ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52633.6— 2012

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к индикации близости предъявленных биометрических данных образу «Свой»

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «Пензенский научно-исследовательский электротехнический институт» (ФГУП «ПНИЭИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 сентября 2012 г. № 294-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

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 Обозначения и сокращения 4
5 Общие положения и задачи индикации 4
5.1 Классы индикаторов и их назначение 4
5.2 Размещение индикаторов в схеме преобразования биометрия-код 5
5.3 Значения, возвращаемые индикаторами 6
6 Жесткие индикаторы, использующие хэш-функцию 8
7 Мягкие индикаторы 9
7.1 Индикатор, перебирающий пространство близких значений выходного кода 9
7.2 Индикатор, использующий коды с обнаружением ошибок 9
7.3 Индикатор, оценивающий качество входных биометрических параметров 10
7.4 Индикатор, наблюдающий стабильность разрядов выходного кода 11
7.5 Индикатор, накапливающий промежуточную статистику попыток аутентификации 13
Приложение А (обязательное) Таблица допустимых входных и выходных параметров индикаторов близости к образу «Свой» 14
Приложение Б (справочное) Примеры распределений показателей стабильности и соответствующих им мер Хэмминга 15
Приложение В (справочное) Пример зависимости значения индикатора от расстояния между распределениями показателей стабильности 16
Приложение Г (справочное) Пример зависимости значений индикатора от качества входных биометрических параметров 17

Введение

Настоящий стандарт входит в комплекс стандартов, устанавливающих требования к средствам высоконадежной биометрической аутентификации.

Обеспечиваемая средством биометрической аутентификации стойкость к атакам подбора тем выше, чем сложнее используемый биометрический образ «Свой». Сложный биометрический образ «Свой» может быть получен увеличением длины биометрического образа, выбором редкого образа или объединением нескольких простых образов. Усложнение биометрического образа вызывает рост числа ложных отказов во время процедуры аутентификации и увеличивает ее продолжительность. Для снижения трудоемкости ввода сложного (составного) биометрического образа желательно повторять ввод только тех его фрагментов, в которых имеются ошибки.

Для обнаружения ошибок во вводимых биометрических образах средства высоконадежной биометрической аутентификации должны быть дополнены индикаторами близости биометрического образа к биометрическому образу «Свой». При этом индикаторы не должны существенно компрометировать тайну биометрического образа «Свой».

Настоящий стандарт определяет требования к средствам высоконадежной биометрической аутентификации, имеющим индикаторы близости введенного биометрического образа к образу «Свой», которые, с одной стороны, помогают участнику процесса аутентификации получать информацию о своих ошибках в процессе ввода биометрических данных, а с другой стороны, не дают достаточной информации для упрощения атаки случайного подбора.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к индикации близости предъявленных биометрических данных образу «Свой»

Information protection. Information protection technology. Requirements for fixing compliance between the captured biometric image and the «Owner» biometric image

Дата введения — 2012—12—01

1 Область применения

Настоящий стандарт распространяется на программные и аппаратно-программные средства высоконадежной биометрической аутентификации, выполненные по требованиям ГОСТ Р 52633.0 и дополненные индикаторами близости предъявленных биометрических данных образу «Свой».

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ Р 50779.10 (ИСО 3534-1—93) Статистические методы. Вероятность и основы статистики. Термины и определения

ГОСТ Р 52633.0 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

ГОСТ Р 52633.2 Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

ГОСТ Р 52633.3 Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора

ГОСТ Р 52633.4 Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа

ГОСТ Р 52633.5—2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа

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

автоматическое обучение: Обучение, осуществляемое автоматически без вмешательства человека и осмысления им промежуточных результатов обучения.

[ГОСТ Р 52633.0—2006, пункт 3.1]

3.2

атака случайного подбора: Атака, состоящая в подстановке случайных биометрических образов на вход преобразователя «биометрия-код», либо случайный подбор личного ключа (пароля), образующегося на выходах преобразователя.

[ГОСТ Р 52633.0—2006, пункт 3.3]

3.3

биометрический образ «Свой»: Биометрический образ легального пользователя.

[ГОСТ Р 52633.0—2006, пункт 3.8]

3.4

биометрический образ «Чужой»: Биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту.

[ГОСТ Р 52633.0—2006, пункт 3.9]

3.5 **биометрические образы «Все чужие»:** Совокупность множества биометрических образов «Чужой», верно отражающая статистику попыток подбора злоумышленниками образов «Свой».

3.6

преобразователь «биометрия-код»: Преобразователь, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код ключа (пароля). Преобразователь, откликающийся случайным выходным кодом на воздействие случайного входного вектора, не принадлежащего множеству образов «Свой».

[ГОСТ Р 52633.0—2006, пункт 3.18]

3.7

нейросетевой преобразователь «биометрия-код»: Заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «Свой» в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код.

[ГОСТ Р 52633.0—2006, пункт 3.17]

3.8

донор биометрических образов: Лицо, добровольно участвующее в формировании базы естественных биометрических образов путем предоставления своих собственных биометрических образов для преобразования их в цифровую форму.

[ГОСТ Р 52633.1—2009, пункт 3.1]

3.9

злоумышленник: Лицо, заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, представляющей промышленную и коммерческую тайну, предпринимающее попытку такого доступа или совершившее его.

[ГОСТ Р 52633.1—2009, пункт 3.2]

3.10

стойкость к атакам подбора: Показатель, определяющий число попыток подбора, необходимое злоумышленнику для получения на выходе преобразователя неизвестного ему кода доступа «Свой» при использовании для атаки заранее сформированной базы биометрических образов «Чужой».

[ГОСТ Р 52633.3—2011, пункт 3.1]

3.11

выходной код: Код, получаемый на выходе нейросетевого преобразователя биометрия-код в качестве результата.

[ГОСТ Р 52633.4—2011, пункт 3.14]

3.12

вектор биометрических параметров; ВБП: Нумерованный набор биометрических параметров или производных от них параметров, имеющих одну и ту же интерпретацию и формат представления.

[ГОСТ Р 52633.4—2011, пункт 3.13]

3.13

нейрон: Сумматор нескольких биометрических параметров, на выходе которого подключена нелинейная пороговая функция с двумя выходными состояниями «0» и «1».

[ГОСТ Р 52633.5—2011, пункт 3.23]

3.14

нейронная сеть: Множество нейронов, объединенных в сеть путем соединения входов нейронов одного слоя с выходами нейронов другого слоя, причем входы нейронов первого слоя являются входами всей нейронной сети, а выходы нейронов последнего слоя являются выходами нейронной сети.

Примечание — Настоящий стандарт в преобразователях биометрия-код рекомендует использовать однослойные или двухслойные нейронные сети. Нейронные сети с большим числом слоев в данном стандарте не рассматриваются.

[ГОСТ Р 52633.5—2011, пункт 3.24]

3.15

показатель стабильности разряда выходного кода: Показатель, изменяющийся в пределах от 0,0 (разряд абсолютно нестабилен) до 1,0 (разряд полностью стабилен), вычисляемый по следующей формуле

$$\omega_i = 2|0{,}5 - P_{0,i}| = 2 \cdot |0{,}5 - P_{1,i}|,$$

где $P_{0,i}$ — вероятность появления состояния «0» в контролируемом i-м разряде;

$P_{1,i}$ — вероятность появления состояния «1» в контролируемом i-м разряде.

Примечание — Для образов «Свой» разряды выходного кода обычно стабильны, то есть для них выполняется условие $0{,}5 \le \omega_i \le 1{,}0$, а для образов «Чужой» большинство разрядов выходного кода нестабильны, то есть для них выполняется условие $0{,}0 \le \omega_i \le 0{,}5$.

[ГОСТ Р 52633.5—2011, пункт 3.25]

3.16

обучение нейрона: Операция по вычислению либо подбору весовых коэффициентов нейрона, обеспечивающая высокую вероятность заранее заданного выходного состояния нейрона («0» или «1») при воздействии на него примерами образа «Свой» и равновероятные выходные состояния («0» и «1») при воздействии на нейрон примерами случайных образов «Чужой».

[ГОСТ Р 52633.5—2011, пункт 3.26]

3.17 **жесткий индикатор:** Преобразователь выходного кода, определяющий с заданной вероятностью факт совпадения введенного биометрического образа с биометрическим образом «Свой», по возвращаемым значениям и хранимым данным которого нельзя значительно упростить атаку случайного подбора.

3.18 **мягкий индикатор:** Преобразователь биометрических параметров и выходного кода, выполняющий количественную оценку близости введенного биометрического образа эталонному биометрическому образу «Свой», по возвращаемым значениям которого нельзя значительно упростить атаку случайного подбора.

3.19 **защищенный мягкий индикатор:** Мягкий индикатор, по хранимым данным которого нельзя значительно упростить атаку случайного подбора.

3.20 **значение индикатора:** Значение, возвращаемое жестким и мягким индикаторами.

3.21 **порог обнаружения ошибок:** Максимальное число ошибок, которое может быть обнаружено индикатором в выходном коде (биометрическом образе) и возвращено в качестве значения индикатора.

3.22 **порог индикации ошибок:** Максимальное значение индикатора, достоверно отображающее число обнаруженных в выходном коде (биометрическом образе) ошибок.

4 Обозначения и сокращения

В настоящем стандарте использованы следующие обозначения и сокращения:

$\sigma(.)$ — оператор вычисления стандартного отклонения (по ГОСТ Р 50779.10);

ω_i — показатель стабильности i-го разряда выходного кода;

ψ — стандартное отклонение генератора шума, используемого мягким индикатором;

P_1 — вероятность ошибки первого рода (ошибочное отображение индикатором образа «Свой» как образа «Чужой»);

P_2 — вероятность ошибки второго рода (ошибочное отображение индикатором образа «Чужой» как образа «Свой»);

N — число разрядов выходного кода;

D — порог обнаружения ошибок;

H — значение меры Хэмминга сравниваемых выходных кодов;

E — число обнаруженных ошибок в выходном коде;

ПБК — преобразователь биометрия-код;

ВБП — вектор биометрических параметров;

ИНС — искусственная нейронная сеть;

ЖИ — жесткий индикатор;

МИ — мягкий индикатор;

ЭП — элементарный преобразователь.

5 Общие положения и задачи индикации

5.1 Классы индикаторов и их назначение

5.1.1 Задачи индикаторов близости (далее — индикатор) предъявленных биометрических данных образу «Свой»:

а) определение соответствия вводимого биометрического образа образу «Свой»;

б) определение принадлежности биометрического образа к множеству биометрических образов «Все чужие»;

в) определение близости биометрического образа к образу «Свой»;

г) сравнение примеров разных биометрических образов и их ранжирование на основе оценки близости образов к соответствующим образам «Свой».

5.1.2 Индикаторы близости к образу «Свой» делятся на 2 класса: жесткие индикаторы и мягкие индикаторы.

5.1.3 Жесткие индикаторы должны выполнять задачи перечислений а), б) 5.1.1 вне зависимости от формата представления выходного кода и наличия эффекта размножения ошибок в нем. Функция значений жесткого индикатора должна иметь вид согласно 5.3.1.

5.1.4 Мягкие индикаторы должны выполнять задачи перечислений а), в), г) 5.1.1 с учетом наложенных во время их настройки ограничений. Функция значений мягкого индикатора должна иметь вид согласно 5.3.2—5.3.6.

5.1.5 В зависимости от характеристик хранимой информации мягкие индикаторы подразделяются на незащищенные и защищенные. Информация, хранимая защищенными индикаторами, не должна приводить к компрометации большего числа разрядов выходного кода, чем значение порога индикации ошибок. К незащищенным индикаторам требования по хранению не предъявляются.

Примечание — Для использования защищенного мягкого индикатора перед обучением ПБК в схеме преобразования для ЭП типа МИ устанавливают флаг защищенного ЭП согласно ГОСТ Р 52633.4.

5.1.6 В зависимости от максимального числа обнаруживаемых ошибок в выходном коде или входных биометрических параметрах мягкие индикаторы подразделяются на индикаторы:

- с низким порогом индикации ошибок, способные обнаруживать и отображать до 2 % ошибок в выходном коде;
- со средним порогом индикации ошибок, способные обнаруживать и отображать до 15 % ошибок в выходном коде;
- с высоким порогом индикации ошибок, способные обнаруживать и отображать более 15 % ошибок в выходном коде.

Примечание 1 — Приведенное деление МИ справедливо для выходных кодов длиной 256 бит. При уменьшении длины выходного кода значение порога индикации ошибок тех же индикаторов в процентном отношении может увеличиваться, а при увеличении длины, наоборот, уменьшаться.

Примечание 2 — Переход к МИ с большим значением порога индикации ошибок в большинстве случаев приводит к снижению чувствительности индикатора.

5.2 Размещение индикаторов в схеме преобразования биометрия-код

5.2.1 Индикаторы реализуются разработчиками преобразователя биометрия-код и функционируют совместно с ПБК в единой доверенной вычислительной среде, ограничивающей доступ злоумышленника к данным и программам.

Примечание — Доступ к функциям индикаторов осуществляется через программный интерфейс, выполненный по ГОСТ Р 52633.4.

5.2.2 Жесткий индикатор размещают в схеме преобразования так, чтобы входным параметром для него был выходной (промежуточный) код, имеющий единственное допустимое значение для биометрического образа «Свой», как показано на рисунке 1а. Жесткий индикатор выполняют в соответствии с требованиями раздела 6.

5.2.3 Мягкий индикатор допускается размещать в схеме преобразования двумя способами: для обработки выходного (промежуточного) кода согласно рисунку 1а, для обработки входных биометрических параметров с использованием выходного (промежуточного) кода согласно рисунку 1б.

Примечание — Вариант размещения МИ, использующего только входные биометрические параметры, в настоящем стандарте не рассматривается.

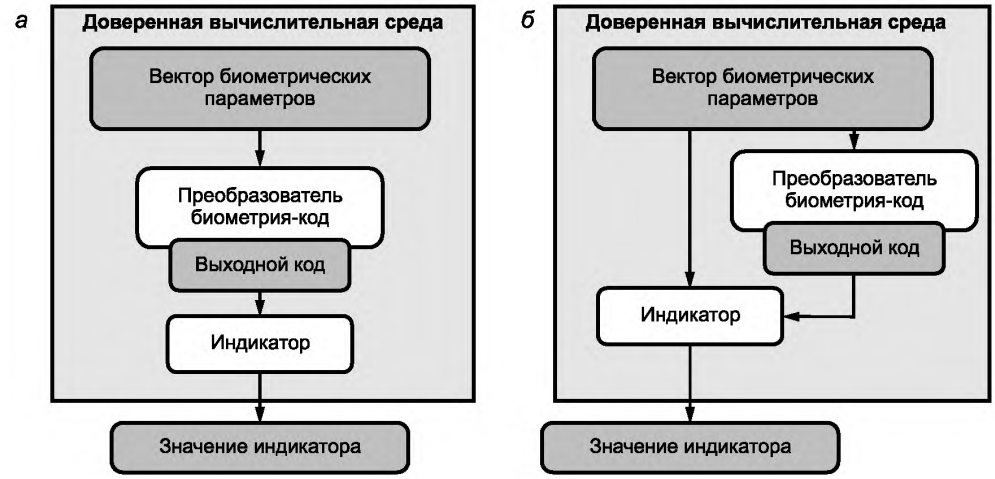

Рисунок 1 — Варианты размещения индикаторов близости:

а — использование выходного кода; *б* — использование биометрических параметров и выходного кода

5.2.4 При построении мягкого индикатора для обработки выходного кода используют варианты МИ, реализуемые согласно 7.1, 7.4 или 7.5.

5.2.5 При построении мягкого индикатора для обработки вектора биометрических параметров с использованием выходного кода применяют варианты МИ, реализуемые согласно 7.2, 7.3.

5.2.6 При наличии эффектов размножения ошибок в выходном коде используют варианты МИ, реализуемые согласно 7.3 или 7.5.

5.2.7 При построении защищенных МИ используют варианты МИ, реализуемые согласно 7.1, 7.2 или 7.5.

5.2.8 Включение индикаторов в схему преобразования и установку их параметров выполняют с учетом таблицы допустимых входных и выходных параметров индикаторов близости к образу «Свой», приведенной в приложении А.

5.2.9 Вариант реализации МИ выбирается разработчиком ПБК с учетом определенных для МИ входных и выходных параметров, его положения в схеме преобразования, порога индикации ошибок, наличия эффектов размножения ошибок в выходном коде и требования использовать защищенный МИ.

5.3 Значения, возвращаемые индикаторами

5.3.1 Значение жесткого индикатора устанавливается в 0, если выходной код совпадает с выходным кодом «Свой». В противном случае значение индикатора устанавливается в *N*, как показано на рисунке 2.

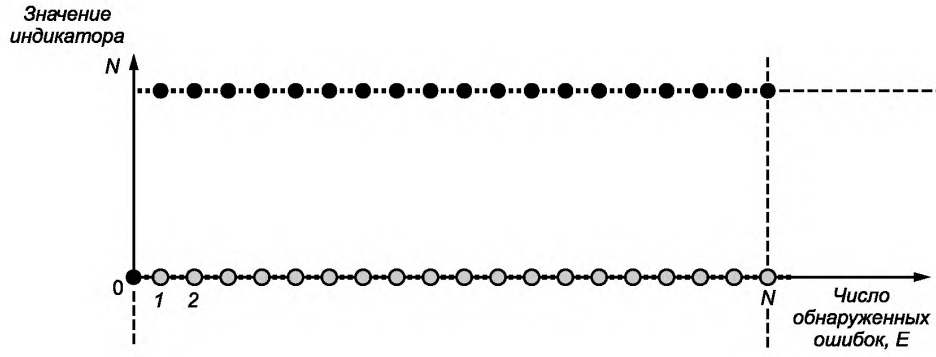

Рисунок 2 — Функция значений жесткого индикатора

5.3.2 Значение мягкого индикатора формируется с помощью двух функций, определенных, соответственно, для числа обнаруженных ошибок в интервале [0, *D*] и вне его [*D* + 1, *N*], как показано на рисунке 3.

5.3.3 Порог индикации ошибок выбирается разработчиком биометрического приложения и устанавливается им в качестве выходного параметра МИ перед его настройкой. По умолчанию должно использоваться целочисленное значение, эквивалентное 1 % от *N*. Соответствующее ему значение порога обнаружения ошибок *D* рассчитывается разработчиком ПБК.

Примечание — В общем случае значение порога индикации ошибок и порога обнаружения ошибок совпадают.

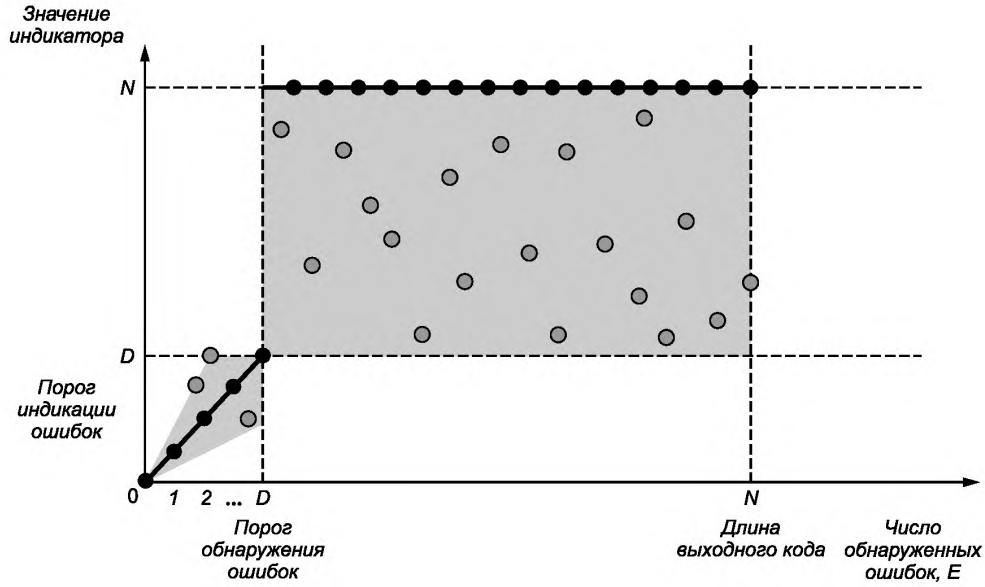

Рисунок 3 — Функция значений мягкого индикатора

5.3.4 В интервале [0, *D*] значение индикатора устанавливается в *E*, где *E* — число обнаруженных ошибок в выходном коде. Допускаются отклонения значений индикатора для части значений входных параметров, но при этом выход значений индикатора за границы [0, *D*] не допускается. При отсутствии ошибок значение индикатора устанавливается в 0.

5.3.5 В интервале [D + 1, N] значение индикатора в общем случае устанавливается в N. При этом допускаются другие значения индикатора из интервала [D + 1, N].

5.3.6 Для защищенных МИ значение D не должно превышать 2 % от N. Значения индикаторов в интервале [D + 1, N] должны устанавливаться в N или быть представимы функцией, имеющей множество точек экстремума, препятствующих использованию мягкого индикатора для упрощения атаки случайного подбора.

5.3.7 Индикаторы с низким и средним порогом обнаружения ошибок должны дополняться ЖИ, если для обучающей выборки биометрических образов «Свой» значения МИ $I_{Свой}$, отличны от 0. Во время использования МИ его значения в интервале от 1 до $\max(I_{Свой})$ должны заменяться на 0, а значение 0 заменяться на 1, если значение ЖИ равно 0 и N соответственно. Число хранимых разрядов ЖИ не должно превышать $\max(I_{Свой})$.

Примечание — Функция $\max(X)$ возвращает максимальное значение из множества X.

6 Жесткие индикаторы, использующие хэш-функцию

6.1 Блок-схема работы жесткого индикатора приведена на рисунке 4. Жесткий индикатор реализуют с помощью хэш-функции, дающей случайные значения на всем множестве значений выходных кодов. Значение хэш-функции, вычисленное для выходного кода, усекают до требуемой величины и сравнивают с эталонным значением, вычисленным заранее. При совпадении значения с эталонным значение индикатора устанавливают в 0, при несовпадении значений — в N.

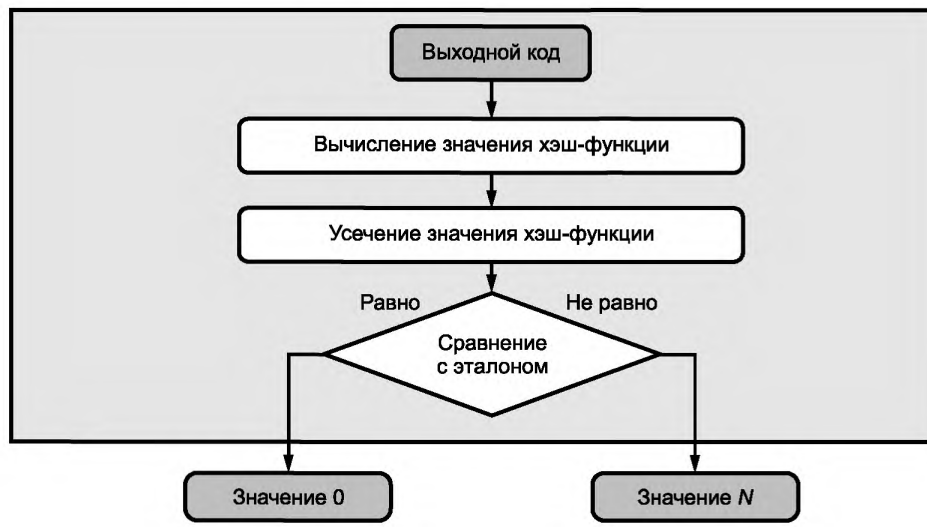

Рисунок 4 — Блок-схема работы жесткого индикатора

6.2 Усеченное значение формируется разработчиком ПБК путем выбора нескольких произвольно расположенных разрядов значения хэш-функции.

6.3 Число выбираемых разрядов определяется разработчиком биометрического приложения путем установки требуемого значения в качестве значения индикатора перед его настройкой. Если число выбираемых разрядов не установлено, должно использоваться значение из интервала от 7 до 10.

Примечание — Использование от 7 до 10 разрядов хэш-функции обеспечивает вероятность ошибок второго рода индикатора на уровне от 2^{-7} до 2^{-10}.

6.4 Эталонное усеченное значение хэш-функции формируют во время настройки мягкого индикатора путем его вычисления для выходного кода «Свой».

6.5 Для последующего использования ЖИ сохраняют только эталонное усеченное значение хэш-функции.

7 Мягкие индикаторы

7.1 Индикатор, перебирающий пространство близких значений выходного кода

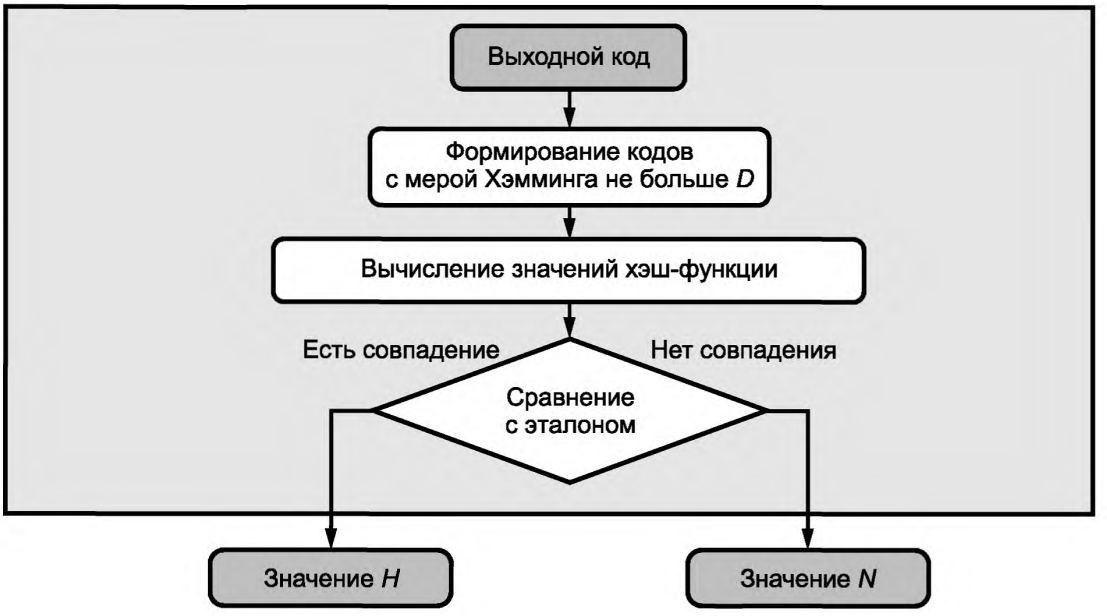

Рисунок 5 — Блок-схема работы мягкого индикатора, перебирающего пространство близких значений выходного кода

7.1.1 Работа мягкого индикатора строится на использовании жесткого индикатора и динамически формируемых кодов, удаленных по мере Хэмминга не более чем на D от выходного кода. Блок-схема работы мягкого индикатора, перебирающего пространство близких значений выходного кода, показана на рисунке 5. Для каждого кода выполняется вычисление усеченного значения хэш-функции и сравнение его с эталонным значением, вычисленным для выходного кода «Свой» во время настройки МИ. При совпадении усеченных значений хэш-функции значение индикатора устанавливается в H, где H — мера Хэмминга соответствующего кода. Если в ходе сравнения усеченное значение хэш-функции ни одного из кодов не совпадает с эталонным значением, значение индикатора устанавливается в N.

Примечание — Описанный вариант МИ требует больших вычислительных мощностей, поэтому его следует применять только для обнаружения небольшого числа ошибок ($D \le 2$).

7.1.2 Для последующего использования МИ сохраняют только эталонное усеченное значение хэш-функции и значение D.

7.2 Индикатор, использующий коды с обнаружением ошибок

7.2.1 Блок-схема работы мягкого индикатора, использующего коды с обнаружением ошибок, приведена на рисунке 6. Для выходного кода формируется проверочный код, позволяющий обнаружить до D ошибок в выходном коде. Формируется однослойная ИНС, в качестве входных параметров которой используются входные параметры ПБК, а в качестве выходного параметра используется проверочный код. Обучение ИНС проводится по алгоритму согласно ГОСТ Р 52633.5 для однослойной сети нейронов.

7.2.2 Значение индикатора формируется путем подачи на вход ИНС индикатора входных биометрических параметров и получения на выходе проверочного кода. Проверочный код используется для обнаружения ошибок в выходном коде ПБК с помощью выбранного разработчиком ПБК метода обнару-

жения ошибок. Значение индикатора устанавливается в *E*, где *E* — число обнаруженных ошибок. Если число ошибок превышает *D*, значение индикатора устанавливается в *N*. Если ошибки не обнаружены, значение индикатора устанавливается в 0.

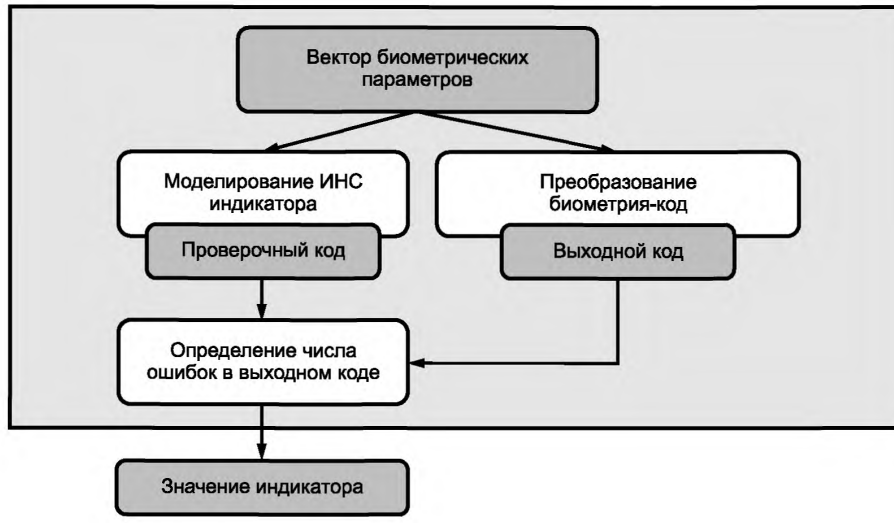

Рисунок 6 — Блок-схема работы мягкого индикатора, использующего коды с обнаружением ошибок

7.2.3 Для последующего использования МИ сохраняют только таблицу весов и связей ИНС индикатора и значение *D*.

7.3 Индикатор, оценивающий качество входных биометрических параметров

7.3.1 Мягкий индикатор, оценивающий качество входных биометрических параметров, для своей работы должен использовать отдельную ИНС индикатора, по индикаторному коду которой устанавливается соответствие между числом ошибок в выходном коде *E* и мерой Хэмминга *H*, вычисленной для индикаторного кода и его эталонного значения. Блок-схема работы мягкого индикатора приведена на рисунке 7.

7.3.2 В качестве входных биометрических параметров ИНС индикатора допускается применять неиспользуемые ПБК биометрические параметры или параметры, имеющие минимальное значение показателя качества биометрического параметра среди входных биометрических параметров ПБК.

7.3.3 Допускается использовать не более 7 % входных биометрических параметров ПБК.

7.3.4 Индикаторный код должен выбираться случайно, независимо от выходного кода. Длина индикаторного кода не должна превышать 7 % от выходного кода.

7.3.5 Обучение ИНС индикатора проводится по алгоритму согласно ГОСТ Р 52633.5 для однослойной сети сумматоров нейронов с номерами 0, ..., *n*. При этом для *i*-го нейрона используют образы с увеличенным в $(1 + 0{,}5i/n)$ раз стандартным отклонением σ по отношению к образу «Свой». Пример обучения ИНС мягкого индикатора приведен в приложении Г.

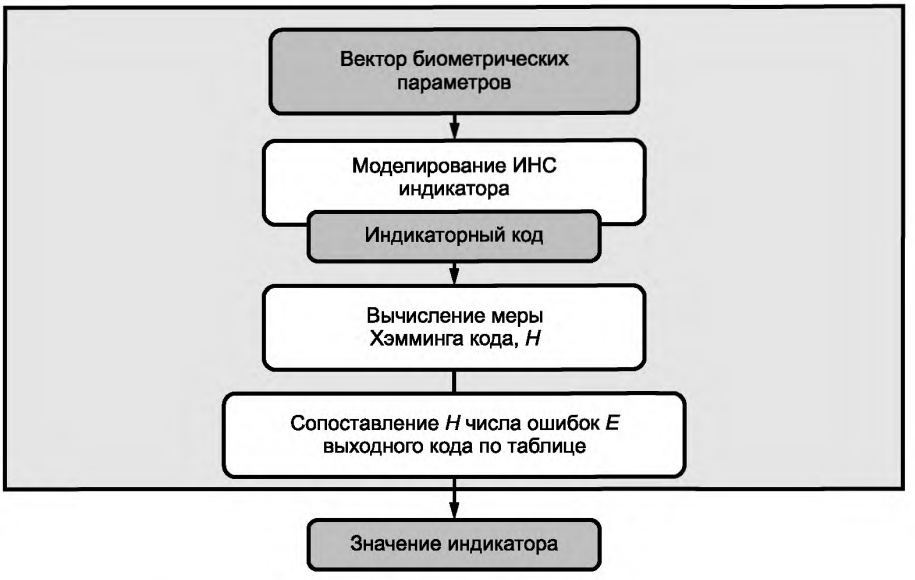

Рисунок 7 — Блок-схема работы мягкого индикатора, оценивающего качество входных биометрических параметров

7.3.6 Для установления соответствия между E и H на вход ИНС индикатора и ПБК подаются примеры образа «Свой» с увеличенным стандартным отклонением в диапазоне $[\sigma, 1{,}5\sigma]$. Для каждого примера вычисляется значение H и соответствующее ему значение E. Число примеров образа «Свой» с увеличенным стандартным отклонением выбирается таким образом, чтобы значению H можно было с высокой вероятностью сопоставить значение E из интервала $[0, D]$. Полученные H и E запоминают.

7.3.7 Значение индикатора формируется путем вычисления значения H для биометрических параметров, поданных на входы ИНС индикатора, и определения соответствующего ему значения E. Значение индикатора устанавливается в E в интервале $[0, D]$ и в N за его пределами. Пример формирования значений индикатора приведен в приложении Г.

7.3.8 Для последующего использования МИ сохраняют только параметры работы ИНС индикатора, эталонное значение индикаторного кода, значения E для H в интервале $[0, D]$.

7.4 Индикатор, наблюдающий стабильность разрядов выходного кода

7.4.1 Блок-схема работы мягкого индикатора, построенного на наблюдении стабильности разрядов выходного кода, приведена на рисунке 8.

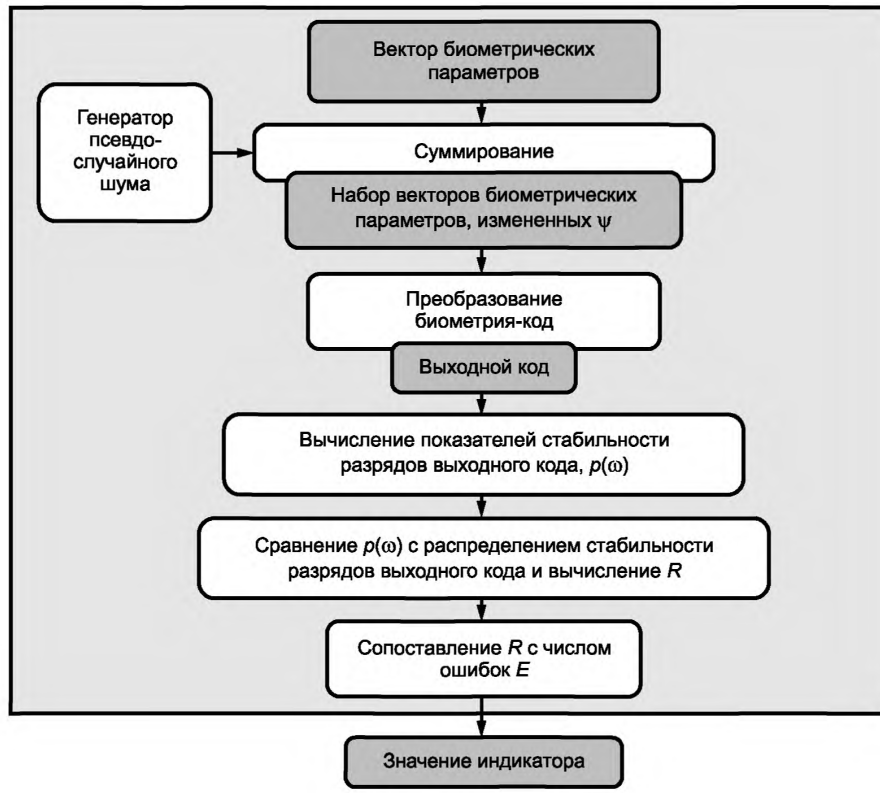

Рисунок 8 — Блок-схема работы мягкого индикатора, наблюдающего распределение показателей стабильности разрядов выходного кода, $p(\omega)$

7.4.2 В мягком индикаторе используется генератор псевдослучайного шума с нулевым математическим ожиданием и стандартным отклонением, равным ψ, которое обеспечивает получение значения показателя стабильности разряда выходного кода $\omega_i < 0{,}95$ для разрядов от 3 % до 10 % выходного кода «Свой». Суммирование независимых значений генератора псевдослучайного шума с каждым биометрическим параметром входного ВБП приводит к формированию набора ВБП, измененных ψ.

7.4.3 Набор ВБП, измененных ψ и полученный из ВБП примеров биометрических образов согласно 7.4.2, используется для вычисления показателей стабильности разрядов выходного кода ω_i. Показатели стабильности разрядов выходного кода ω_i вычисляют по ГОСТ Р 52633.5—2011 (пункт 3.25). Для разрядов, выбираемых во время настройки МИ, строится гистограмма стабильности $p(\omega)$. Примеры гистограмм распределения показателей стабильности приведены в приложении Б.

7.4.4 Во время настройки мягкого индикатора выполняют следующие операции:

а) строят гистограмму $p_{\text{Свой}}(\omega)$ по 7.4.3 для примеров образа «Свой», для построения которой выбирают только разряды с $\omega_i < 0.95$;

б) строят D гистограмм $p_{\text{Чужой}}(\omega)_H$ по 7.4.3 для примеров образов «Чужой», удаленных по мере Хэмминга от «Свой» на $H = 1, 2, \ldots, D$ и сгруппированных по H;

в) для каждой $p_{\text{Чужой}}(\omega)_H$ выполняют расчет значения R_H по формуле:

$$R = \sum_{i=1}^{N} |p_{\text{Чужой}}(\omega_i) - p_{\text{Свой}}(\omega_i)|;$$

г) для каждой из групп примеров образов «Чужой» сохраняют H и соответствующее ему значение R_H, для $H = 0$ сохраняют $R = 0$;

д) сохраняют гистограмму $p_{\text{Свой}}(\omega)$ и значение ψ.

7.4.5 Значение индикатора формируют следующим образом:

а) для предъявленного биометрического образа вычисляют значение $p_{\text{Чужой}}(\omega)$;

б) по гистограмме $p_{\text{Чужой}}(\omega)$ и хранимой гистограмме $p_{\text{Свой}}(\omega)$ вычисляют значение $R_{\text{Чужой}}$ по приведенной выше формуле;

в) находят наиболее близкое к $R_{\text{Чужой}}$ хранимое значение R_H;

г) устанавливают значение индикатора в H, соответствующего R_H, если $R_{\text{Чужой}}$ не больше R_D, и в N — в противном случае.

Пример функции значений индикатора приведен в приложении В.

7.5 Индикатор, накапливающий промежуточную статистику попыток аутентификации

7.5.1 Мягкий индикатор, накапливающий промежуточную статистику попыток аутентификации, реализуется как защищенный или незащищенный мягкий индикатор с высоким порогом индикации ошибок.

7.5.2 Во время работы мягкого индикатора сохраняют в памяти не более D последних вычисленных выходных кодов ПБК V, а также соответствующие им вычисленные по 7.5.3 значения $s_{\max}$.

7.5.3 Значение индикатора формируют следующим образом:

а) выходной код ПБК v, для предъявленного биометрического образа сравнивают со всеми имеющимися выходными кодами V;

б) сравнение v с каждым кодом из V осуществляют путем подсчета числа совпадающих разрядов s_i с первого по N-й (по первый отличающийся, если используется защищенный МИ) в порядке их вычисления в ПБК;

в) среди всех значений s_i находят максимальное значение $s_{\max}$;

г) для незащищенного МИ значение индикатора вычисляют как N минус $s_{\max}$, если $s_{\max} \geq (N - D)$ и N, если $s_{\max} < (N - D)$; для защищенного МИ значение индикатора вычисляют как ближайшее целое от $N/s_{\max}$ и N соответственно;

д) значение $s_{\max}$ сохраняют, а выходной код добавляют к V, если значение $s_{\max}$ не меньше сохраненных ранее значений, соответствующих выходным кодам V, или число выходных кодов V меньше D.

Приложение А
(обязательное)

Таблица допустимых входных и выходных параметров индикаторов близости к образу «Свой»

А.1 В таблице А.1 приведены ограничения числа параметров, их формата и интерпретации для индикаторов близости для различных вариантов из размещения.

Примечание — В таблице А.1 используются сокращения, обозначения и значения типов данных, определенные в ГОСТ Р 52633.4.

Таблица А.1 — Допустимые входные и выходные параметры индикаторов близости к образу «Свой»

Тип ЭП	Тип параметра(ов)	Число параметров	Формат параметра(ов)	Интерпретация параметра(ов)
Жесткий индикатор				
*nb*BT_HARD_INDICATOR	Входной	1	по ГОСТ Р 52633.4	Выходной код
	Специальный входной	0		
	Специальный выходной	0		
	Выходной	1	по ГОСТ Р 52633.4	Значение жесткого индикатора
Мягкий индикатор, использующий выходной код				
*nb*BT_SOFT_INDICATOR	Входной	1	по ГОСТ Р 52633.4	Выходной код
	Специальный входной	0		
	Специальный выходной	0		
	Выходной	1	по ГОСТ Р 52633.4	Значение мягкого индикатора
Мягкий индикатор, использующий биометрические параметры и выходной код				
*nb*BT_SOFT_INDICATOR	Входной	1 + k	по ГОСТ Р 52633.4	1 выходной код и *k* связанных с ним входных ВБП
	Специальный входной	0		
	Специальный выходной	0		
	Выходной	1	по ГОСТ Р 52633.4	Значение мягкого индикатора

Приложение Б
(справочное)

Примеры распределений показателей стабильности и соответствующих им мер Хэмминга

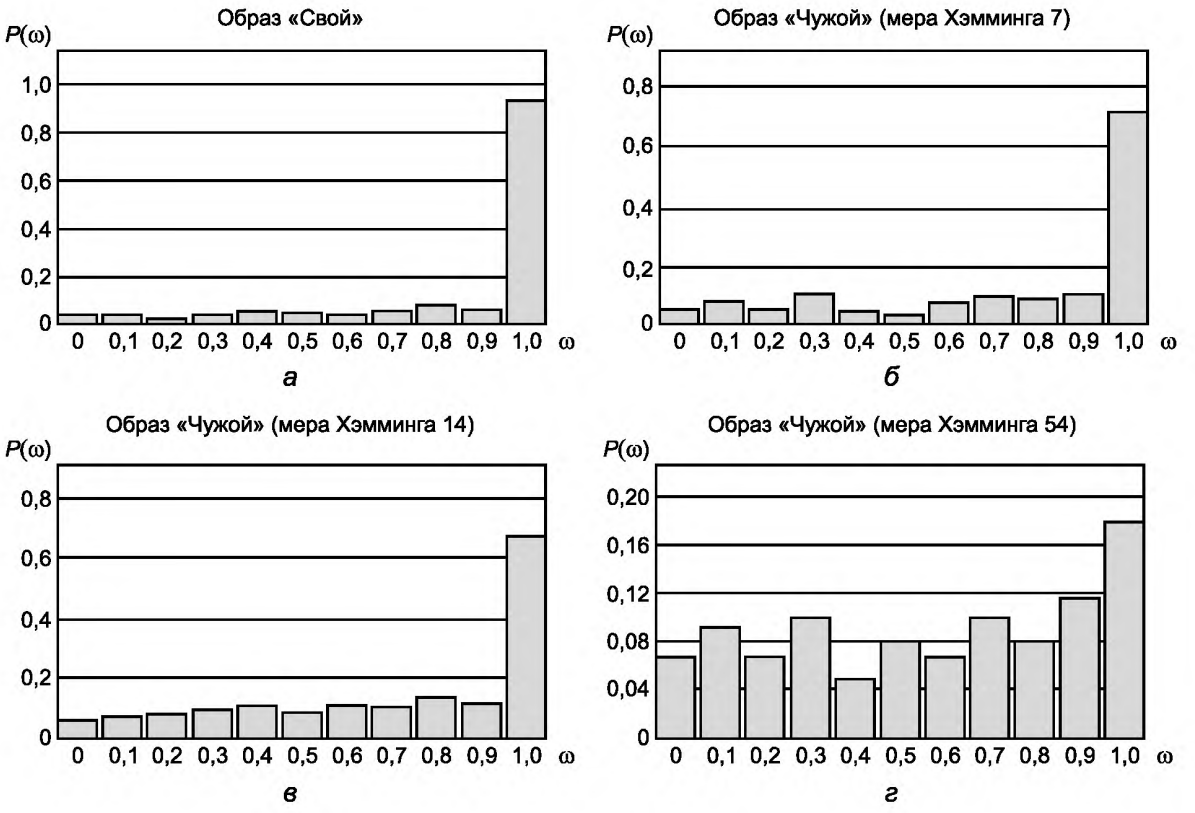

Рисунок Б.1 — Распределения показателей стабильности примеров образа «Свой» и образов «Чужой» для выходного кода длиной 256 разрядов, отличающихся от образа «Свой» по мере Хэмминга:

а — на 0 разрядов, *б* — на 7 разрядов, *в* — на 14 разрядов, *г* — на 54 разряда

Приложение В
(справочное)

Пример зависимости значения индикатора от расстояния между распределениями показателей стабильности

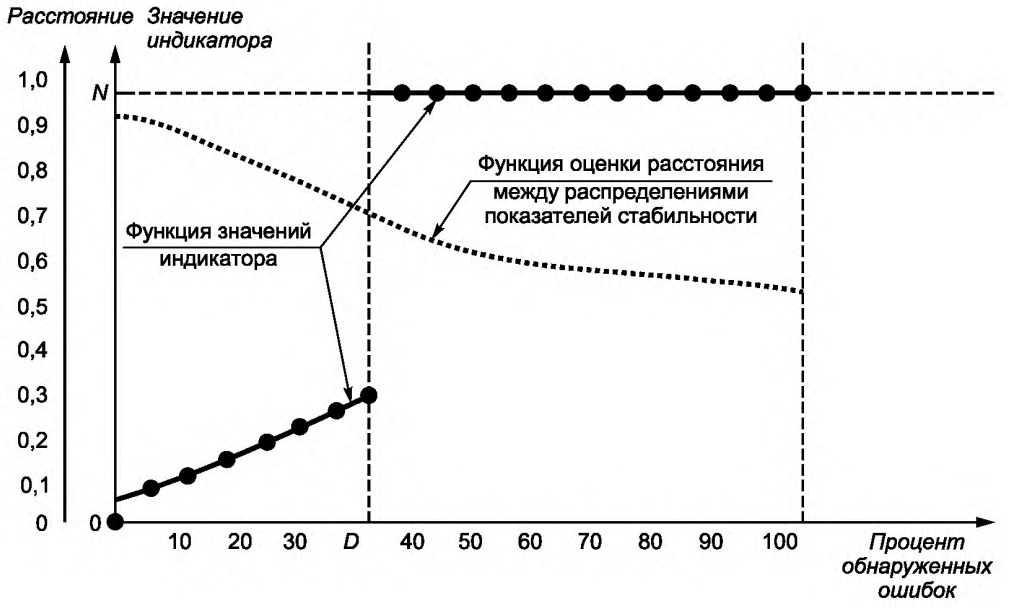

Рисунок В.1 — Пример зависимости значения индикатора от расстояния между распределениями показателей стабильности

Приложение Г
(справочное)

Пример зависимости значений индикатора от качества входных биометрических параметров

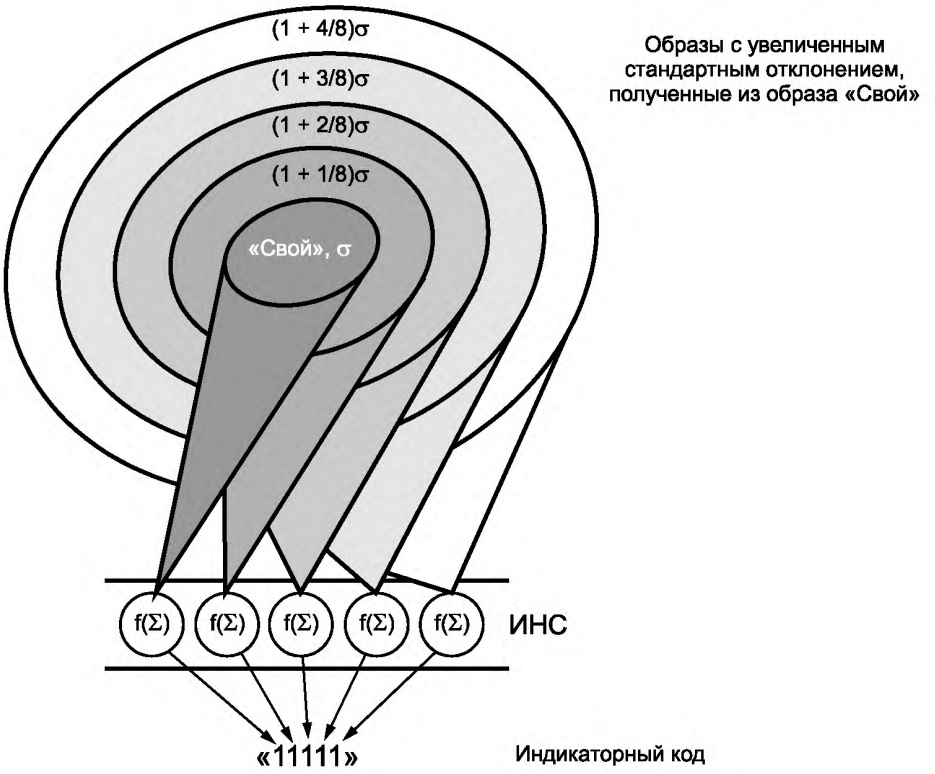

Рисунок Г.1 — Обучение ИНС мягкого индикатора на образах с возрастающим среднеквадратичным отклонением

На рисунке Г.1 показан пример обучения ИНС мягкого индикатора на индикаторном коде «11111». ИНС содержит 5 нейронов. Каждый нейрон обучается на отдельной группе примеров, полученной из исходного образа «Свой» путем пропорционального увеличения отклонений от математического ожидания биометрических параметров.

После обучения ИНС мягкого индикатора строится таблица соответствия значений E выходного кода значениям H индикаторного кода, полученных на одних и тех же группах биометрических образов.

- Тестовые примеры биометрических образов

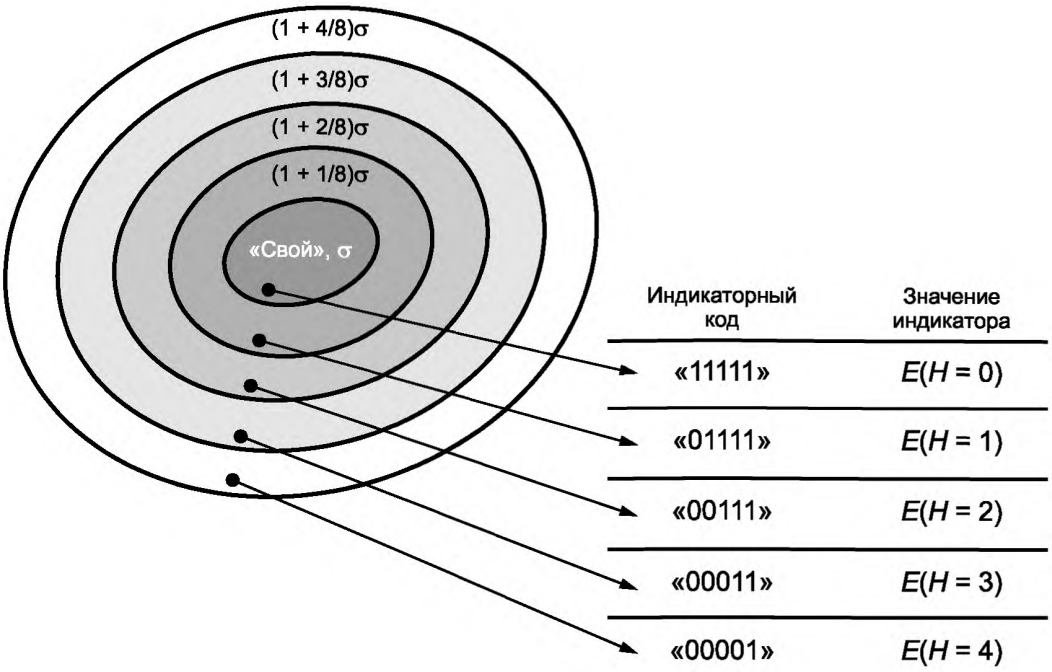

Рисунок Г.2 — Формирование значений индикатора для разных тестовых примеров

На рисунке Г.2 показан пример формирования значений индикатора. Для подаваемого на вход мягкого индикатора биометрического образа с помощью ИНС вычисляется значение индикаторного кода. После этого подсчитывается число разрядов, отличающихся от эталонного значения «11111», *H*. Значение индикатора устанавливается по таблице соответствия *E*(*H*), сформированной во время обучения мягкого индикатора.

УДК 681.18:006.354 ОКС 35.040

Ключевые слова: защита информации, техника защиты информации, порог обнаружения ошибок, порог индикации ошибок, показатель стабильности состояний разрядов биометрического кода, жесткий индикатор, мягкий индикатор

Редактор *Н.В.Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 09.10.2018. Подписано в печать 22.10.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.

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

gost.e-ecolog.ru