ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52633.1— 2009

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

Издание официальное

БЗ 5—2009/178

Москва
Стандартинформ
2010

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «Пензенский научно-исследовательский электротехнический институт» (ФГУП «ПНИЭИ»), Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 839-ст

4 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

Содержание

Введение

Настоящий стандарт входит в комплекс стандартов, устанавливающих требования к разработке и тестированию средств высоконадежной биометрической аутентификации.

Доверие к средствам высоконадежной биометрической аутентификации определяется результатами их тестирования, выраженными в форме гарантий производителя, подтвержденных при необходимости сертификационными документами.

Для тестирования средств биометрической аутентификации необходимы базы биометрических образов «Свой» и «Чужой», размеры которых должны быть достаточными для подтверждения характеристик тестируемых средств.

Необходимые для достоверного тестирования размеры баз биометрических образов «Свой» малы, и формирование таких баз легко осуществимо, а для образов «Чужой» велики (1012 образов и больше). Соответственно процесс создания баз естественных биометрических образов «Чужой» является крайне длительным и трудоемким. Создать базы такого размера в короткие сроки невозможно. В связи с этим при тестировании приходится ограничиваться усеченными базами естественных образов «Чужой» размерами 103—105 образов, непосредственно полученными с тестируемого средства аутентификации. Дополнять такие базы приходится естественными биометрическими образами «Чужой», ранее полученными при тестировании средств аутентификации с аналогичными биометрическими преобразователями. Кроме того, приходится увеличивать размеры тестовой базы за счет применения искусственно синтезированных (синтетических) биометрических образов.

В настоящем стандарте изложены требования по формированию баз естественных биометрических образов. Вопросы пересчета биометрических образов, полученных на одном биометрическом преобразователе, в данные другого биометрического преобразователя в настоящем стандарте не рассматриваются. Также не рассматриваются и вопросы создания баз синтетических биометрических образов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

Information protection. Information protection technology. Requirements for creation procedures for bases of natural biometric images, intended for high-reliability biometric authentication means testing

Дата введения — 2010—01—01

1 Область применения

Настоящий стандарт распространяется на средства формирования баз естественных биометрических образов и на процесс создания таких баз в интересах оценки качества средств высоконадежной биометрической аутентификации при их обучении, тестировании и сертификации на соответствие требованиям ГОСТ Р 52633.0.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ Р 52633.0—2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

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 ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины по ГОСТ Р 52633.0, а также следующие термины с соответствующими определениями:

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

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

3.3 **естественный биометрический образ:** Биометрический образ донора, полученный в виде выходных биометрических данных первичного преобразователя и представленный одним или несколькими примерами.

Издание официальное

3.4 **синтетический биометрический образ:** Биометрический образ, полученный путем имитационного моделирования естественных биометрических образов и представленный одним или несколькими примерами.

3.5 **база естественных биометрических образов «Чужой»:** Совокупность естественных биометрических образов, имитирующих предъявляемые средству аутентификации злоумышленником (злоумышленниками) случайные биометрические образы при реализации атаки подбора.

3.6 **база естественных биометрических образов «Свой»:** Совокупность естественных биометрических образов, состоящая из нескольких примеров одних и тех же биометрических образов, предназначенных для обучения или тестирования средств биометрической аутентификации.

3.7 **показатель стабильности биометрического параметра:** Характеристика *i*-го контролируемого биометрического параметра, вычисляемая по формуле

$$c(\nu_i) = \frac{\sigma_{\text{Чужой}}(\nu_i)}{\sigma_{\text{Свой}}(\nu_i)}, \tag{1}$$

где $\sigma_{\text{Чужой}}(\nu_i)$ — стандартное отклонение *i*-го биометрического параметра множества образов «Чужой»;

$\sigma_{\text{Свой}}(\nu_i)$ — стандартное отклонение *i*-го биометрического параметра множества образов «Свой».

3.8 **показатель средней стабильности параметров биометрического образа:** Характеристика средней стабильности всех параметров биометрического образа, вычисляемая по формуле

$$E(c(\nu)) = \frac{1}{n}\sum_{i=1}^{n} c(\nu_i), \tag{2}$$

где n — число контролируемых параметров биометрического образа.

3.9 **показатель уникальности биометрического параметра:** Характеристика *i*-го биометрического параметра, отражающая отличие контролируемого параметра от среднестатистического значения этого параметра, характерного для всех пользователей, вычисляемая по формуле

$$u(\nu_i) = \frac{|E_{\text{Чужой}}(\nu_i) - E_{\text{Свой}}(\nu_i)|}{\sigma_{\text{Чужой}}(\nu_i)}, \tag{3}$$

где $E_{\text{Чужой}}(\nu_i)$ — математическое ожидание *i*-го биометрического параметра множества биометрических образов «Чужой»;

$E_{\text{Свой}}(\nu_i)$ — математическое ожидание *i*-го биометрического параметра множества биометрических образов «Свой».

3.10 **показатель средней уникальности параметров биометрического образа:** Характеристика средней уникальности всех параметров биометрического образа, вычисляемая по формуле

$$E(u(\nu_i)) = \frac{1}{n}\sum_{i=1}^{n} u(\nu_i). \tag{4}$$

3.11 **показатель качества биометрического параметра:** Характеристика *i*-го биометрического параметра, вычисляемая по формуле

$$q(\nu_i) = \frac{|E_{\text{Чужой}}(\nu_i) - E_{\text{Свой}}(\nu_i)|}{\sigma_{\text{Чужой}}(\nu_i) + \sigma_{\text{Свой}}(\nu_i)}. \tag{5}$$

3.12 **показатель среднего качества параметров биометрического образа:** Характеристика среднего качества всех параметров биометрического образа, вычисляемая по формуле

$$E(q\ (\nu_i)) = \frac{1}{n}\sum_{i=1}^{n} q(\nu_i). \tag{6}$$

3.13 **показатель средней нормированной погрешности отображения математических ожиданий в тестовой базе биометрических образов:** Характеристика качества усеченной тестовой базы биометрических образов, отражающая среднее значение нормированного смещения математических ожиданий контролируемых параметров по отношению к математическим ожиданиям в более полной эталонной базе

$$\Delta E = \frac{1}{n}\sum_{i=1}^{n} \frac{|E_{\text{Тест}}(\nu_i) - E_{\text{Эталон}}(\nu_i)|}{\sigma_{\text{Эталон}}(\nu_i)}, \tag{7}$$

где $E_{\text{Тест}}(\nu_i)$ — математическое ожидание *i*-го параметра в усеченной тестовой базе биометрических образов;

$E_{Эталон}(\nu_i)$ — математическое ожидание i-го параметра в более полной эталонной базе биометрических образов;

$\sigma_{Эталон}(\nu_i)$ — стандартное отклонение i-го параметра в более полной эталонной базе биометрических образов.

3.14 **показатель средней относительной погрешности стандартного отклонения в тестовой базе:** Характеристика качества усеченной тестовой базы биометрических образов, отражающая погрешность воспроизведения стандартных отклонений каждого из контролируемых биометрических параметров

$$\Delta\sigma = \frac{1}{n}\sum_{i=1}^{n}\frac{|\sigma_{Тест}(\nu_i) - \sigma_{Эталон}(\nu_i)|}{\sigma_{Эталон}(\nu_i)}, \tag{8}$$

где $\sigma_{Тест}(\nu_i)$ — стандартное отклонение i-го биометрического параметра в усеченной тестовой базе биометрических образов.

3.15 **показатель средней погрешности отображения плотностей распределения значений биометрических параметров в тестовой базе:** Характеристика качества усеченной тестовой базы биометрических образов, отражающая погрешности воспроизведения ею распределений каждого из контролируемых биометрических параметров

$$\Delta p = \frac{1}{2n}\sum_{i=1}^{n}\int_{\min(\nu_i)}^{\max(\nu_i)}|p_{Эталон}(\nu_i) - p_{Тест}(\nu_i)|d\nu_i, \tag{9}$$

где $p_{Эталон}(\nu_i)$ — плотность распределения значений (нормированная гистограмма) i-го биометрического параметра в более полной эталонной базе биометрических образов;

$p_{Тест}(\nu_i)$ — плотность распределения значений (нормированная гистограмма) i-го биометрического параметра в усеченной тестовой базе биометрических образов.

3.16 **критерий Хемминга:** Мера сравнения двух кодов одинаковой длины, вычисляемая путем подсчета различающихся разрядов сравниваемых кодов.

3.17 **полная база естественных биометрических образов «Чужой»:** Совокупность биометрических образов «Чужой», содержащая достаточное число случайных естественных образов ($N_{Полн}$) для достоверной оценки ожидаемой вероятности ошибки второго рода средства высоконадежной биометрической аутентификации, тестируемого прямым подбором.

3.18 **показатель неполноты базы естественных биометрических образов «Чужой»:** Непрерывная величина, показывающая степень неполноты имеющейся базы из N естественных биометрических образов по сравнению с полной базой из $N_{Полн}$ образов, вычисляемая по формуле

$$\Phi = \frac{\log(N)}{\log(N_{Полн})}. \tag{10}$$

3.19 **усеченная тестовая база естественных биометрических образов «Чужой»:** Фрагмент базы естественных биометрических образов «Чужой», отражающий с некоторыми погрешностями статистические моменты исходной эталонной более полной базы и используемый для последующего тестирования средств высоконадежной биометрической аутентификации.

3.20 **полная база естественных биометрических образов «Свой»:** Совокупность биометрических образов «Свой», содержащая их достаточное число для тестирования, и принадлежащих ко всем классам показателей стабильности, уникальности и качества биометрических параметров.

4 Обозначения

ν — значение биометрического параметра;

$\sigma(\nu)$ — стандартное отклонение биометрического параметра;

$E(\nu)$ — математическое ожидание биометрического параметра;

P_1 — вероятность ошибки первого рода (ошибочное непризнание «Своего»);

P_2 — вероятность ошибки второго рода (ошибочный допуск «Чужого»);

N — число образов в базе естественных биометрических образов;

D — идентификационный номер донора биометрии.

5 Общие положения

5.1 Для повышения качества разрабатываемых средств высоконадежной биометрической аутентификации необходимо проводить их тестирование. Для тестирования средств высоконадежной биометрической аутентификации необходимо сформировать базы биометрических образов, размеры которых должны гарантировать подтверждение заданных характеристик тестируемых средств.

5.2 Для создания базы естественных биометрических образов тестируемых средств высоконадежной биометрической аутентификации используют технологию, показанную на рисунке 1.

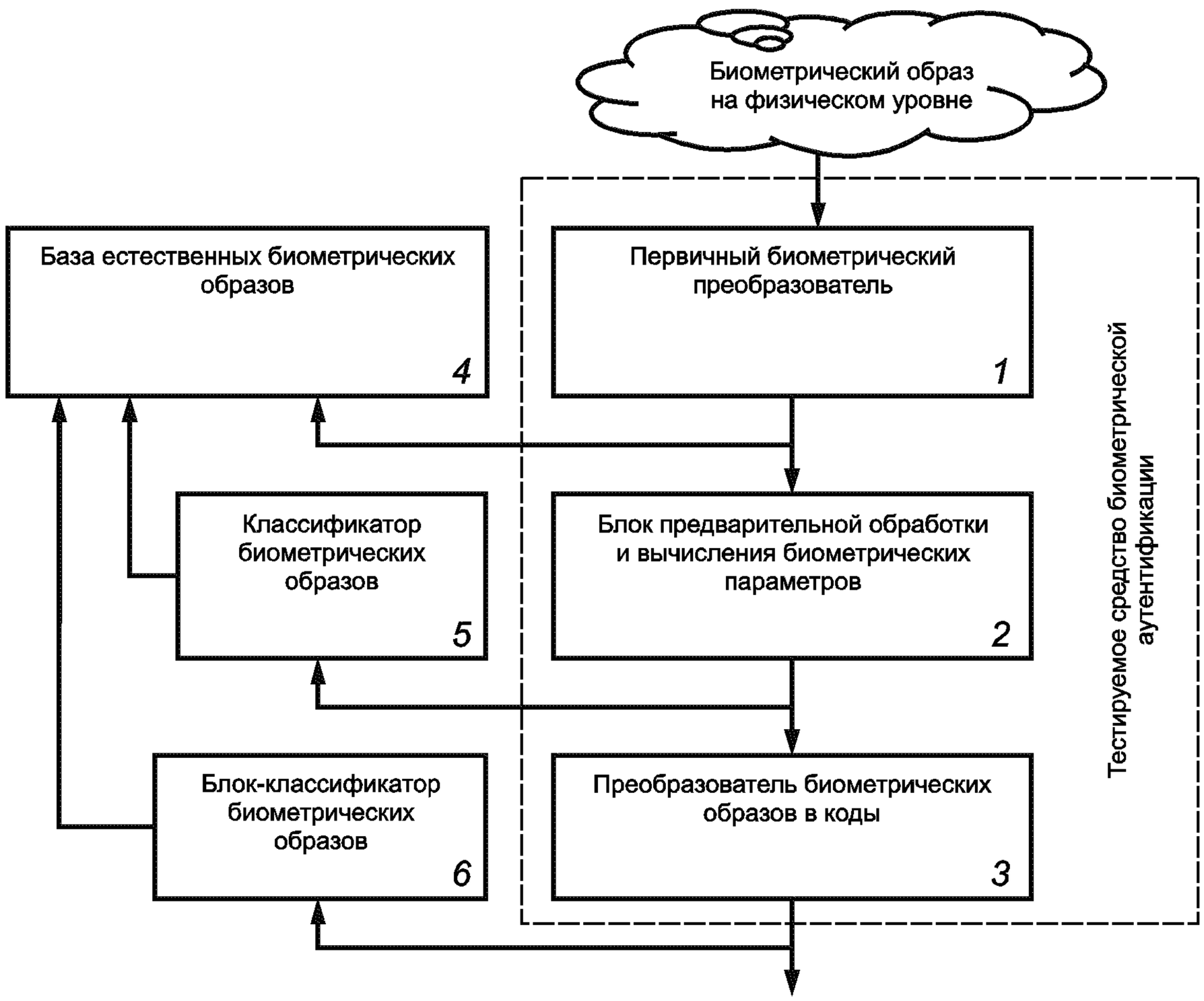

Рисунок 1 — Блок-схема формирования базы естественных биометрических образов тестируемого средства аутентификации и классификации собираемых образов

5.3 На первом этапе формирования базы естественных биометрических образов необходимо биометрический образ (описание биометрических характеристик) человека преобразовать в цифровую форму. Эту процедуру осуществляет первичный биометрический преобразователь *1*.

5.4 На втором этапе цифровой биометрический образ подвергается предварительной обработке в соответствующем блоке *2* (осуществляются его сглаживание, масштабирование, вычисление контролируемых биометрических параметров).

5.5 На третьем этапе вычисленные биометрические параметры биометрического образа преобразуются в код аутентификации преобразователем *3*.

5.6 Естественные биометрические образы размещаются в соответствующей базе *4* после их преобразования в цифровую форму преобразователем *1*. При этом, формируя базу естественных биометрических образов, необходимо сделать предварительный вывод о полноте этой базы и возможности ее использования для последующего тестирования.

5.7 Для классификации естественных биометрических образов параллельно с их сбором осуществляют статистическую обработку по всем биометрическим параметрам. Статистическую обработку

осуществляет блок классификации биометрических образов *5*. Это позволяет уже на этапе сбора естественных биометрических образов классифицировать их по средней стабильности [см. формулу (2)], средней уникальности [см. формулу (4)], среднему качеству [см. формулу (6)] их параметров. В свою очередь, такая классификация позволяет обеспечить полноту формируемой базы тестирования сертифицируемого средства биометрической аутентификации без излишних затрат на сбор неоправданно больших баз биометрических образов.

5.8 Помимо процедур, описанных в 5.7, средством классификации естественных биометрических образов является наблюдение статистик появления различных кодовых состояний на выходе обученного преобразователя *3*.

Классификацию естественных биометрических образов по значению критерия Хемминга осуществляет блок-классификатор *6*.

5.9 Задачей совместной работы классификаторов *5* и *6* является экономия наиболее дорогих ресурсов тестирования — времени и усилий доноров биометрии. Необходимо собрать минимальное (но достаточное) число биометрических образов «Свой» и «Чужой» для достоверного тестирования.

5.10 Так как собрать полную базу естественных биометрических образов «Чужой» практически невозможно, неполная база таких образов должна дополняться ранее собранными образами с аналогичных первичных преобразователей биометрии. Базы естественных биометрических образов одних первичных преобразователей пересчитываются в базы других близких по типу первичных преобразователей. Пересчет образов одного биометрического преобразователя в образы другого биометрического преобразователя не рассматривается в настоящем стандарте.

5.11 Кроме того, базы естественных биометрических образов дополняют искусственно созданными синтетическими биометрическими образами в целях повышения достоверности последующего тестирования. Требования к формированию баз синтетических образов не рассматриваются в настоящем стандарте.

5.12 Для возможности сбора баз естественных биометрических образов и последующего достоверного тестирования проверяемое средство высоконадежной биометрической аутентификации в режиме тестирования должно иметь специальный открытый интерфейс тестирования, позволяющий наблюдать и замещать:

- данные на выходе биометрического преобразователя 1;
- биометрические параметры на выходе блока 2;
- данные на выходе преобразователя 3.

5.13 Для тестирования и подтверждения соответствия (сертификации) средств высоконадежной биометрической аутентификации, выполненных по ГОСТ Р 52633.0, для каждого конкретного первичного биометрического преобразователя создается своя база естественных биометрических образов, обладающая достаточной полнотой. Полная база должна быть способна совместно с базами других близких по типу биометрических преобразователей обеспечивать тестирование всего многообразия средств, использующих конкретный биометрический преобразователь.

Первое тестирование средства с новым первичным биометрическим преобразователем всегда связано с необходимостью создавать для него новую базу его естественных биометрических образов. Формирование такой базы должно обеспечить возможность будущего тестирования и сертификации других средств биометрической аутентификации с аналогичным первичным биометрическим преобразователем.

6 Классификация баз естественных биометрических образов

Базы естественных биометрических образов могут классифицироваться:

- по типу биометрического образа и технологии его преобразования;
- по признаку «Свой» — «Чужой»;
- по области применения.

6.1 Классификация по типу биометрического образа и технологии его преобразования

6.1.1 Классификация по типу биометрического образа

6.1.1.1 Естественные биометрические образы классифицируются по влиянию на них психологических способностей (воли) проверяемого человека. Выделяются статические и динамические биометрические образы. Статические биометрические образы не зависят от психологических способностей проверяемого человека. Динамические биометрические образы легко изменяются в зависимости от психологических способностей проверяемого человека.

6.1.1.2 Средства биометрической аутентификации, выполненные в соответствии с ГОСТ Р 52633.0, являются высоконадежными при использовании ими динамических естественных био-

метрических образов, сохраняемых пользователем в тайне. Возможно усиление таких средств аутентификации статическими естественными биометрическими образами, которые трудно сохранять в тайне и невозможно изменить в случае их компрометации.

6.1.1.3 Естественные статические биометрические образы классифицируются по типу биометрического образа. Выделяются следующие типы статических биометрических образов:

- рисунки кровеносных сосудов глазного дна;
- рисунки радужной оболочки глаза;
- двухмерные и трехмерные отображения геометрии лица;
- отображения геометрии ушных раковин;
- папиллярные рисунки кожи пальцев;
- отображения геометрии складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони;
- рисунки кровеносных сосудов, отображения геометрии складок кожи тыльной стороны ладони;
- отображения геометрических соотношений частей тела.

6.1.1.4 Естественные динамические биометрические образы по типу биометрического образа классифицируются на:

- образы, воспроизведенные рукописным почерком;
- образы динамики клавиатурного почерка;
- образы, воспроизведенные голосом;
- образы характерных движений походки.

6.1.2 Классификация по технологии преобразования биометрического образа

Биометрические образы одного типа могут быть получены преобразователями, построенными на разных физических принципах, имеющих разное поле захвата биометрического образа, разный уровень шумов, разный уровень квантования. Соответственно естественные биометрические образы классифицируются по технологии их преобразования и характеристикам использованного преобразователя.

6.2 Классификация по признаку «Свой» — «Чужой»

6.2.1 Общие положения

Естественные биометрические образы классифицируются по признаку «Свой» — «Чужой». Образы «Свой» отражают статистику распределения биометрических параметров легального пользователя при его попытках аутентификации. Образы «Чужой» отражают статистику распределения биометрических параметров злоумышленников, пытающихся нелегально аутентифицироваться.

6.2.2 Классификация баз биометрических образов «Свой»

6.2.2.1 Базы естественных биометрических образов «Свой» делятся:

- на базы естественных биометрических образов «Свой», предназначенные для обучения (переобучения) средств биометрической аутентификации;
- на базы естественных биометрических образов «Свой», предназначенные для тестирования качества обучения (переобучения) средств биометрической аутентификации.

6.2.2.2 Базы естественных биометрических образов «Свой», предназначенные для обучения и тестирования, взаимозаменяемы, но не тождественны. Все образы в базах обучения и тестирования должны быть различными и получены независимым вводом биометрических данных.

6.2.2.3 Фрагменты естественных биометрических образов базы «Свой» классифицируются по значениям показателя средней стабильности их параметров $E(c(v))$, вычисляемого по формуле (2), показателя средней уникальности их параметров — $E(u(v))$, вычисляемого по формуле (4), и показателя среднего качества их параметров $E(q(v))$, вычисляемого по формуле (6).

6.2.2.4 При классификации по вышеперечисленным признакам динамический диапазон средней стабильности, средней уникальности или среднего качества биометрических параметров образов «Свой» разбивается на классы (поддиапазоны изменения значений) с шириной каждого класса, равной стандартному отклонению наблюдаемого распределения значений для разных образов. Классификация строится таким образом, чтобы минимальное значение средней стабильности, средней уникальности или среднего качества параметров биометрического образа совпадало с левой границей наименее стабильного, уникального или качественного класса биометрических образов. Примеры гистограмм распределения рукописных биометрических образов по классам средней стабильности, средней уникальности и среднего качества воспроизведения их параметров приведены в приложениях А, Б и В.

6.2.3 Классификация баз биометрических образов «Чужой»

6.2.3.1 Классификация баз биометрических образов «Чужой» в соответствии с критерием Хемминга

6.2.3.1.1 Базы статических и динамических естественных биометрических образов «Чужой» фрагментируются и классифицируются по их близости к конкретному образу «Свой» и/или конкретному пре-

образователю биометрия — код, обученному на образе «Свой». В качестве меры близости используют критерий Хемминга. Величину меры близости получают путем вычисления расстояния между кодом образа «Свой» и кодами образов «Чужие».

6.2.3.1.2 Множество естественных биометрических образов «Чужой» по критерию Хемминга делится на классы (поддиапазоны изменения значений) с шириной каждого класса, равной стандартному отклонению наблюдаемого распределения значений меры близости образов «Чужой». Классы естественных биометрических образов «Чужой» располагают таким образом, чтобы центр класса наиболее часто встречающихся кодов совпадал с математическим ожиданием критерия Хемминга.

6.2.3.2 Классификация баз динамических биометрических образов «Чужой» в соответствии со степенью компрометации тайны биометрического образа «Свой»

6.2.3.2.1 Базы динамических естественных биометрических образов «Чужой» в соответствии со степенью компрометации тайны биометрического образа «Свой» делятся:

- на базы динамических естественных биометрических образов «Чужой», сформированные без знания донорами тайной составляющей биометрического образа «Свой» (без знания пароля, без компрометации биометрического образа «Свой»);
- базы динамических естественных биометрических образов «Чужой», сформированные с частичным знанием донорами тайной составляющей биометрического образа «Свой» (знание нескольких символов или звуков биометрического пароля и соответствующая этому частичная компрометация биометрического образа «Свой»). Образы, содержащиеся в таких базах, в свою очередь, классифицируются в соответствии с мерой знания донором образа «Свой» (например, количеством известных букв рукописного пароля);
- базы динамических естественных биометрических образов «Чужой», сформированные донорами с полным знанием тайной составляющей биометрического образа «Свой» (знание всего биометрического пароля с полной компрометацией тайны биометрического образа «Свой»).

6.3 Классификация по области применения

6.3.1 Базы естественных биометрических образов, предназначенные для тестирования качества средств биометрической аутентификации

6.3.1.1 Базы естественных биометрических образов, предназначенные для тестирования качества работы средств биометрической аутентификации, с биометрическими образами «Свой» разных классов показателей стабильности, уникальности и качества формируют лица, уполномоченные проводить подтверждение соответствия (сертификацию) средств аутентификации. Базы для тестирования качества средств биометрической аутентификации имеют значительные размеры и размещаются вне этих средств.

6.3.1.2 Размеры формируемых баз отражают потребности в гарантиях на заявляемые вероятностные показатели надежности средств высоконадежной биометрической аутентификации (вероятности ошибок первого рода P_1 и вероятности ошибок второго рода P_2). Размеры полной базы «Свой», как правило, невелики, и этот тип полной базы может быть сформирован при тестировании конкретного средства аутентификации. Размеры базы «Чужой» для достоверной оценки малых (нано или пико) вероятностей P_2 должны быть велики, полную базу этого типа для тестирования средств высоконадежной биометрии невозможно создать в короткое время. Приходится довольствоваться неполными базами естественных биометрических образов «Чужой», собранными непосредственно с тестируемого средства.

6.3.1.3 При тестировании качества средств биометрической аутентификации допускается использование усеченных тестовых баз естественных биометрических образов «Свой» и «Чужой». При этом рекомендуется производить согласование таких усеченных тестовых баз в соответствии с требованиями, заявленными в разделах 7 и 8.

6.3.2 Базы естественных биометрических образов, предназначенные для тестирования качества очередного обучения средства биометрической аутентификации

6.3.2.1 Базы естественных биометрических образов «Свой», предназначенные для тестирования качества очередного обучения средства биометрической аутентификации, формируются, хранятся, используются и уничтожаются пользователем или доверенной системой в процессе обучения средства биометрической аутентификации. Этот тип баз имеет малые размеры [20 примеров (выборок) — один образ] и размещается внутри средства высоконадежной биометрической аутентификации.

6.3.2.2 Базы естественных биометрических образов «Чужой», предназначенные для тестирования качества очередного обучения средства биометрической аутентификации, формируются производителем средств высоконадежной биометрической аутентификации и поставляются в комплекте со средством биометрической аутентификации, но могут быть дополнены пользователем. Этот тип баз

имеет малые размеры [по 1 примеру (выборке) — 100 образов] и размещается внутри средства высоконадежной биометрической аутентификации. При формировании малой тестовой базы «Чужой» производитель должен производить ее согласование в соответствии с разделами 7 и 8.

7 Требования к формированию баз естественных биометрических образов «Свой»

7.1 Требования к формированию баз естественных биометрических образов «Свой», предназначенных для тестирования средств биометрической аутентификации

7.1.1 Базы естественных биометрических образов «Свой», предназначенные для тестирования средств биометрической аутентификации, должны содержать множество примеров (выборок) различных биометрических образов, принадлежащих разным людям.

7.1.2 Для каждого биометрического образа человека в базе должны быть указаны показатели:

- средней стабильности параметров биометрического образа [см. формулу (2)];
- средней уникальности параметров биометрического образа [см. формулу (4)];
- среднего качества параметров биометрического образа [см. формулу (6)].

7.1.3 Приведенные выше данные относительны и должны быть указаны для всех средств, на которых было произведено тестирование, с указанием даты тестирования, обозначения и полного названия средства и его производителя.

7.1.4 Число примеров того или иного образа «Свой» одного человека должно быть достаточно для обучения и тестирования средства высоконадежной биометрической аутентификации [рекомендуется использовать по 20 и более примеров (выборок) для обучения и столько же для тестирования].

7.1.5 Статистические параметры базы естественных биометрических образов «Свой» документируются лицом, ее сформировавшим, в виде указания принадлежности того или иного биометрического образа к разным классам показателей средней стабильности, уникальности и качества.

7.1.6 При формировании базы естественных биометрических образов «Свой» необходимо обеспечить ее полноту, добиваясь присутствия в ней, как минимум, одного образа «Свой» в каждом из классов показателей средней стабильности, уникальности и качества биометрических параметров образов.

7.1.7 Для усеченных тестовых баз естественных биометрических образов «Свой» необходимо приводить величину средней погрешности математического ожидания показателей [см. формулу (7)] в совокупности с другими аналогичными показателями контроля погрешностей усеченной базы [см. формулы (8) и (9)].

7.2 Требования к формированию естественных биометрических образов «Свой», предназначенных для тестирования качества очередного обучения средства биометрической аутентификации

7.2.1 Базы естественных биометрических образов «Свой», предназначенные для тестирования качества очередного обучения средств биометрической аутентификации, формируются при обучении средства биометрической аутентификации и далее могут быть использованы для переобучения и тестирования средства биометрической аутентификации. Базы формируются путем последовательного предъявления биометрического образа «Свой» заданное производителем количество раз. Рекомендуется дополнять базы примерами (выборками, не участвующими в обучении) для тестирования.

7.2.2 Структура базы задается производителем средства аутентификации.

7.2.3 Хранение базы осуществляется только в защищенном (зашифрованном) виде внутри средства биометрической аутентификации, при доступе к базе обязательны контроль ее целостности и авторизация.

8 Требования к формированию баз естественных биометрических образов «Чужой»

8.1 Формирование баз естественных биометрических образов »Чужой», предназначенных для тестирования средств биометрической аутентификации

8.1.1 Обеспечение представительности баз

8.1.1.1 Базы естественных биометрических образов «Чужой», предназначенные для тестирования средств биометрической аутентификации, должны отражать статистику распределения активного населения в масштабе страны, региона, по возрасту, половому признаку, роду занятий, квалификации и иным характеристикам, присущим людям, для которых создано тестируемое средство высоконадежной биометрической аутентификации.

8.1.1.2 Формирование баз естественных биометрических образов «Чужой» должно осуществляться исходя из десятикратного превышения находящихся в базе случайных образов «Чужой» по отношению к показателю ожидаемой стойкости к атакам подбора тестируемого средства аутентификации. Прогноз стойкости к атакам подбора (обратной величины вероятности ошибки второго рода) должен быть осуществлен внутренними средствами тестирования средства аутентификации. Число биометрических образов полной базы определяют по формуле

$$N_{\text{Полн}} = \frac{10}{P_2}. \qquad (11)$$

8.1.1.3 При отсутствии доверия к внутренним средствам тестирования (либо при отсутствии таких средств) прогноз вероятности ошибок второго рода P_2 вычисляют приближенно исходя из гипотезы нормального закона распределения значений вероятности ошибок по формуле

$$P_2 \approx \frac{1}{\sqrt{2\pi}} \int_{\sqrt{n}E(q(\nu))}^{\infty} \exp\left(-\frac{x^2}{2}\right) dx, \qquad (12)$$

где n — число учитываемых средством аутентификации биометрических параметров;

$E(q(\nu))$ — среднее качество всех учитываемых средством биометрической аутентификации биометрических параметров.

8.1.2 Неполные базы естественных биометрических образов «Чужой»

8.1.2.1 Формирование полной базы естественных биометрических образов «Чужой» для тестирования средств высоконадежной биометрической аутентификации сопряжено, как правило, с огромными затратами времени и иных материальных ресурсов. Неполнота базы приводит к снижению достоверности тестирования, но во многих случаях вполне допускается формировать неполные базы естественных биометрических образов «Чужой».

8.1.2.2 При формировании неполной базы из N биометрических образов «Чужой» показатель неполноты базы определяют по формуле (10).

8.1.2.3 В дальнейшем при тестировании неполные базы необходимо многократно увеличивать за счет дополнения их синтетическими биометрическими образами.

Количество дополняющих синтетических образов определяют по формуле

$$N_{\text{Синт}} \approx N^{1/\phi} - N \quad \text{или} \quad N_{\text{Полн}} \approx N_{\text{Синт}} + N, \qquad (13)$$

где ϕ — показатель неполноты (10);

$N_{\text{Синт}}$ — число синтетических образов, дополняющих неполную базу до полной.

8.1.2.4 Требования к показателю неполноты формируемой базы определяются методами тестирования и синтеза дополняющих базу синтетических биометрических образов. Эти требования не рассматриваются в настоящем стандарте.

8.1.3 Обеспечение случайности образов базы «Чужой»

8.1.3.1 Случайность биометрических образов обеспечивается использованием различных доноров биометрических образов, а также различием вариантов биометрических образов каждого донора.

8.1.3.2 Изменение однотипных биометрических образов в случае использования статической биометрии может быть обеспечено только изменением личности донора. Например, донор биометрии папиллярных рисунков отпечатков пальцев «Чужой» потенциально способен предоставить по одному образу рисунков с каждого из своих пальцев. Разные примеры рисунка одного образа отпечатка пальца не могут быть использованы в одной базе естественных биометрических образов «Чужой» из-за их близости.

8.1.3.3 Изменение биометрических образов в случае использования динамической биометрии может быть обеспечено через изменение донором слова пароля. Возможные размеры базы динамических биометрических образов «Чужой», формируемой одним донором, много больше размеров базы его статических биометрических образов.

8.1.3.4 Формирование базы естественных биометрических образов «Чужой» рукописных паролей осуществляют путем использования разных смысловых или не имеющих смысла паролей, а также путем привлечения к написанию одного пароля нескольких доноров.

8.1.3.5 Формирование базы естественных биометрических образов «Чужой» голосовых паролей осуществляют путем использования разных слов и буквосочетаний, характерных для языка донора.

8.1.3.6 Рекомендуется после формирования базы «Чужой» проверить наличие в ней близких образов, так как в любой из формируемых баз «Чужой» нежелательно присутствие слишком близких друг к другу естественных биометрических образов. При проверке сравнивают между собой выходные коды естественных биометрических образов «Чужой» (блок *6* рисунка 1) на выходе обученного преобра-

зователя биометрия — код (блок 3 рисунка 1) по значению критерия Хемминга. Два образа «Чужой» считаются недопустимо близкими, если отличаются по значению критерия Хемминга менее чем на 3 % для преобразователя с длиной кода 128 бит и более, обученного на одном из сравниваемых кодов. При длине кода менее 128 бит недопустимо близкими считаются образы с расстоянием Хемминга, равным 3 бит и менее.

8.2 Формирование баз естественных биометрических образов »Чужой», предназначенных для тестирования качества очередного обучения средств биометрической аутентификации

8.2.1 Базы естественных биометрических образов «Чужой», предназначенные для тестирования качества очередного обучения средств биометрической аутентификации, формируются производителем средства аутентификации путем выборки биометрических образов из базы естественных биометрических образов, предназначенных для тестирования средств биометрической аутентификации. За достоверность и согласованность базы биометрических образов «Чужой», предназначенной для тестирования качества очередного обучения средств биометрической аутентификации, несет ответственность производитель средства высоконадежной биометрической аутентификации.

8.2.2 В средствах биометрической аутентификации желательно размещать базы биометрических параметров образов «Чужой», в силу того что базы биометрических параметров компактнее баз биометрических образов. Однако производитель обязан хранить и исходную базу образов «Чужой», не сжатую в базу биометрических параметров «Чужой».

8.2.3 Рекомендуется привлекать одного донора одновременно к созданию нескольких типов баз естественных динамических биометрических образов в целях сокращения затрат. Структура совмещения различных баз естественных динамических биометрических образов, формируемых одним донором, а также процесс формирования баз естественных биометрических образов при многократном привлечении одного донора приведены в приложении Г.

8.3 Согласование усеченных тестовых баз естественных биометрических образов «Чужой»

8.3.1 Усеченные тестовые базы естественных биометрических образов «Чужой» формируются путем выборки образов из полной базы естественных биометрических образов «Чужой» для снижения затрат по сопровождению полной базы естественных биометрических образов «Чужой». При этом необходимо, чтобы полученная усеченная тестовая база повторяла полную базу по совокупности характеристик, к которым относятся:

- статистические моменты биометрических параметров (плотность статистического распределения значений, математическое ожидание и стандартное отклонение значения каждого параметра);
- распределение парных корреляций входных параметров.

8.3.2 Для численной оценки согласованности усеченной тестовой базы используют показатели, вычисляемые по формулам (7)—(9), и их аналоги при контроле распределений парных корреляций.

8.3.3 Необходимая представительность усеченной тестовой базы по числу примеров, содержащихся в ней, и прочим характеристикам задается лицом, применяющим базу для тестирования, в соответствии с требуемым уровнем достоверности тестирования и/или показателем неполноты [см. формулу (10)].

8.3.4 Пример расчета статистических величин контроля уровня согласованности усеченных баз рукописных образов, а также гистограммы статистического распределения биометрического параметра v_1 исходной более полной базы, согласованной и несогласованной усеченной тестовой баз приведены в приложении Д.

9 Требования к обеспечению конфиденциальности персональных данных, целостности и достоверности баз естественных биометрических образов

9.1 Для доноров биометрических образов «Свой» и «Чужой», участвующих в создании баз естественных биометрических образов, должны быть обеспечены требования сохранения конфиденциальности их персональных данных.

9.2 Конфиденциальность персональных данных доноров биометрии обеспечивается посредством:

- невозможности определения по биометрическим образам из базы естественных биометрических образов «Чужой» личности доноров биометрии;
- недопустимости хранения в базе естественных биометрических образов любых персональных данных донора биометрии (кроме его идентификационного номера).

9.3 Допускается при формировании баз биометрических образов присваивать донорам идентификационные номера и контролировать доноров биометрии путем нейросетевого связывания их образов «Свой» с их идентификационным номером по ГОСТ Р 52633.0.

9.4 Достоверность баз естественных биометрических образов обеспечивается:

- получением примеров естественных биометрических образов донора только под контролем доверенного лица (лиц);
- при формировании баз естественных динамических биометрических образов — путем задания донору воспроизводимых им слов от генератора случайных паролей;
- при формировании баз естественных статических биометрических образов — путем учета доноров естественных статических биометрических образов, не позволяющего несанкционированно дублировать в базе биометрический образ;
- контролем целостности баз естественных биометрических образов со стороны пользователей и лиц, их формирующих.

9.5 Пример структуры организации базы рукописных образов одного донора приведен в приложении Ж.

Приложение А
(рекомендуемое)

Пример гистограммы распределения рукописных биометрических образов по классам средней стабильности воспроизведения их параметров

При анализе использовано 100 образов «Свой», состоящих из 5 букв (по 20 примеров каждого образа), и 2000 образов «Чужой» по одному примеру. Учитывалось 416 биометрических параметров образов, полученных с графического планшета WizardPen 5 × 4 фирмы Genius.

Для тестируемого средства после усреднения результатов получено:

- математическое ожидание средней стабильности — 3,452;
- стандартное отклонение средней стабильности — 1,517;
- минимальное значение средней стабильности — 0,721;
- максимальное значение средней стабильности — 10,86.

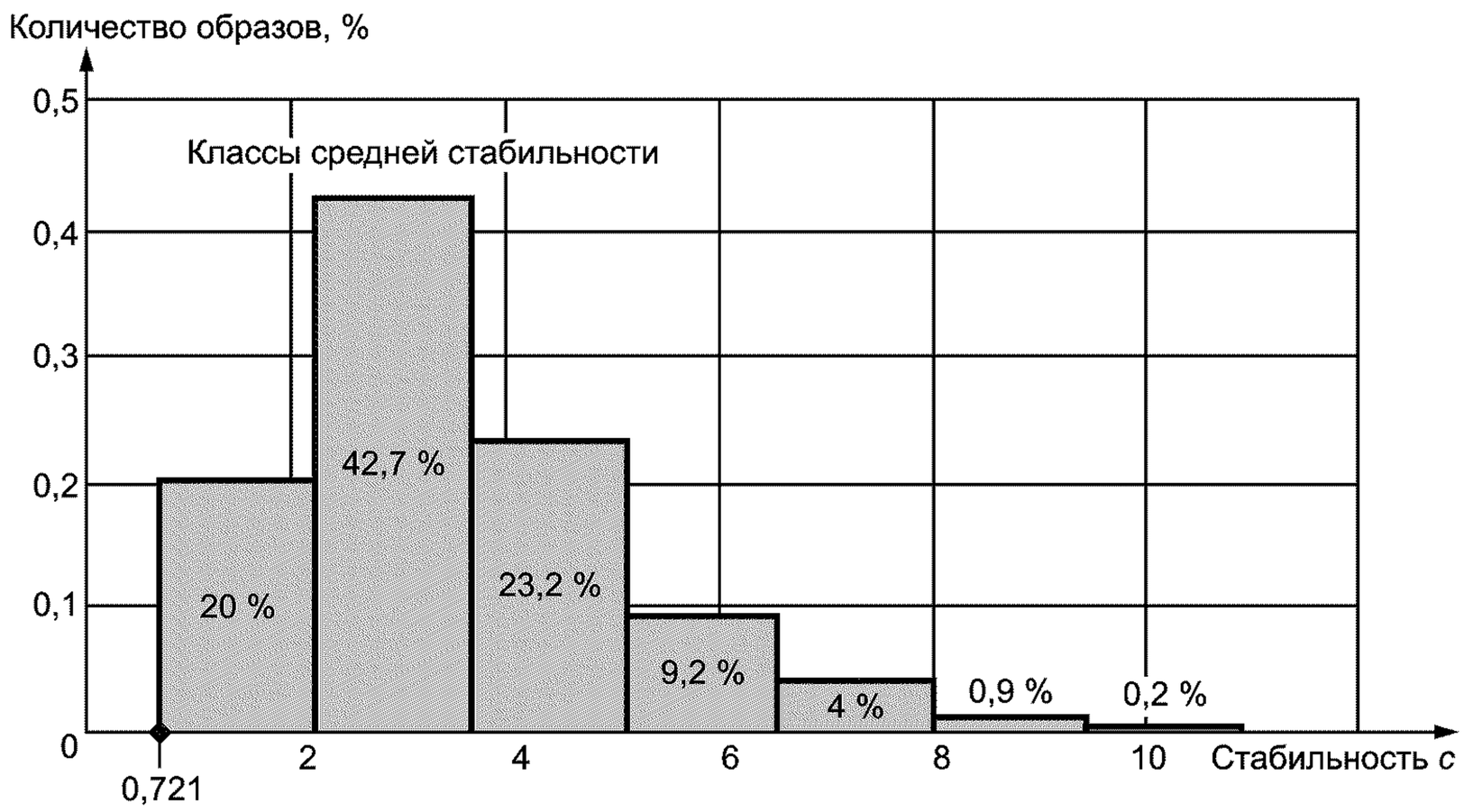

Рисунок А.1 — Процентное распределение биометрических рукописных образов «Свой» по классам средней стабильности

Примечание — Вид статистического распределения рукописных образов «Свой» существенно зависит от длины вектора учитываемых биометрических параметров и способов вычисления этих параметров. Тестируемое средство может отбрасывать наиболее нестабильные биометрические параметры, что приводит к росту асимметрии распределения.

Приложение Б
(рекомендуемое)

Пример гистограммы распределения рукописных биометрических образов по классам средней уникальности воспроизведения их параметров

При анализе использовано 100 образов «Свой», состоящих из 5 букв (по 20 примеров каждого образа), и 2000 образов «Чужой» по одному примеру. Учитывалось 416 биометрических параметров образов, полученных с графического планшета WizardPen 5 × 4 фирмы Genius.

Для тестируемого средства после усреднения результатов получено:

- математическое ожидание средней уникальности — 0,568;
- стандартное отклонение средней уникальности — 0,223;
- минимальное значение средней уникальности — 0,203;
- максимальное значение средней уникальности — 1,926.

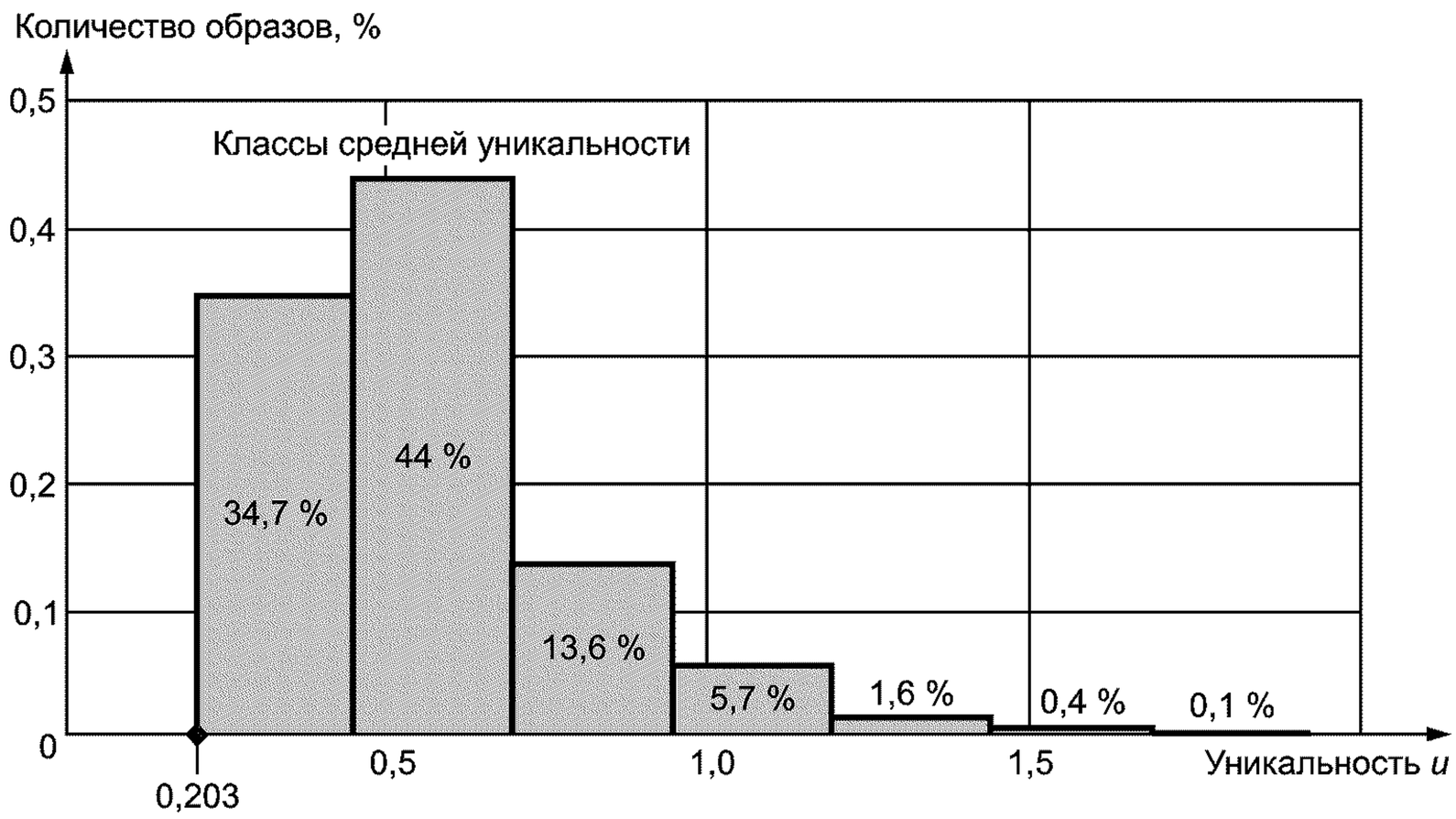

Рисунок Б.1 — Процентное распределение биометрических рукописных образов «Свой» по классам средней уникальности

Приложение В
(рекомендуемое)

Пример гистограммы распределения рукописных биометрических образов по классам среднего качества воспроизведения их параметров

При анализе использовано 100 образов «Свой», состоящих из 5 букв [по 20 примеров (выборок) каждого образа], и 2000 образов «Чужой» по одному примеру (выборке). Учитывалось 416 биометрических параметров образов, полученных с графического планшета WizardPen 5 × 4 фирмы Genius.

Для тестируемого средства после усреднения результатов получено:

- математическое ожидание среднего качества — 0,385;
- стандартное отклонение среднего качества — 0,111;
- минимальное значение среднего качества — 0,151;
- максимальное значение среднего качества — 0,851.

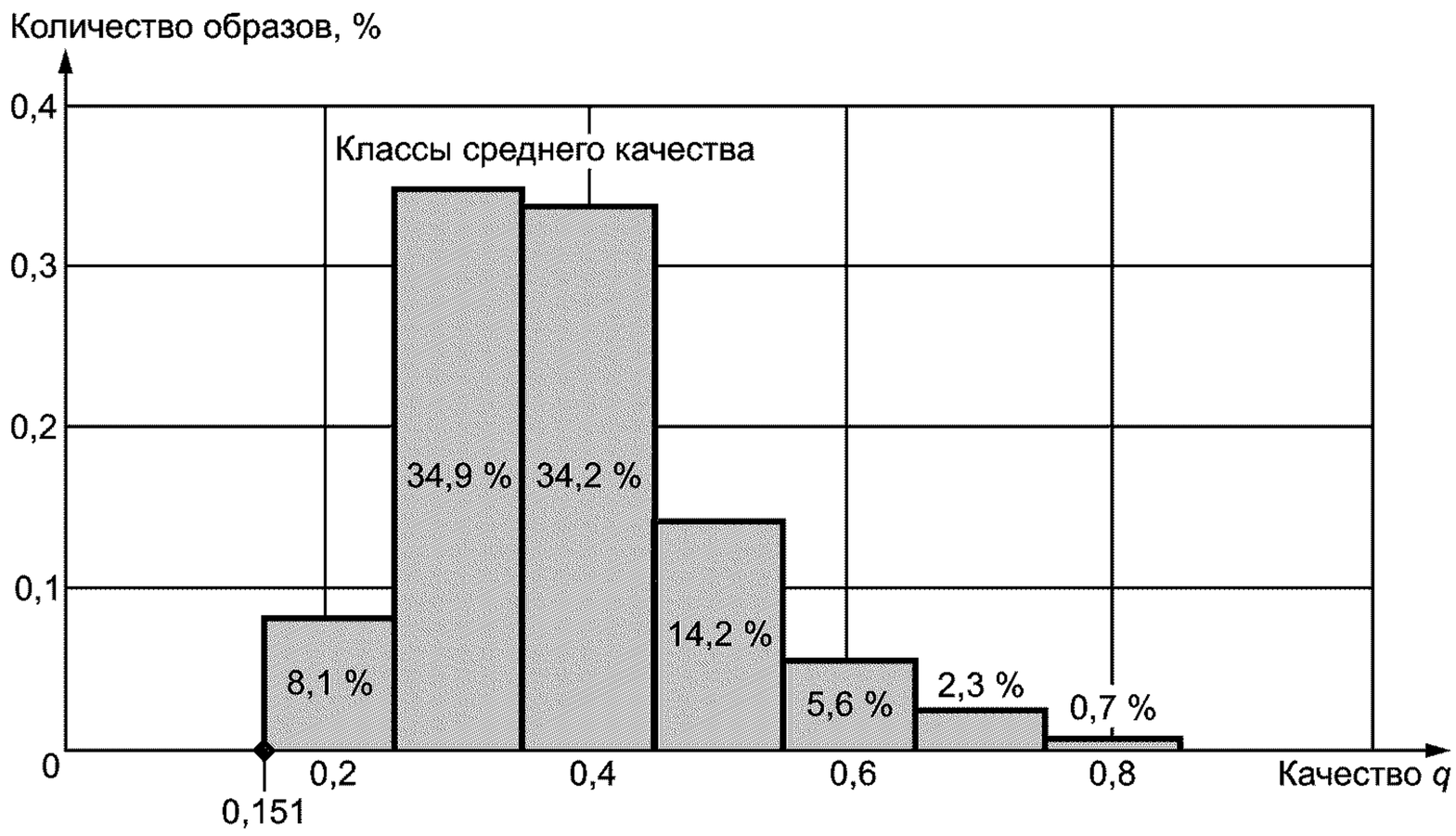

Рисунок В.1 — Процентное распределение биометрических рукописных образов «Свой» по классам среднего качества

Приложение Г
(рекомендуемое)

Совмещенное формирование баз естественных биометрических образов «Свой» и «Чужой»

Наиболее затратной частью процесса формирования баз естественных биометрических образов является работа доноров биометрии. Для сокращения затрат рекомендуется привлекать одного донора одновременно к созданию нескольких типов баз естественных динамических биометрических образов. Структура совмещения различных баз естественных динамических биометрических образов, формируемых одним донором, приведена на рисунке Г.1.

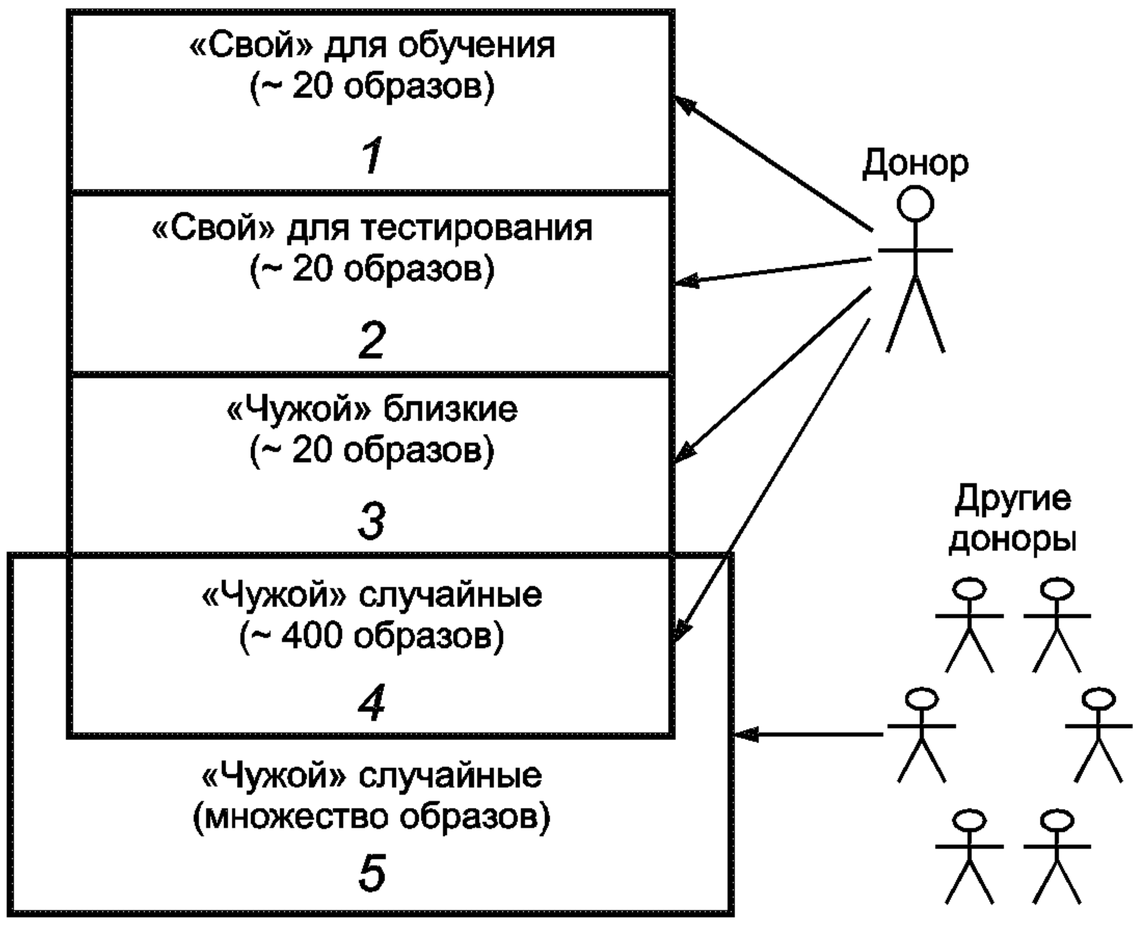

Рисунок Г.1 — Базы биометрических образов «Свой» и «Чужой»

Базы *1*, *2* и *3* формируются донором «Свой». При этом база «Свой» *1* предназначена для обучения преобразователя биометрия — код; база «Свой» *2* предназначена для тестирования ошибок первого рода обученного преобразователя биометрия — код; база «Чужой» *3* представляет собой базу естественных биометрических образов, близких к образу «Свой» (например, рукописных образов слов, отличающихся на один или несколько символов), предназначенную для тестирования ошибок второго рода обученного преобразователя биометрия — код при скомпрометированном образе. База *5* представляет собой имеющуюся в наличии базу «Чужой», составленную различными донорами без знания ими биометрического образа «Свой». Эта база предназначена для тестирования ошибок второго рода преобразователя биометрия — код при нескомпрометированной тайне (сохранение конфиденциальности) образа «Свой». База *4* представляет собой часть базы *5*, составленную из биометрических образов, написанных тем же донором. Эта база предназначена для тестирования ошибок второго рода обученного преобразователя биометрия — код. Процесс формирования баз естественных биометрических образов схематично изображен на рисунке Г.2.

При первом сеансе формирования баз личность донора подтверждают уполномоченные люди и донору присваивается анонимный идентификатор. После формирования баз создается нейросетевой биометрический контейнер, содержащий идентификатор донора, связанный с его известным системе биометрическим образом. Идентификатор донора связывается с каждым примером биометрического образа из базы либо с базой в целом.

При повторном сеансе формирования или дополнения базы тем же донором производится авторизация донора: при предъявлении донором его биометрического образа «Свой D.1» из нейросетевого биометрического контейнера извлекается идентификатор, по которому определяется база, ранее созданная этим донором, либо примеры биометрических образов, ранее созданные этим донором. Донору разрешается дальнейшая работа с этой базой через ее дополнение новым парольным образом «Свой D.2», близкими образами к «Свой D.2» и далекими от парольных образов образами «Чужой D».

При наличии во фрагменте базы донора D записи о значении пароля «Свой», словах, близких к паролю «Свой», и случайных паролях упрощается последующая сортировка этого фрагмента и происходит автоматическое дополнение его данными различных типов баз биометрических образов, описанных в настоящем стандарте.

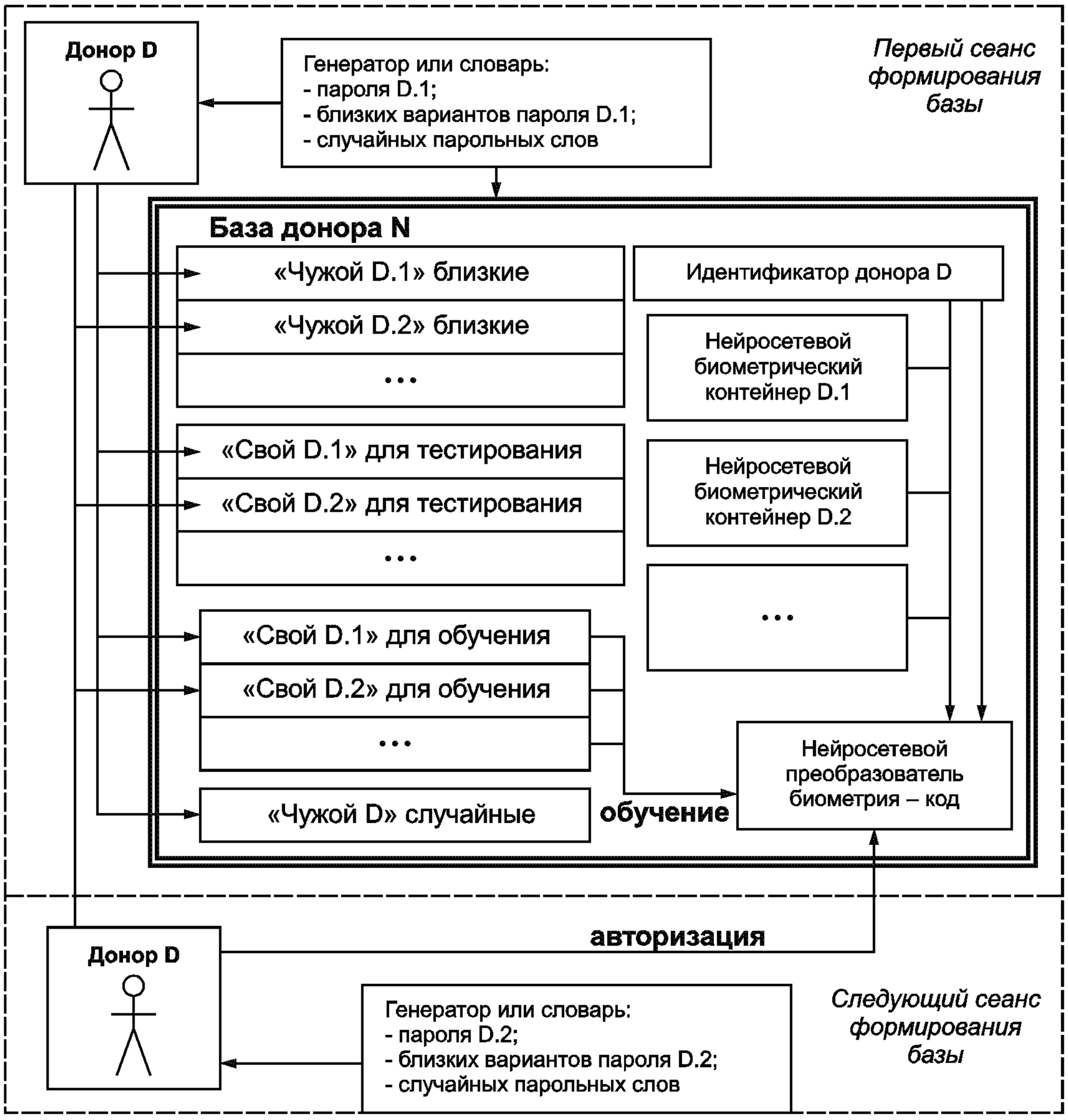

Рисунок Г.2 — Процесс формирования баз естественных биометрических образов при многократном привлечении одного донора (D)

Приложение Д
(справочное)

Согласование фрагментов баз естественных биометрических образов «Чужой»

Согласование фрагментов баз естественных биометрических образов может осуществляться любым методом и по любому статистическому параметру. В частности, согласование может быть осуществлено в целях уменьшения погрешности, вычисляемой по формуле (7) рукописных образов (для 416 параметров рукописного биометрического образа).

Пример расчета статистических величин контроля уровня согласованности усеченных баз рукописных образов приведен в таблице Д.1.

Таблица Д.1 — Показатели отклонения статистических параметров усеченных согласованной и несогласованной баз тестовых образов от полной эталонной базы, состоящей из 2000 биометрических образов, по 416 параметрам

Параметры	Несогласованная база		Согласованная база	
Количество образов в базе	100	300	100	300
Число контролируемых биометрических параметров	416			
ΔE [расчетная формула (7)]	0,174	0,126	0,148	0,114
$\Delta \sigma$ [расчетная формула (8)]	0,12	0,137	0,152	0,122
Δp [расчетная формула (9)]	0,177	0,131	0,168	0,119

Гистограммы статистического распределения биометрического параметра v_1 исходной полной базы, согласованной и несогласованной усеченной тестовой баз приведены на рисунках Д.1, Д.2 и Д.3.

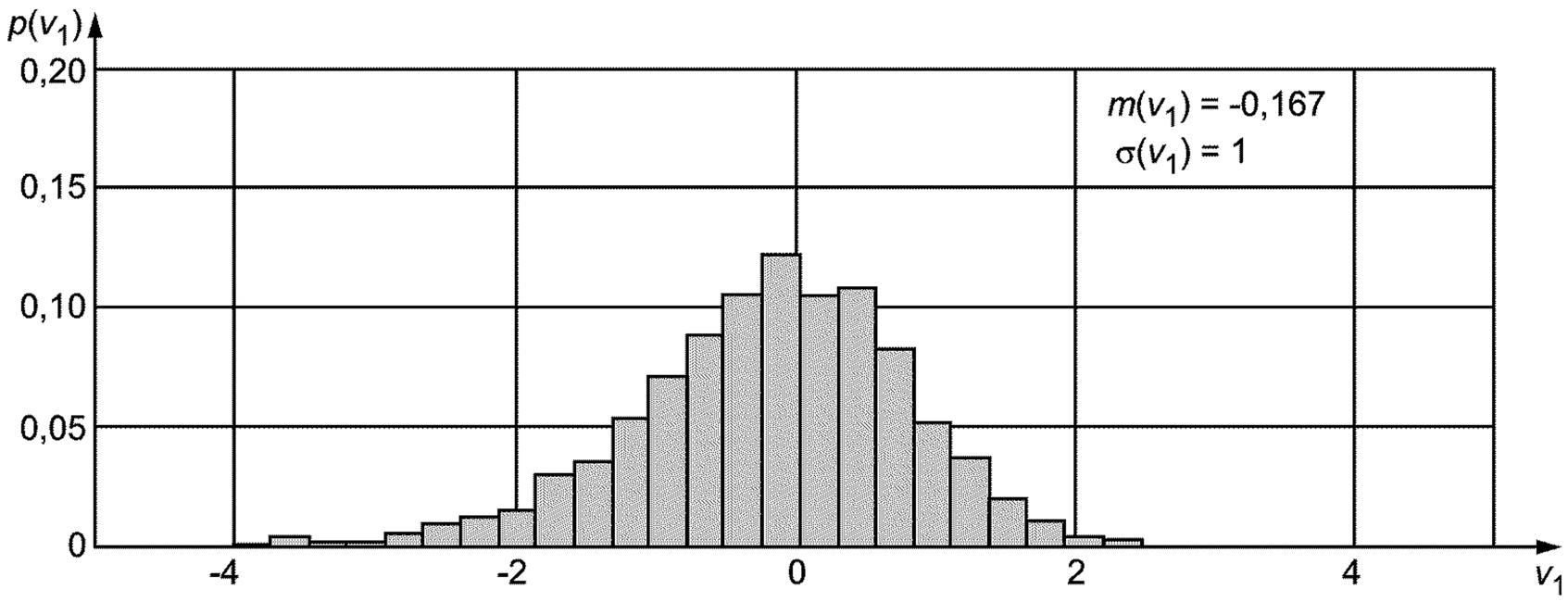

Рисунок Д.1 — Гистограмма плотности распределения биометрического параметра v_1 для 2000 тестовых биометрических образов исходной базы «Чужой»

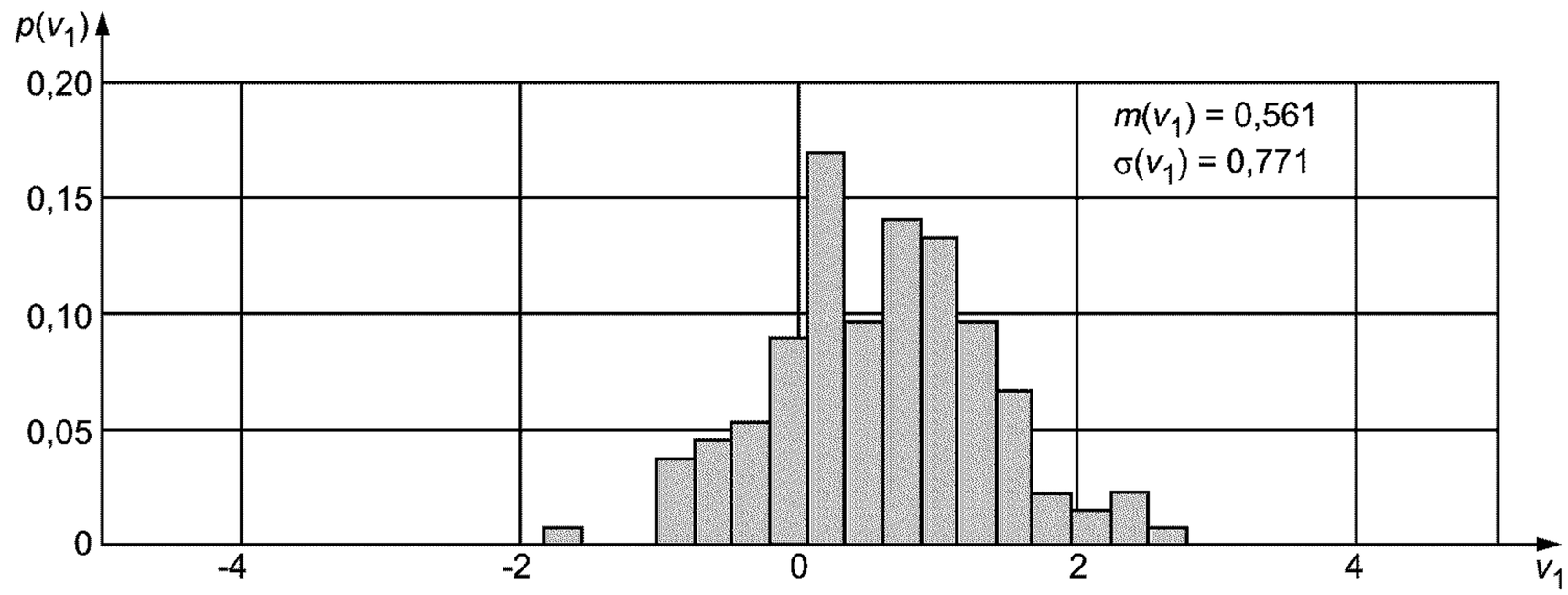

Рисунок Д.2 — Гистограмма плотности распределения биометрического параметра v_1 для 100 несогласованных по ΔE тестовых биометрических образов усеченной базы «Чужой»

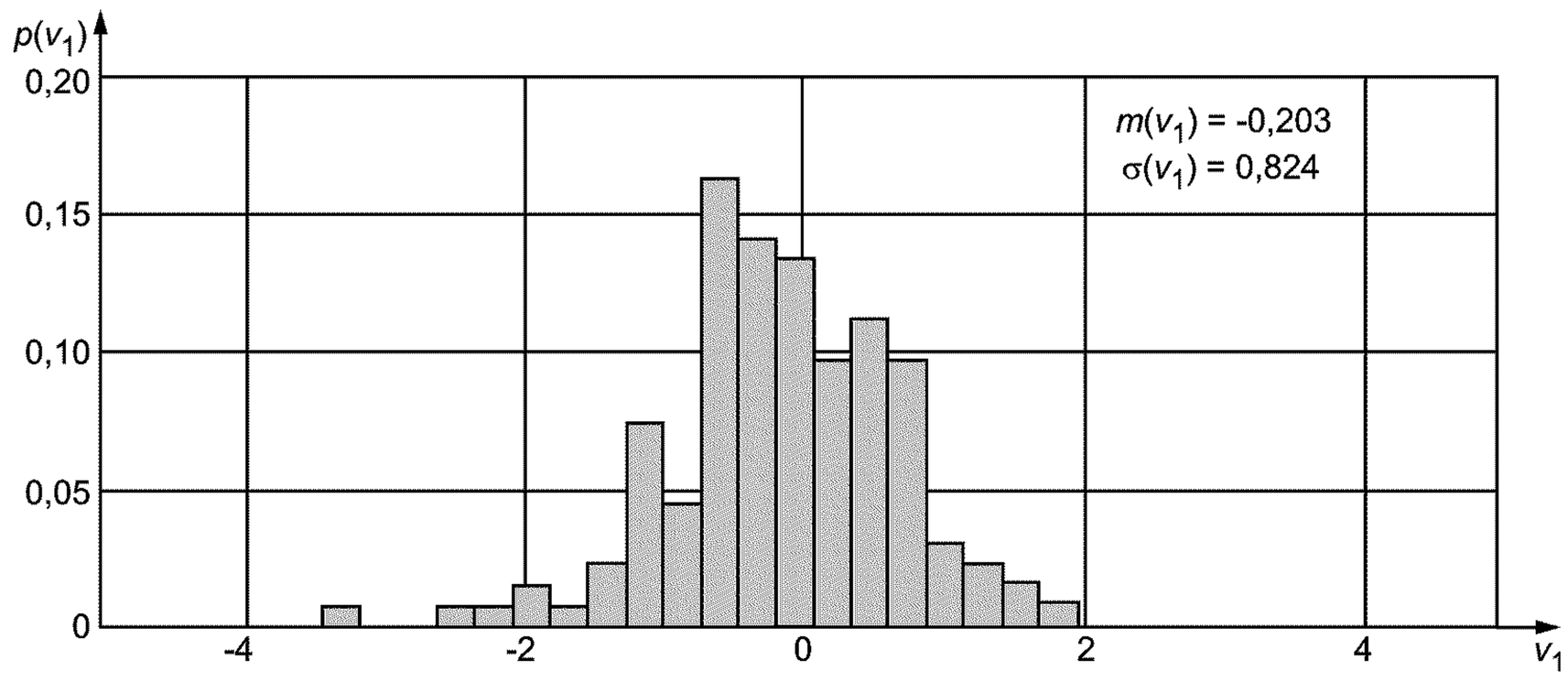

Рисунок Д.3 — Гистограмма плотности распределения биометрического параметра v_1 для 100 согласованных по ΔE тестовых биометрических образов усеченной базы «Чужой»

Приложение Ж
(справочное)

Пример структуры организации базы рукописных образов доноров

Пример структуры организации базы рукописных образов одного донора приведен на рисунке Ж.1.

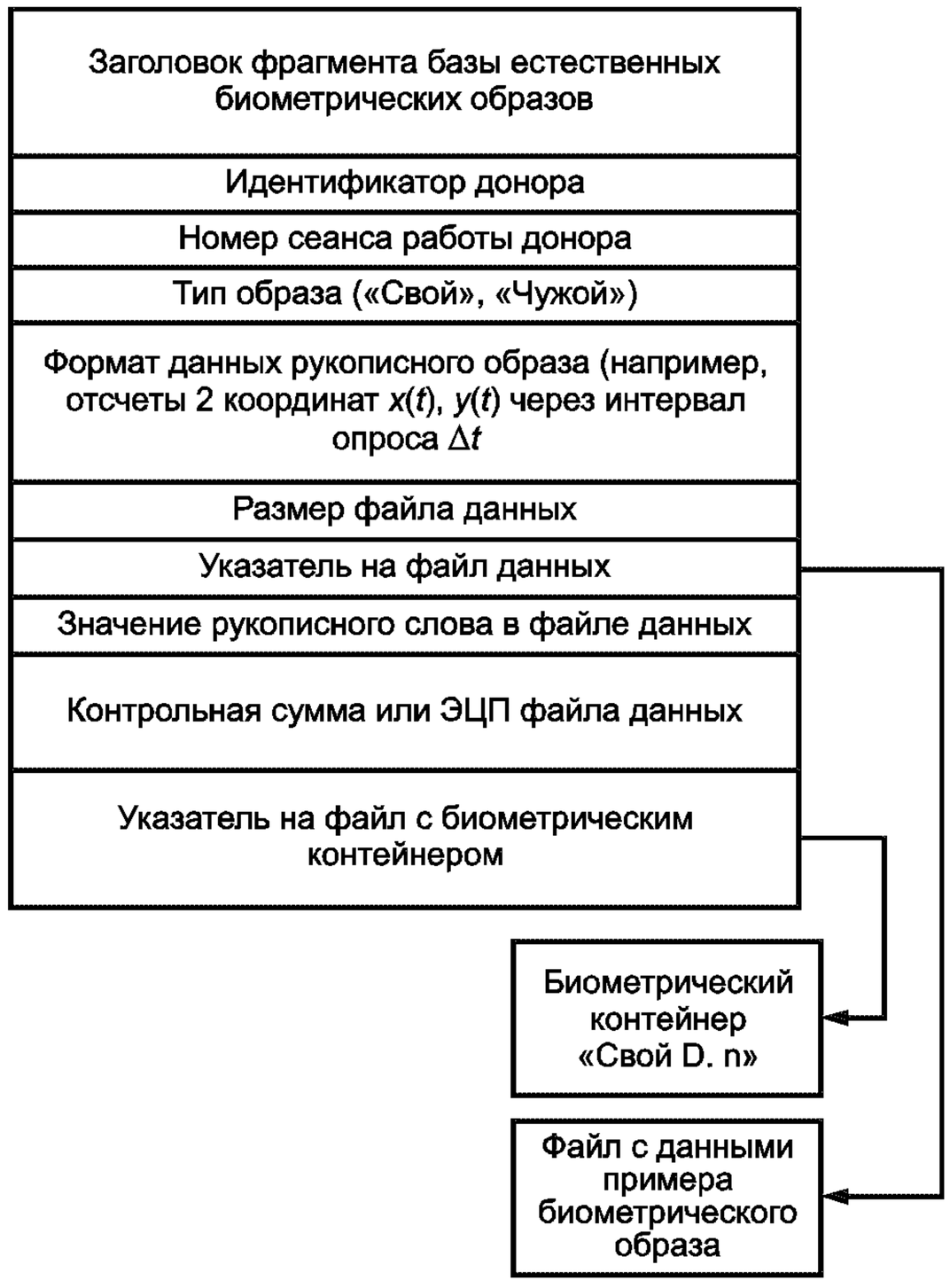

Рисунок Ж.1 — Пример структуры базы рукописных образов одного донора

УДК 681.18:006.354 ОКС 01.040.01 Т00

Ключевые слова: техническая защита информации, биометрия, базы биометрических образов, тестирование, донор биометрии

Редактор *П.М. Смирнов*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 06.09.2010. Подписано в печать 21.09.2010. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 2,79. Уч.-изд. л. 2,51. Тираж 101 экз. Зак. 733.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.