. Рекомендуется специфицировать следующие требования:

- к типу модели ИИ и ее архитектуре, соответствующим специфике задачи;

- к подбору гиперпараметров модели ИИ, таких как скорость обучения, количество эпох и слоев в нейронной сети (в случае использования);
- к итеративности обучения модели ИИ, а также к использованию перекрестной валидации для оценки ее качества;
- к запуску нескольких циклов обучения с различными параметрами для достижения оптимальных результатов;
- к регулярному сохранению промежуточных значений параметров модели ИИ для возможного восстановления или дообучения;
- к оценке производительности модели ИИ, для чего применяют метрики, состав и целевые значения которых должны быть указаны в ТЗ на ПО;
- к проверке на тестовом наборе данных для оценки обобщающей способности модели ИИ;
- к проведению дополнительных тестов на контрольных выборках, данные в которых не участвовали в процессе обучения, для выявления потенциальных проблем и переобученности модели ИИ;
- к оценке стабильности и надежности модели ИИ при варьировании входных данных и условий.

7.11 В ТЗ или ЧТЗ на ПО специфицируют требования к данным для детектирования дефектов на поверхности аэродромных покрытий, включая (но не ограничиваясь) следующие требования:
- к видам, типам, форматам, объемам данных, необходимых для детектирования дефектов на поверхности аэродромных покрытий;
- к ограничениям и к качеству исходных данных, возможных допусков;
- к процедурам сбора данных, используемым средствам измерения, их техническим характеристикам.

7.12 В процессе обучения модели ИИ необходимо осуществлять документирование всех этапов процесса обучения, включая настройки, гиперпараметры, методы аугментации и результаты перекрестной валидации, тестирования и оценки различных характеристик обученной модели. Документирование рекомендуется проводить по ГОСТ 19.402.

7.13 Оценку робастности полученной модели ИИ следует осуществлять в соответствии с требованиями ГОСТ Р 70462.1.

7.14 По результатам обучения модели ИИ должен быть составлен отчет о достигнутых значениях показателей качества модели и выводах о применимости для решения задачи распознавания дефектов искусственных покрытий гражданских аэродромов.

8 Требования к методам тестирования

8.1 Оценку качества АС, в составе которого функционируют ПС, реализующие ЧАИИ, необходимо осуществлять в соответствии с ГОСТ Р 59898.

8.2 Целью тестирования и оценки является проверка точности, надежности и эффективности ПС, реализующих ЧАИИ и используемых для распознавания дефектов на искусственных покрытиях гражданских аэродромов, включая проверку соответствия техническим характеристикам.

8.3 Тестовая среда может включать:
- реальные и аугментированные данные о дефектах покрытия;
- аппаратно-техническое обеспечение, аналогичное используемому в эксплуатационных условиях;
- средства для записи и анализа результатов.

8.4 Для тестирования следует использовать тестовые наборы данных, содержащие изображения или данные иных форматов, а также описания известных дефектов покрытий. Тестовые наборы данных должны быть подготовлены в соответствии с требованиями ГОСТ Р 59898.

8.5 Тестовые наборы данных, используемые для тестирования, обезличивают и освобождают от конфиденциальной информации.

8.6 Тестирование ПС ЧАИИ должно основываться на методе перекрестной валидации тестовым набором данных, предварительно разделенным на тестовую и валидирующую выборки.

8.7 Для проведения тестирования ПС ЧАИИ составляют программу и методику испытаний (по ГОСТ 19.301), в которой должны быть отражены целевые значения метрик качества ПС ЧАИИ, в том числе:
- точность и полнота модели ИИ, либо метрика F1;
- другие показатели качества модели ИИ (при необходимости).

8.8 Результаты тестирования ПС ЧАИИ необходимо документировать по ГОСТ Р 58973.

9 Требования к обеспечению информационной безопасности

9.1 Объектом защиты при обеспечении информационной безопасности является АС, в составе ПО которой реализовано ПС ЧАИИ. Основными значимыми защищаемыми компонентами являются:

- методика разметки данных;
- обучающие и тестовые выборки для обучения модели ИИ;
- результаты работы модели ИИ;
- каналы поступления входных данных.

9.2 Для решения задач обеспечения информационной безопасности при функционировании АС в ТЗ на разработку АС или в ЧТЗ на разработку ПИБ АС устанавливают требования на ПИБ с использованием положений следующих стандартов (не ограничиваясь): ГОСТ Р 51583, ГОСТ Р 56546, ГОСТ Р 56939, ГОСТ Р 58833, ГОСТ Р 59547, а также требования [3, 4] и принятые в соответствии с ними нормативные правовые акты.

9.3 ПО АС, реализующее ПС ЧАИИ, должно проходить регулярные мероприятия (работы) по выявлению и устранению уязвимостей, а также соответствия существующих (реализованных) требований информационной безопасности установленным требованиям [5, 6], ГОСТ Р 59547, ГОСТ Р 71207 и ГОСТ Р 56939, в том числе путем выявления и устранения уязвимостей в ПО. В качестве методов поиска и выявления уязвимостей ПО могут использоваться (не ограничиваясь):

- статический анализ ПО;
- динамический анализ ПО;
- композиционный анализ при использовании привлекаемых или заимствуемых компонентов ПО;
- комплексные стратегии, имитирующие действия возможных злоумышленников.

По результатам проверок составляют и реализовывают план устранения уязвимостей. Частоту проверок определяют в эксплуатационной документации, но не реже, чем один раз в год.

9.4 Права доступа к данным, используемым ПС ЧАИИ, должны определяться с использованием принципа минимума необходимых привилегий. При организации доступа к данным, используемым ПС ЧАИИ, необходимо использовать идентификацию и строгую аутентификацию пользователей и (или) средств вычислительной техники, которые реализуют в соответствии с требованиями ГОСТ Р 58833.

9.5 Для защиты данных, используемых в ПС ЧАИИ для распознавания дефектов, от несанкционированного копирования, модификации, удаления и блокирования, должна быть разработана модель угроз с учетом рекомендаций [5, 7], на основе которой должны определяться меры защиты.

9.6 Разработку ПС, реализующего ЧАИИ, осуществляют с учетом требований ГОСТ Р 56939, ГОСТ Р 58412 и [4].

9.7 Разработку ПС ЧАИИ (включая разработку и обучение модели ИИ) следует осуществлять в соответствии с требованиями ГОСТ Р 56939 и [7, 8], а также предусматривать (но не ограничиваться ими) организационно-технические меры по предотвращению атак с внедрением вредоносного кода, атак искажением данных, атак подмены модели машинного обучения и других типов атак на модели ИИ, известные на момент разработки и обучения модели ИИ, используемой в ЧАИИ.

9.8 Все передаваемые и хранимые данные должны быть защищены с использованием СКЗИ в соответствии с законодательством Российской Федерации [3, 9], применение которых должно быть достаточно для реализации заявленного в ТЗ или ЧТЗ на ПИБ уровня информационной безопасности [10]. Для хранимых данных необходимо обеспечить проверку подлинности. При использовании для шифрования данных СКЗИ должны быть соблюдены требования законодательства Российской Федерации в части эксплуатации СКЗИ.

9.9 Ключи шифрования данных для обучения модели ИИ следует регулярно менять в соответствии с политиками безопасности и хранить в защищенных хранилищах ключей. Частоту смены ключей определяет политика безопасности, внедренная организацией — разработчиком ПС ЧАИИ, или документаця на СКЗИ.

9.10 ПИБ АС должна реализовывать следующие функции защиты: обеспечение конфиденциальности и контроля целостности обучающих и тестовых наборов данных, а также защиты от несанкционированного доступа к ПС ЧАИИ.

9.11 Данные из обучающего набора должны быть защищены от несанкционированного доступа и неправомерного использования.

9.12 Необходимо обеспечить конфиденциальность тестовых наборов данных, используемых при добровольной сертификации ПС ЧАИИ на соответствие требованиям.

9.13 При применении коммуникационных каналов для передачи данных, используемых ПС ЧАИИ для распознавания дефектов и результатов их распознавания, необходимо обеспечить защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию строгой аутентификации в соответствии с ГОСТ Р 58833.

9.14 Обеспечение информационной безопасности АС ЧАИИ, отнесенных к значимым объектам критической информационной инфраструктуры, должно осуществляться в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (см. [3]).

Библиография

[1] Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»). — URL: gost.e-ecolog.ru (дата обращения: 21.10.2024)

[2] Воздушный кодекс Российской Федерации от 19 марта 1997 г. № 60-ФЗ

[3] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[4] Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах»

[5] Методический документ «Методика оценки угроз безопасности информации» (утвержден Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

[6] Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)» (утвержден Федеральной службой по техническому и экспортному контролю 17 мая 2023 г.)

[7] Методический документ «Меры защиты информации в государственных информационных системах» (утвержден Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.)

[8] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены Приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239)

[9] Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утверждено Приказом ФСБ России от 9 февраля 2005 г. № 66)

[10] Р 1323565.1.012—2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

УДК 62-52:006.354 ОКС 35.240.60

Ключевые слова: аэродромы гражданские, искусственные покрытия, искусственный интеллект, распознавание дефектов

Редактор *З.А. Лиманская*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 03.12.2024. Подписано в печать 16.12.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.

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

gost.e-ecolog.ru