ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71895.2— 2025

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

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

Часть 2

Методология проведения испытаний

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») и Акционерным обществом «ЭЛВИС-НеоТек» (АО «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. № 597-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», 2025

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 3
5 Проведение эксплуатационных испытаний 3
5.1 Виды эксплуатационных испытаний 3
5.2 Планирование испытания 4
5.3 Объем испытания 4
5.4 Общие требования к наборам данных для испытаний 5
6 Метрики оценки ИСПНКИ 5
6.1 Общие положения 5
6.2 Метрики оценки ИСПНКИ 5
7 Протоколы испытаний 8
7.1 Фундаментальные показатели 8
7.2 Учет особенностей испытания 8
7.3 Графическое представление результатов испытания 8
Приложение А (справочное) Объем испытаний и случайная неопределенность 11
Приложение Б (рекомендуемое) Форма протокола технологического испытания ИСПНКИ 13

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

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

Часть 2

Методология проведения испытаний

Cyberphysical systems.
An intelligent system to prevent unauthorized copying of information from the workplaces of operators of automated information systems.
Part 2. Testing methodology

Дата введения — 2025—08—01

1 Область применения

Настоящий стандарт устанавливает требования:
- к проведению эксплуатационных испытаний;
- порядку и объему выборки;
- принципам и методам оценки эксплуатационных характеристик;
- протоколам испытаний;
- базовым наборам данных для демонстрации или проверки систем.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

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

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.

Издание официальное

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.

3.4 **испытательная организация:** Официальная организация, под руководством которой проводится испытание.

3.5 **экспериментатор:** Человек, несущий ответственность за описание, разработку и анализ испытания.

3.6 **администратор испытания:** Человек, проводящий испытание.

3.7 **наблюдатель испытания:** Человек, записывающий данные испытания или наблюдающий за испытуемой группой.

3.8 **вероятность ошибки классификации предъявления с фактом несанкционированного копирования информации;** ВКсФН: Доля предъявлений с фактом несанкционированного копирования информации, которые некорректно классифицируют как предъявления без факта несанкционированного копирования информации, от общего количества предъявлений с фактом несанкционированного копирования информации в конкретном сценарии.

3.9 **вероятность ошибки классификации предъявления без факта несанкционированного копирования информации;** ВКбФН: Доля предъявлений без факта несанкционированного копирования информации, которые некорректно классифицируют как предъявления с фактом несанкционированного копирования информации, от общего количества предъявлений без факта несанкционированного копирования информации в конкретном сценарии.

3.10 **вероятность отсутствия ответа на предъявление с фактом несанкционированного копирования информации;** ВОсФН: Доля попыток предъявлений с фактом несанкционированного копирования информации, которые вызывают отсутствие ответа со стороны системы, от общего количества попыток предъявлений с фактом несанкционированного копирования информации в конкретном сценарии.

3.11 **вероятность отсутствия ответа на предъявление без факта несанкционированного копирования информации;** ВОбФН: Доля попыток предъявлений без факта несанкционированного копирования информации, которые вызывают отсутствие ответа со стороны системы, от общего количества попыток предъявлений без факта несанкционированного копирования информации в конкретном сценарии.

3.12 **обобщенная вероятность ошибки классификации предъявления с фактом несанкционированного копирования информации;** ОВКсФН: Доля попыток предъявлений с фактом несанкционированного копирования информации, которые некорректно классифицируют как предъявления без факта несанкционированного копирования информации, от общего количества попыток предъявлений с фактом несанкционированного копирования информации в конкретном сценарии.

3.13 **обобщенная вероятность ошибки классификации предъявления без факта несанкционированного копирования информации;** ОВКбФН: Доля попыток предъявлений без факта несанкционированного копирования информации, которые некорректно классифицируют как предъявления с фактом несанкционированного копирования информации или которые вызывают отсутствие ответа со стороны системы, от общего количества попыток предъявлений без факта несанкционированного копирования информации в конкретном сценарии.

3.14 **длительность обработки предъявления с фактом несанкционированного копирования информации;** ДОсФН: Время, необходимое для классификации системой предъявления с фактом несанкционированного копирования информации.

3.15 **длительность обработки предъявления без факта несанкционированного копирования информации;** ДОбФН: Время, необходимое для классификации системой предъявления без факта несанкционированного копирования информации.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ВКсФН — Вероятность ошибки классификации предъявления с фактом несанкционированного копирования информации;

ВКбФН — Вероятность ошибки классификации предъявления без факта несанкционированного копирования информации;

ВОсФН — Вероятность отсутствия ответа на предъявление с фактом несанкционированного копирования информации;

ВОбФН — Вероятность отсутствия ответа на предъявление без факта несанкционированного копирования информации;

ДОсФН — Длительность обработки предъявления с фактом несанкционированного копирования информации;

ДОбФН — Длительность обработки предъявления без факта несанкционированного копирования информации;

КОО — Компромиссное определение ошибки;

ОВКсФН — Обобщенная вероятность ошибки классификации предъявления с фактом несанкционированного копирования информации;

ОВКбФН — Обобщенная вероятность ошибки классификации предъявления без факта несанкционированного копирования информации;

РВО — Равная вероятность ошибок первого и второго рода;

РХ — Рабочая характеристика;

ССОЗ — Средняя скорость обработки запросов.

5 Проведение эксплуатационных испытаний

5.1 Виды эксплуатационных испытаний

Технические эксплуатационные испытания ИСПНКИ могут быть трех видов: технологическое, сценарное и оперативное.

В процессе технологического испытания проводят испытание одного или нескольких алгоритмов с использованием базы данных. Сбор базы данных может быть частью испытания, или можно использовать заранее собранную базу данных, доступную экспериментатору. Несмотря на то, что для разработки и настройки ИСПНКИ перед испытанием можно использовать демонстрационные данные, фактическое испытание необходимо проводить на данных, которые ранее не использовались разработчиками алгоритмов. Испытание проводят путем обработки данных в режиме отложенного задания. Вследствие неизменяемости базы данных результаты технологических испытаний являются воспроизводимыми. Тем не менее, эксплуатационные характеристики по отношению к этой базе данных будут зависеть как от внешних условий, так и от выборки.

В процессе сценарного испытания проводят испытание одной или нескольких полнокомплектных ИСПНКИ в условиях, моделирующих определенную ситуацию, максимально приближенную к действительности. Каждая испытуемая система имеет свой собственный датчик сбора данных, в результате чего могут быть небольшие различия в получаемых начальных данных. Следовательно, если сравниваются несколько ИСПНКИ, необходимо уделить внимание тому, чтобы сбор данных для всех испытуемых систем проходил в одних и тех же условиях окружающей среды и с использованием одной и той же выборки. В зависимости от требований к испытанию обработка данных может быть как в режиме

отложенного задания, так и в режиме реального времени. Воспроизводимость результатов испытания обеспечивается тщательным контролем выполнения сценария.

Оперативное испытание обычно проводится в режиме реального времени для обеспечения согласованности со средой применения (если только испытуемые системы не обрабатывают данные в режиме отложенного задания). Воспроизводимость результатов оперативного испытания может быть ограничена из-за неизвестных и недокументированных различий в условиях эксплуатации. Более того, может быть трудно установить «истинную информацию» поведения субъектов сбора данных, особенно в условиях отсутствия администратора испытания, наблюдателя испытания или обслуживающего персонала.

5.2 Планирование испытания

5.2.1 Общие положения

На первом этапе испытания экспериментатор должен определить:

а) тип испытуемых систем, их применение, условия испытания и выборку;

б) эксплуатационные характеристики, которые необходимо измерить;

в) данные, необходимые для оценки эксплуатационных характеристик (т. е. определить тип испытания: технологическое, сценарное или оперативное).

Вышеуказанные данные являются основой для разработки соответствующего протокола испытания, определяя необходимые средства контроля условий испытаний, выборку испытуемых субъектов и объем испытаний.

Примечание — Вид испытания может быть определен заранее, например при наличии базы данных для технологического испытания или установленной системы для оперативного испытания. Возможны также условия, при которых все виды испытаний могут быть проведены последовательно, с постепенным сужением вариантов систем, рассматриваемых для ввода в эксплуатацию.

Настоящий стандарт регламентирует основные принципы проведения оценки эксплуатационных характеристик и оформления протокола испытаний. Методы и требования к конкретным видам испытаний, биометрическим модальностям и целевым применениям в настоящем стандарте не рассматриваются.

5.2.2 Контроль факторов, влияющих на эксплуатационные характеристики

Показатели эксплуатационных характеристик ИСПНКИ могут значительно зависеть от способов ее применения, условий окружающей среды и выборки.

Факторы, влияющие на измеряемые эксплуатационные характеристики, должны быть явно или неявно отнесены к одному из следующих четырех классов:

а) контролируемые управляемые факторы, включенные в методику испытания (как независимые переменные), которые можно наблюдать, протоколировать и анализировать;

б) контролируемые неуправляемые факторы (постоянные в течение испытаний), являющиеся частью условий испытания;

в) неконтролируемые факторы — случайные и независимые от испытания факторы;

г) незначительные факторы, эффект от которых не будет учитываться. Без данной категории факторов испытание будет очень сложным.

До начала сбора данных должно быть определено, каким образом будет осуществляться контроль данных факторов.

При технологическом испытании могут быть учтены особенности применения и выборки, гарантирующие, что испытания будут не слишком трудными и не слишком простыми для испытуемых алгоритмов.

Для того чтобы ИСПНКИ могла быть испытана на репрезентативной выборке в реальных условиях, при сценарном испытании должны быть определены и смоделированы условия реального применения и выборка.

При оперативном испытании условия окружающей среды и выборка определяются в реальных условиях под контролем экспериментатора.

5.3 Объем испытания

Масштаб испытания с точки зрения объема базы данных влияет на точность измерения вероятностей ошибок. Чем больше объем испытания, тем выше точность результатов. Для установления нижних границ количества попыток или предъявлений, необходимых для заданного уровня точности, применяют правило трех или правило тридцати (см. приложение А, раздел А.1).

5.4 Общие требования к наборам данных для испытаний

Для проведения технологических испытаний ИСПНКИ необходима база данных.

База данных для проведения технологических испытаний ИСПНКИ должна быть объективной: в частности, она не должна быть доступна разработчикам ИСПНКИ.

Для формирования базы данных создают два раздела:

- раздел «Предъявления с фактом несанкционированного копирования информации»;
- раздел «Предъявления без факта несанкционированного копирования информации».

Раздел «Предъявления с фактом несанкционированного копирования информации» представляет собой набор видеозаписей/видеопотоков, на которых съемка с экрана производится с помощью смартфона или планшета. При этом смартфон или планшетный компьютер должен находиться в положении, в котором возможна съемка с экрана.

База данных формируется путем объединения двух разделов. Перед объединением создается список с принадлежностями каждого предъявления к разделу. После объединения раздел подвергается дополнительному перемешиванию и переименованию файлов.

Для проведения технологических испытаний экспериментатор должен располагать базой данных для проведения технологических испытаний ИСПНКИ для каждого типа сканера средств фото/видеофиксации (web-камера; 3D камера). Общие технические требования к базе данных для проведения технологических испытаний ИСПНКИ представлены в таблице 1.

Таблица 1 — Общие технические требования к базе данных для проведения технологических испытаний ИСПНКИ

№	Параметр	Описание
1	Разрешение файла, пикселей	Не менее 220 x 220
2	Соотношение сторон кадра	От 3:4 до 16:9
3	Интервал следования ключевых кадров	Не более 1 с

6 Метрики оценки ИСПНКИ

6.1 Общие положения

Эксплуатационные характеристики ИСПНКИ могут быть выражены вероятностями ошибок классификации, вероятностями отсутствия ответа и другими вероятностными метриками. Такие метрики можно использовать в оценках безопасности, научно-образовательных оценках, процессах методических технологий или разработки продукта либо в оперативной оценке производительности конечным пользователем.

6.2 Метрики оценки ИСПНКИ

6.2.1 Общие положения

При оценке ИСПНКИ измеряют способность систем правильно классифицировать факт несанкционированного копирования информации.

6.2.2 Метрики отсутствия ответа

Принимая во внимание рекомендации разработчика ИСПНКИ и предполагаемый сценарий использования, экспериментатор должен определить, что представляет собой отсутствие ответа, и указать условия, при которых отсутствие ответа влияет на вероятность ошибок классификации.

Экспериментатор должен указать вероятности отсутствия ответа для ИСПНКИ, используя следующие характеристики:

- ВОсФН и размер выборки, по которой проведены вычисления;
- ВОбФН и размер выборки, по которой проведены вычисления.

ВОсФН рассчитывают по формуле

$$\text{ВОсФН} = \left(\frac{1}{N}\right)\sum_{i=1}^{N} Res_i, \quad (1)$$

где N — число попыток предъявлений с фактом несанкционированного копирования информации;

Res_i — результат классификации; равен 1, если i-е предъявление не классифицируется, и равен 0, если классифицируется.

ВОбФН рассчитывают по формуле

$$\text{ВОбФН} = \left(\frac{1}{N}\right)\sum_{i=1}^{N} Res_i, \quad (2)$$

где N — число попыток предъявлений без факта несанкционированного копирования информации;

Res_i — результат классификации; равен 1, если i-е предъявление не классифицируется, и равен 0, если классифицируется.

6.2.3 Метрики классификации

В протоколе оценки ИСПНКИ должны быть указаны ВКсФН и ВКбФН.

В протоколе должно быть указано, каким образом решения системы и баллы использованы для классификации предъявлений.

ВКсФН рассчитывают по формуле

$$\text{ВКсФН} = 1 - \left(\frac{1}{N}\right)\sum_{i=1}^{N} Res_i, \quad (3)$$

где N — число предъявлений с фактом несанкционированного копирования информации;

Res_i — результат классификации; равен 1, если i-е предъявление классифицировано как предъявление с фактом несанкционированного копирования информации, и равен 0, если предъявление без факта несанкционированного копирования информации.

В протоколе оценки ИСПНКИ должны быть указаны числа правильно и неправильно классифицированных предъявлений с фактом несанкционированного копирования информации.

ВКбФН рассчитывают по формуле

$$\text{ВКбФН} = \frac{\sum_{i=1}^{N} Res_i}{N}, \quad (4)$$

где N — число предъявлений без факта несанкционированного копирования информации;

Res_i — результат классификации; равен 1, если i-е предъявление классифицируется как предъявление с фактом несанкционированного копирования информации, и равен 0, если предъявление без факта несанкционированного копирования информации.

Указание в протоколе испытаний совокупного показателя ВКсФН и ВКбФН (например, усредненной вероятности ошибок) не соответствует требованиям настоящего стандарта.

Показатели классификации могут быть указаны в виде единого значения ВОКПбФНКИ при фиксированном значении ВКсФН.

Пример — В протоколе может быть указано, что при ВКсФН, равной 5 %, ВКбФН принимает значение 20 %.

В протоколе оценки ИСПНКИ могут быть указаны ОВКсФН и ОВКбФН.

ОВКсФН рассчитывают по формуле

$$\text{ОВКсФН} = (1 - \text{ВОсФН}) \cdot \text{ВКсФН} \quad (5)$$

ОВКбФН рассчитывают по формул:

$$\text{ОВКбФН} = \text{ВОбФН} + (1 - \text{ВОбФН}) \cdot \text{ВКбФН} \quad (6)$$

В протоколе оценки ИСПНКИ должна быть указана РВО. РВО для ИСПНКИ рассчитывают по формуле

$$\text{РВО} = \arg\min_{\text{ВКбФН}} |\text{ВКбФН} - \text{ВКсФН}| \quad (7)$$

В протоколе оценки ИСПНКИ может быть указана обобщенная РВО. Обобщенную РВО для ИСПНКИ рассчитывают по формуле

$$\text{РВО}_{\text{обобщенная}} = \arg\min_{\text{ОВКбФН}} |\text{ОВКбФН} - \text{ОВКсФН}| \quad (8)$$

6.2.4 Метрики эффективности

Экспериментатор должен указать длительность обработки системой как среднее значение длительности. Длительность следует указывать отдельно для предъявлений с фактом несанкционированного копирования информации (ДОсФН) и без него (ДОбФН). Отсутствие ответа не учитывают при расчете длительности. Длительность может быть определена прямым наблюдением.

ДОсФН рассчитывают по формуле

$$\text{ДОсФН} = \frac{\sum_{i=1}^{N} \tau_i}{N}, \quad (9)$$

где N — число предъявлений с фактом несанкционированного копирования информации;

τ_i — длительность обработки системой предъявления с фактом несанкционированного копирования информации.

ДОбФН рассчитывают по формуле

$$\text{ДОбФН} = \frac{\sum_{i=1}^{N} \tau_i}{N}, \quad (10)$$

где N — число предъявлений без факта несанкционированного копирования информации;

τ_i — длительность обработки системой предъявления без факта несанкционированного копирования информации.

ССОЗ рассчитывают по формуле (запросов/с)

$$\text{ССОЗ} = \frac{N}{T_2 - T_1}, \quad (11)$$

где N — число поданных предъявлений;

T_1 — время отправки первого предъявления/первого пакета с предъявлениями на проверку;

T_2 — время получения ответа от ИСПНКИ по последнему обработанному предъявлению.

6.2.5 Краткие выводы

В таблице 2 перечислены эксплуатационные характеристики для оценки ИСПНКИ.

Таблица 2 — Метрики эксплуатационных характеристик ИСПНКИ

Метрика	Тип предъявления	Занесение в протокол испытаний
ВКсФН	С фактом несанкционированного копирования информации	Обязательное
ВКбФН	Без факта несанкционированного копирования информации	Обязательное
ВОсФН	С фактом несанкционированного копирования информации	Обязательное
ВОбФН	Без факта несанкционированного копирования информации	Обязательное
ОВКсФН	С фактом несанкционированного копирования информации	Необязательное
ОВКбФН	Без факта несанкционированного копирования информации	Необязательное
ДОсФН	С фактом несанкционированного копирования информации	Обязательное
ДОбФН	Без факта несанкционированного копирования информации	Обязательное
ССОЗ	Все	Необязательное
РВО	Все	Обязательное
РВО (обобщенная)	Все	Необязательное

7 Протоколы испытаний

7.1 Фундаментальные показатели

В протоколе эксплуатационных испытаний ИСПНКИ должны быть указаны следующие показатели:

а) ВОсФН или указание, что ВОсФН неизвестна;

б) ВОбФН или указание, что ВОбФН неизвестна;

в) ВКсФН и соответствующая ВКбФН (по всему диапазону пороговых значений);

г) ОВКсФН и соответствующая ОВКбФН (по всему диапазону пороговых значений) с описанием метода обобщения (при необходимости);

д) ДОсФН;

е) ДОбФН;

ж) ССОЗ (при необходимости);

и) РВО;

к) РВО (обобщенная) (при необходимости).

7.2 Учет особенностей испытания

Показатели эксплуатационных характеристик зависят от вида испытания, особенностей применения системы и выборки. Для получения правильного представления о данных показателях необходимо знать:

а) подробную информацию об испытуемой системе (системах);

б) вид испытания:

- технологическое;
- сценарное;
- оперативное.

в) объем испытания;

г) условия окружающей среды;

д) критерии принятия решений;

е) параметры контроля факторов, воздействующих на эксплуатационные характеристики;

ж) данные о внештатных ситуациях и данные, не включенные в анализ;

и) данные о неконтролируемых факторах (и методы оценки данных факторов);

к) любые отклонения от требования настоящего стандарта должны быть обоснованы.

7.3 Графическое представление результатов испытания

7.3.1 Общие положения

Эксплуатационные характеристики должны быть изображены в виде кривых РХ или КОО по всему диапазону пороговых значений.

Масштабы осей (граничные значения и использование логарифмических масштабов) должны обеспечивать наглядно представленные результаты и быть согласованы для различных графиков в одном протоколе испытаний. Для обеспечения наглядности при изменении масштаба на графиках должна быть пометка об изменении масштаба.

7.3.2 График рабочей характеристики

Вероятность ошибки можно представить на графике в виде функции от порога принятия решения, например как на рисунке 1.

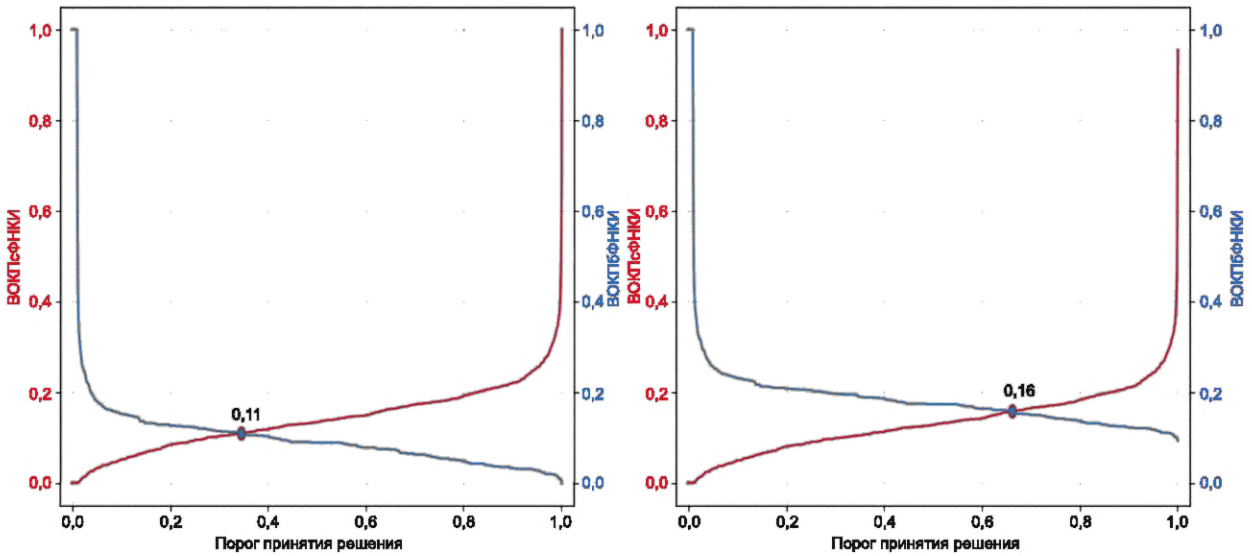


Рисунок 1 — Пример графиков РХ с отмеченной РВО

7.3.3 График КОО

Эксплуатационные характеристики системы могут быть изображены в виде графика КОО по всему диапазону порогов принятия решения. Графики КОО являются независимыми от порога, что позволяет сравнивать эксплуатационные характеристики различных систем при одинаковых условиях или одной системы при различных условиях.

Графики КОО могут быть использованы для построения вероятностей ошибок классификации (ВКбФН в зависимости от ВКсФН, ОВКбФН в зависимости от ОВКсФН).

На графике КОО по оси абсцисс (ось *x*) откладывают ложноположительную вероятность, а оси ординат (ось *y*) — ложноотрицательную вероятность. Шкалы осей, показывающие граничные значения, должны обеспечивать наглядное представление результатов. Для лучшего определения вероятностей ошибок в интересующем диапазоне графики КОО обычно строят с использованием шкалы с нормальным отклонением или логарифмической шкалы. Построение графика КОО с логарифмической шкалой по осям обеспечивает большую детализацию при низких вероятностях ошибок и помогает различать системы, работающие похожим образом.

На рисунке 2 показан пример построения графиков КОО с использованием логарифмической шкалы.

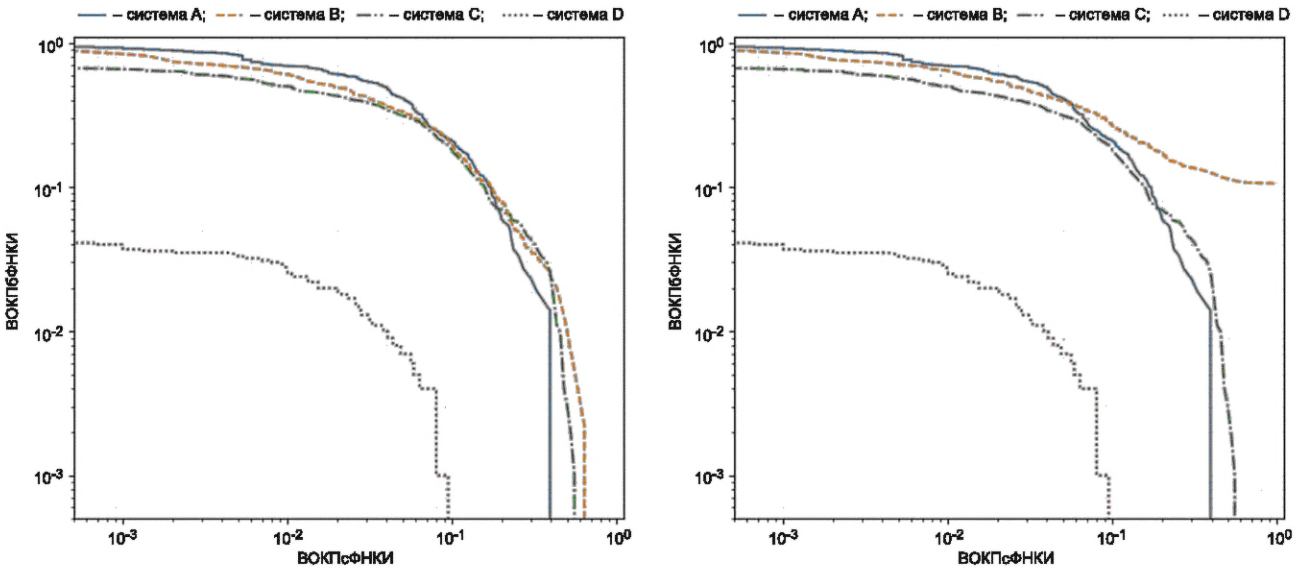


Рисунок 2 — Примеры графиков КОО с использованием логарифмической оси

Приложение А
(справочное)

Объем испытаний и случайная неопределенность

А.1 Доверительные интервалы и объем испытаний для независимых одинаково распределенных результатов

А.1.1 Правило трех

Правило трех используется при определении наименьшей вероятности ошибки, которая может быть статистически значимо установлена для N независимых одинаково распределенных результатов. Если значение вероятности ошибки p, для которого вероятность нулевой погрешности при N испытаниях является случайной и равна, например, 5 %, то

$$p \approx 3/N$$

с доверительной вероятностью 95 %*.

Примечание — $1\ p \approx 2/N$ с доверительной вероятностью 90 %.

А.1.2 Правило тридцати

В правиле тридцати утверждается, что для того, чтобы с доверительной вероятностью 90 % истинная вероятность ошибки находилась в диапазоне ± 30 % от установленной вероятности ошибки, должно быть зарегистрировано не менее 30 ошибок. Правило следует непосредственно из биномиального распределения при независимых попытках и может применяться с учетом ожидаемых эксплуатационных характеристик для выполнения оценки.

Примечание — Правило является общим для разных доверительных интервалов. Например, чтобы быть на 90 % уверенным, что истинная вероятность ошибки находится в диапазоне ±10 % установленного значения, необходимо, чтобы было выявлено не менее 260 ошибок. Чтобы быть на 90 % уверенным, что истинная вероятность ошибки находится в диапазоне ±50 % наблюдаемого значения, необходимо, чтобы было выявлено не менее 11 ошибок.

А.1.3 Число сравнений для обеспечения требуемой вероятности ошибки

Число статистически независимых результатов, необходимых для обеспечения требуемой вероятности ошибки, показано на рисунке А.1.

* Здесь и далее доверительная вероятность определяется как 100 %-ный уровень значимости, т. е. доверительная вероятность 95 % соответствует уровню значимости 5 %.

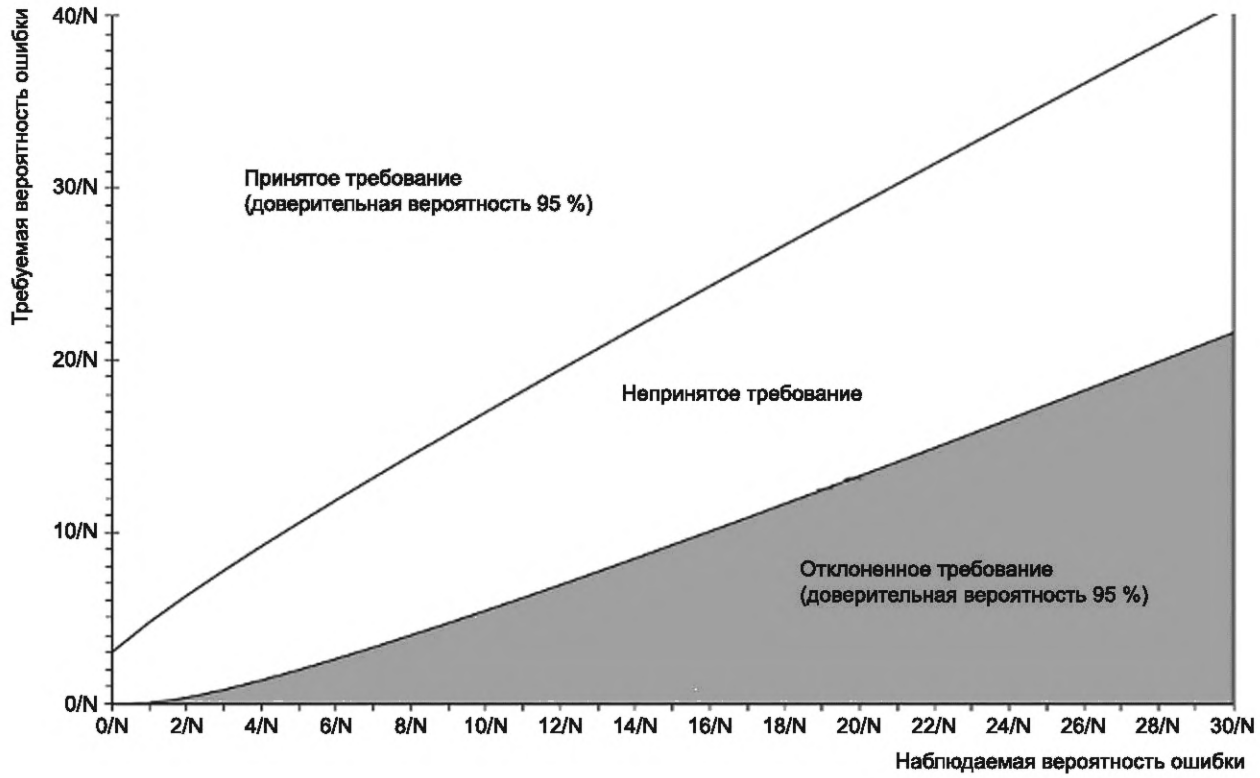


Рисунок А.1 — Области, определяемые с доверительной вероятностью 95 %, для принятия (или отклонения) требуемой вероятности ошибки при объеме испытаний *N*

Примечание — Диаграмма, приведенная на рисунке А.1, обеспечивает корректное приближение, если требуемая вероятность ошибки не более 1 %.

А.2 Оценка дисперсии эксплуатационных характеристик

А.2.1 Общие положения

В данном разделе приведены формулы и методы оценки дисперсии эксплуатационных характеристик. Дисперсия — статистическая мера погрешности, которая может использоваться при оценке доверительных интервалов и др. Применение данных формул зависит от следующих предположений относительно распределения ошибок сравнения:

а) попытки несанкционированного копирования информации не зависят от порогов принятия решений. В ином случае оценки вероятностей ошибок могут быть смещены;

б) число наблюдаемых ошибок является достаточно большим. При отсутствии наблюдаемых ошибок при вычислении по формулам получают нулевую дисперсию, и в этом случае применяют правило трех.

А.2.2 Оценка дисперсии

Для оценки дисперсии наблюдаемой вероятности ошибки используют следующие формулы:

$$\hat{p} = \frac{a}{n}, \tag{A.1}$$

$$\hat{V}(\hat{p}) = \frac{\hat{p} \cdot (1 - \hat{p})}{n - 1}, \tag{A.2}$$

где n — общее число результатов классификации;

a — число ошибочных результатов классификации;

$\hat{p}$ — наблюдаемая вероятность ошибки;

$\hat{V}(\hat{p})$ — оценка дисперсии наблюдаемой вероятности ошибки.

Приложение Б
(рекомендуемое)

Форма протокола технологического испытания ИСПНКИ

Б.1 Основные положения

Б.1.1 Объект испытаний

ИСПНКИ — интеллектуальная система предотвращения несанкционированного копирования информации.
<Полное наименование разработчика ИСПНКИ>
<Дата выпуска (релиза) ИСПНКИ>
<Номер версии ИСПНКИ в формате A.B.C.D>

Б.1.2 Цель испытания ИСПНКИ

Целью проведения испытания ИСПНКИ является определение следующих эксплуатационных характеристик:
- ВКсФН;
- ВКбФН;
- ВОсФН;
- ВОбФН;
- ОВОсФН;
- ОВОбФН;
- ДОсФН;
- ДОбФН;
- ССОЗ;
- РВО;
- РВО (обобщенная).

Б.1.3 Испытательная лаборатория (Экспериментатор)

<Полное наименование испытательной лаборатории>
<Фамилия, имя, отчество руководителя испытательной лаборатории>
<Фамилия, имя, отчество сотрудника испытательной лаборатории, проводящего испытания>

Б.1.4 Заказчик испытания ИСПНКИ

<Полное наименование заказчика испытания ИСПНКИ>

Б.1.5 Место проведения испытания ИСПНКИ

<Адрес испытательной лаборатории>

Б.1.6 Дата проведения испытания ИСПНКИ

<Дата начала проведения испытания ИСПНКИ в формате ДД.ММ.ГГГГ>
<Дата окончания проведения испытания ИСПНКИ в формате ДД.ММ.ГГГГ>

Б.1.7 Материально-техническое обеспечение испытания ИСПНКИ

<Перечень технических средств стенда, используемых во время испытаний>

Б.1.8 Методическое обеспечение испытания ИСПНКИ

Испытание ИСПНКИ проходит в соответствии с утвержденной программой и методикой <обозначение программы и методики>

Б.1.9 Условия проведения испытания ИСПНКИ

Испытание ИСПНКИ проводят в нормальных климатических условиях. В соответствии с ГОСТ 15150, за нормальные значения климатических факторов внешней среды при испытаниях изделий (нормальные климатические условия испытаний) принимают следующие:
- температура — плюс 25 ± 10 °С;
- относительная влажность воздуха — 45—80 %;
- атмосферное давление 84,0—106,7 кПа (630—800 мм. рт. ст.).

Б.2 Методы испытания

Испытание ИСПНКИ проводят в режиме <отложенного задания/реального времени>.

Б.3 Сбор данных

В процессе проведения испытания осуществляют сбор выходных данных ИСПНКИ.

Б.4 Анализ данных

На основе результатов классификации и числа предъявлений с фактом несанкционированного копирования информации вычисляют значения ВКсФН и ВОсФН.

На основе результатов классификации и числа предъявлений без факта несанкционированного копирования информации вычисляют значения ВКбФН и ВОбФН.

На основе значений ВКсФН и ВОсФН вычисляют значение ОВКсФН.

На основе значений ВКбФН и ВОбФН вычисляют значение ОВКбФН.

На основе значений длительности обработки ИСПНКИ всех предъявлений с фактом несанкционированного копирования информации и числа предъявлений с фактом несанкционированного копирования информации вычисляют значение ДОсФН.

На основе значений длительности обработки ИСПНКИ всех предъявлений без факта несанкционированного копирования информации и числа предъявлений без факта несанкционированного копирования информации вычисляют значение ДОбФН.

На основе значений времени отправки первого предъявления/первого пакета с предъявлениями на проверку, времени получения ответа от ИСПНКИ по последнему обработанному предъявлению и числа поданных предъявлений вычисляют значение ССОЗ.

На основе значений ОВКсФН/ВКсФН и ОВКбФН/ВКбФН строят кривую КОО, график рабочей характеристики и вычисляют значение РВО (обобщенная)/РВО.

Б.5 Хранение данных

Данные, полученные в результате испытания, представлены в настоящем протоколе и приложении к протоколу. Приложение к протоколу размещено на [<лазерном компьютерном диске>; <USB флеш-накопителе>].

В приложении представлены все выходные данные ИСПНКИ, являющейся объектом испытаний, в файле формата .csv.

Б.6 Результаты испытания ИСПНКИ

Результатами испытания ИСПНКИ являются:

- значение ВКсФН;
- значение ВКбФН;
- значение ВОсФН;
- значение ВОбФН;
- значение ОВОсФН;
- значение ОВОбФН;
- значение ДОсФН;
- значение ДОбФН;
- значение ССОЗ;
- РВО;
- РВО (обобщенная).

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, методология проведения испытаний

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

gost.e-ecolog.ru