ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52633— 2006

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к средствам высоконадежной биометрической аутентификации

Издание официальное

БЗ 8—2006/210

Москва
Стандартинформ
2007

gost.e-ecolog.ru

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 Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России), Техническим комитетом по стандартизации ТК 362 «Защита информации»

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 27 декабря 2006 г. № 372-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

© Стандартинформ, 2007

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 Классификация средств высоконадежной биометрической аутентификации 3
5 Общие требования к средствам высоконадежной биометрико-криптографической аутентификации 5
6 Требования к обучению средств высоконадежной биометрико-нейросетевой аутентификации 7
7 Требования к средствам высоконадежной биометрической аутентификации, принимающим решение путем анализа нескольких разнородных биометрических образов 9
8 Основные показатели и характеристики для средств высоконадежной биометрической аутентификации 10
9 Требования к индикации режимов работы (конфигурации) и индикации критических переключателей режимов для средств высоконадежной биометрической аутентификации 11
10 Перечень угроз и способов обеспечения информационной безопасности при применении средств высоконадежной биометрической аутентификации 11
11 Правила приемки (поставки) 14
12 Требования к тестированию (испытаниям) 15
Приложение А (справочное) Таблицы рекомендуемых длин кодов ключей (паролей), используемых при совмещении нескольких биометрических технологий 17

Введение

Стандарт устанавливает требования к процедурам обработки биометрической информации и преобразователям нечетких (неоднозначных) биометрических образов пользователя в его длинный пароль или ключ, используемый далее в одной из процедур высоконадежной криптографической аутентификации.

Стандарт распространяется только на средства высоконадежной биометрической аутентификации, производители которых заявляют значения вероятностей ошибочного пропуска «Чужого» менее 10^{-12} (десять в минус 12 степени). Требования к средствам биометрической аутентификации с большей вероятностью ошибочного пропуска «Чужого» регламентируются системой международных стандартов, разработанных ISO/IEC JTC1 SC37 и гармонизированных ТК 355 ПК 7 «Биометрическая идентификация».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Требования к средствам высоконадежной биометрической аутентификации

Information protection.
Information protection technology.
Requirements for the means of high-reliability biometric authentication

Дата введения — 2007 — 04 —01

1 Область применения

Настоящий стандарт распространяется на средства высоконадежной биометрической аутентификации личности, построенные с использованием:

- стандартных механизмов высоконадежной парольной аутентификации с длинными, плохо запоминаемыми людьми паролями из случайных букв (цифр);
- криптографических механизмов аутентификации, использующих ключ длиной более 40 бит;
- множества из нескольких относительно слабых биометрических механизмов, обеспечивающих высоконадежную аутентификацию только при их совместном использовании.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.10—2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р ИСО/МЭК 15408-1—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р 50779.10—2000 (ИСО 3534-1—93) Статистические методы. Вероятность и основы статистики. Термины и определения

ГОСТ Р 50779.21—2004 Статистические методы. Правила определения и методы расчета статистических характеристик по выборочным данным. Часть 1. Нормальное распределение

ГОСТ 34.311—95 / ГОСТ Р 34.11—94 Информационная технология. Криптографическая защита информации. Функция хэширования

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 ежемесячно издаваемым информационным указателем, опубликованным в текущем году. Если ссылочный

Издание официальное

стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (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 с соответствующими определениями:

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

3.2 **атака перехвата:** Атака, направленная на перехват конфиденциальной биометрической информации в виде физического биометрического образа, электронного биометрического образа, вектора биометрических параметров, получаемого из них пароля или криптографического ключа.

3.3 **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.

3.4 **биометрическая аутентификация:** Аутентификация пользователя, осуществляемая путем предъявления им своего биометрического образа.

3.5 **биометрические данные:** Данные с выходов первичных измерительных преобразователей физических величин, совокупность которых образует биометрический образ конкретного человека.

3.6 **биометрическая идентификация:** Преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных нейронов.

3.7 **биометрический образ:** Образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека.

Примечание — Биометрический образ — это континуум множества биометрических примеров, однако с конечной погрешностью континуум примеров может быть представлен всего несколькими различающимися примерами.

3.8 **биометрический образ «Свой»:** Биометрический образ легального пользователя.

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

3.10 **биометрический механизм:** Механизм преобразования физического биометрического образа в вектор биометрических параметров или код ключа (пароля).

Примечание — Биометрический механизм является функционально неполной частью системы защиты или средства защиты информации.

3.11 **биометрические параметры:** Параметры, полученные после предварительной обработки биометрических данных.

Примечание — Параметрами могут быть, например, коэффициенты Фурье кривых колебаний пера при воспроизведении человеком рукописного пароля.

3.12 **вероятность ошибки первого рода:** Вероятность ошибочного отказа «Своему» пользователю в биометрической аутентификации.

3.13 **вероятность ошибки второго рода:** Вероятность ошибочной аутентификации «Чужого» как «Своего» (ошибочная аутентификация).

3.14 **высоконадежная биометрическая аутентификация:** Биометрическая аутентификация с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора.

3.15 **динамический биометрический образ:** Биометрический образ, изменяемый человеком по своему желанию, например рукописный образ слова-пароля.

3.16 **механизм биометрической аутентификации:** Функционально неполный фрагмент средства биометрической аутентификации, преобразующий биометрические данные, но не способный принимать аутентификационные решения высокой надежности из-за низкой размерности анализируемых векторов или отсутствия механизма криптографической аутентификации.

3.17 **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.

3.18 **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».

3.19 **средство биометрической аутентификации;** СБА: Средство биометрической аутентификации, способное принимать аутентификационное решение неопределенного уровня надежности.

3.20 **средство высоконадежной биометрической аутентификации;** СВБА: Средство биометрической аутентификации, способное принимать аутентификационное решение высокой надежности, имеющее в своем составе: биометрические механизмы преобразования биометрических данных в векторы биометрических параметров большой размерности, преобразователь «биометрия-код», механизм криптографической аутентификации.

3.21 **статический биометрический образ:** Образ, данный человеку от рождения, неизменяемый по воле человека, например рисунок отпечатка пальца.

3.22 **тайный биометрический образ:** Биометрический образ, сохраняемый пользователем в тайне.

Примечание — Для сохранения в тайне динамического биометрического образа необходимо сохранить в тайне пароль, порождающий его; для сохранения в тайне статического биометрического образа необходимо обеспечить анонимность пользователя.

3.23 **открытый биометрический образ:** Биометрический образ человека, общедоступный для наблюдения.

Примечание — Обычно открытые биометрические образы являются статическими, однако и динамические биометрические образы могут быть открытыми, например рукописный автограф человека.

3.24 **обучение биометрического средства:** Обучение биометрического средства аутентифицировать человека с заданными вероятностями ошибок первого и второго рода на одном или нескольких примерах биометрических образов «Свой».

3.25 **физический муляж:** Муляж, выполненный на физическом уровне, исходя из знания физического эффекта, на котором работает датчик считывания биометрического средства защиты и знания индивидуальных особенностей, подделываемого на физическом уровне биометрического образа.

3.26 **электронный муляж:** Электронные данные, имитирующие биометрические данные пользователя при тестировании или попытках обхода системы защиты.

Примечание — Различают неслучайный электронный муляж — электронные биометрические данные реального пользователя априорно известны, например перехвачены. Случайный муляж — электронные данные генерируются случайно. Частично случайный муляж — частично или полностью известные электронные биометрические данные реального пользователя искусственно размываются случайным шумом.

4 Классификация средств высоконадежной биометрической аутентификации

4.1 Средства биометрической аутентификации могут быть отнесены к высоконадежным, только если в их состав введены криптографические механизмы аутентификации, работающие совместно с биометрическими механизмами аутентификации через преобразование нечетких (неоднозначных) биометрических образов в однозначный криптографический ключ или длинный пароль. Пользователь подобных систем избавлен от необходимости хранить надлежащим образом ключ или запоминать длинный случайный пароль. Пользователь через присущую ему биометрию сам является ключом (паролем) доступа (аутентификации). Для средств высоконадежной биометрико-криптографической аутентификации сложность подбора биометрии анонимного пользователя или сложность подбора тайного биометрического образа известного пользователя должна быть сопоставима со сложностью подбора используемого в средстве криптографического аутентификационного ключа (длинного пароля).

Средство биометрической аутентификации может быть отнесено к высоконадежным только после его обучения на биометрическом образе «Свой» достаточно высокой информативности.

Примечание — Уровень информативности биометрического образа «Свой» оценивается встроенными средствами прогнозирования ожидаемой стойкости к атакам подбора. Оценка уровня информативности биометрического образа «Свой» приведена также в таблицах А.2 и А.3 (приложение А).

4.2 СВБА классифицируют по использующимся ими биометрическим механизмам или их комбинациям. На настоящий момент апробированы или имеют перспективы широкого практического использования следующие биометрические механизмы:

- анализ кровеносных сосудов глазного дна;
- анализ радужной оболочки глаза;
- двухмерный и трехмерный анализы геометрических особенностей лица в видимом и инфракрасном спектрах света;
- анализ особенностей геометрии ушных раковин;
- анализ особенностей голоса;
- анализ особенностей папиллярных рисунков пальцев;
- анализ геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони;
- анализ рисунка кровеносных сосудов, складок кожи тыльной стороны ладони;
- анализ рукописного почерка;
- анализ клавиатурного почерка;
- анализ геометрических соотношений частей тела;
- анализ особенностей походки.

Каждый из перечисленных выше механизмов способен давать свой уникальный биометрический образ человека. Все биометрические образы человека делятся на статические биометрические образы с ограниченной информативностью и динамические биометрические образы с неограниченной информативностью.

Статические биометрические образы даны человеку от рождения, имеют ограниченную информативность и не могут быть изменяемыми по воле их хозяина. Сохранение в тайне статического биометрического образа человека может быть обеспечено только через обеспечение анонимности пользователя.

Динамические биометрические образы человека имеют неограниченную информативность и могут быть легко изменены по воле человека. Динамические биометрические образы могут быть получены механизмами анализа особенностей голоса, рукописного почерка, клавиатурного почерка. Неограниченная информативность динамических биометрических образов обусловлена возможностью неограниченного увеличения их размеров (увеличения длин вводимых голосом фрагментов речи, рукописно вводимых фрагментов текстов, вводимых с клавиатуры текстов). Сохранение в тайне динамических биометрических образов обеспечивается тем, что их владелец сохраняет в тайне свои голосовые парольные фразы, рукописные парольные слова (фразы), клавиатурные парольные тексты.

4.3 СВБА классифицируют по способам их технической реализации и различают:

- программные средства, ориентированные на использование стандартной вычислительной среды;
- программно-аппаратные средства, частично используемые в специализированной вычислительной среде;
- аппаратные средства, используемые только в специализированной вычислительной среде.

4.4 СВБА классифицируют по уровню безопасности окружающей их среды и различают:

- локальную биометрическую аутентификацию с информацией, не выходящей за пределы контролируемой зоны;
- дистанционную биометрическую аутентификацию с использованием передачи аутентификационной информации по открытым каналам связи за пределы контролируемой зоны.

4.5 СВБА классифицируют по типам носителей информации, используемых для хранения аутентификационной информации. Возможно размещение таблиц преобразователя «биометрия-код»:

- на сервере поддержки биометрического доступа;
- в стационарном компьютере (рабочей станции);
- в мобильном компьютере (карманном или ноутбуке);
- в личном мобильном телефоне;
- на специальной дискете с магнитным носителем информации или на идентификационной карте с магнитной полосой;
- на специальном диске с оптическим считыванием информации;
- на носимом жестком диске;
- в носимой флэш-памяти и других подобных носителях информации;
- в специализированном вычислителе;
- в памяти идентификационной смарт-карты.

4.6 СВБА классифицируют по ориентации их на различные типы политик управления информационной безопасностью:

- полностью децентрализованное управление характеризуется применением механизмов асимметричной криптографии, широкими правами пользователей, самостоятельно обучающих биометрические механизмы доступа к информации и самостоятельно изменяющих свои личные ключи (пароли);
- частично децентрализованное управление может применять механизмы как симметричной, так и асимметричной криптографии, пользователи и администратор системы совместно управляют обучением биометрических механизмов и ключами (длинными паролями);
- централизованное управление характеризуется полным подчинением пользователей администратору системы, который полностью контролирует и процедуру обучения биометрических механизмов, и процедуры управления ключами криптографических механизмов (пользователь не имеет прямого доступа к ключам).

4.7 СВБА классифицируют по стойкости использованных в них криптографических механизмов к атакам подбора и требованиям к стойкости биометрических механизмов. Различают средства:

- с биометрическими механизмами по стойкости к атакам подбора, много слабее аналогичной стойкости используемых криптографических механизмов (в таких системах сторонний наблюдатель имеет доступ только к уже защищенной криптографическими механизмами информации);
- с биометрическими механизмами по стойкости к атакам подбора, эквивалентной аналогичной стойкости используемых криптографических механизмов (входы биометрической защиты доступны внешним наблюдателям, для таких систем длина кода ключа (пароля) приведена в таблицах А.1—А.3 (приложение А).

4.8 Перечисленные выше классы средств высоконадежной биометрической аутентификации существенно отличаются между собой по дружественности к пользователю и по обеспечиваемому ими уровню информационной безопасности. Особенности каждого из классов средств биометрической аутентификации должны быть отражены в профиле защиты по ГОСТ Р ИСО/МЭК 15408-1, ГОСТ Р ИСО/МЭК 15408-2.

5 Общие требования к средствам высоконадежной биометрико-криптографической аутентификации

5.1 Средства высоконадежной биометрико-криптографической аутентификации имеют типовую структуру преобразований, приведенную на рисунке 1.

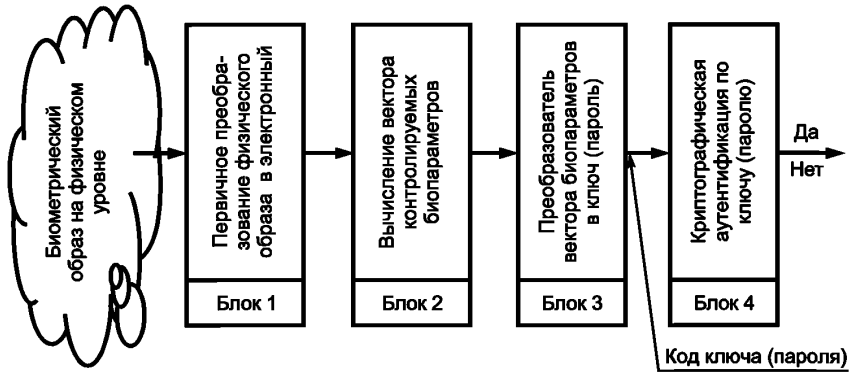

Рисунок 1 — Структурная схема обработки информации в средствах высоконадежной биометрической аутентификации

В структурной схеме блок 1 осуществляет преобразование физического нечеткого биометрического образа человека в электронный биометрический нечеткий образ через первичные преобразователи физических величин в электронные цифровые данные. Блок 2 осуществляет нормирование электронных образов и вычисление вектора биометрических параметров, например в виде коэффициентов

Фурье в средствах аутентификации по динамике воспроизведения рукописного пароля. Блок 3 осуществляет преобразование вектора биометрических параметров в код ключа (пароля) для последующей криптографической аутентификации. Блок 4 осуществляет криптографическую аутентификацию пользователя по его ключу или паролю, выдавая на выход решение «Да» или «Нет».

5.2 Для усиления стойкости биометрической защиты к атакам изучения и модификации программного обеспечения (ПО) высоконадежные варианты ее технической реализации не должны содержать примеров биометрических образов пользователя, биометрического эталона образов пользователя и кода ключа (пароля) пользователя. Эта информация является конфиденциальной и должна быть защищена при хранении. Кроме того, следы этой конфиденциальной информации должны быть гарантированно уничтожены после выполнения каждой конкретной процедуры аутентификации.

5.3 Для средств высоконадежной биометрической аутентификации допустимо сокрытие конфиденциальной информации о коде ключа (пароля) пользователя и его биометрических образах в таблицах параметров и связей нейросетевого преобразователя биометрических параметров в ключ (пароль). Кроме того, допустимо применение и иных способов сокрытия этой информации, например в форме таблиц преобразователя вектора биометрических параметров в ключ (пароль), использующего нечеткую математическую обработку биометрических данных.

5.4 СВБА должно быть способно преобразовывать множество образов «Свой» в ключ (пароль) пользователя с заранее заданной, приемлемой для пользователя вероятностью ошибочного отказа пользователю в доступе или аутентификации.

5.5 Средство высоконадежной биометрической аутентификации должно быть способно преобразовывать множество случайных входных образов «Чужие» в случайные состояния ключа (пароля), каждый разряд которых должен:

- иметь близкие к равновероятным состояния «0» и «1»;
- иметь нулевые коэффициенты парной и групповой корреляции.

5.6 Для увеличения уровня доступности средств высоконадежной биометрической аутентификации пользователям, находящимся в стрессовом состоянии, допустимо разрешать множество попыток аутентификации. Число допустимых попыток аутентификации может быть сопоставимо с числом примеров биометрических образов «Свой», на которых обучалось средство биометрической аутентификации. Число разрешаемых средством попыток аутентификации не является секретом и может храниться открыто.

5.7 Для увеличения уровня доступности средств высоконадежной биометрической аутентификации пользователей, находящихся в стрессовом состоянии, допустимо снабжать СВБА обнаружителями нестабильных бит выходного ключа (пароля) или нестабильных входных биометрических параметров преобразователя, а также системой перебора возможных состояний наиболее нестабильных бит выходного ключа и входных биометрических параметров. Допускается осуществлять перебор возможных состояний до 7 % бит выходного ключа или до 7 % входных биометрических параметров. Информация о положении наиболее нестабильных разрядов выходного ключа и номерах нестабильных биометрических параметров конфиденциальна и должна быть гарантированно уничтожена после завершения процедур аутентификации.

5.8 Средство высоконадежной биометрической аутентификации при каждой попытке аутентификации должно выдавать результат биометрической аутентификации «Да» или «Нет», а также число нестабильных бит кода ключа (число попыток подбора и результат подбора, если подбор разрешен по действующей политике информационной безопасности). Перечисленные выше данные используются для организации аудита биометрической информации и не являются конфиденциальными. Они могут храниться как централизованная система сбора аудита, так и локальное средство личной биометрической аутентификации, собирающим свой аудит биометрической безопасности.

5.9 Средство высоконадежной биометрической аутентификации должно давать пользователю возможность видеть (знать) свой ключ (пароль) и возможность его сохранять (например, на аварийном бумажном носителе, находящемся в опечатанном конверте). Если такая возможность противоречит принятой политике безопасности, то она должна быть отключена администратором безопасности (должна быть предусмотрена возможность такого отключения).

5.10 Средство высоконадежной биометрической аутентификации должно иметь безопасный аварийный вход в виде возможности ручного набора кода ключа (пароля) на случай, если пользователь полностью утратил свои возможности по воспроизведению своего биометрического образа.

6 Требования к обучению средств высоконадежной биометрико-нейросетевой аутентификации

6.1 Обучение средств высоконадежной биометрико-нейросетевой аутентификации сводится к обучению искусственной нейронной сети преобразовывать множество входных образов «Свой» в личный ключ пользователя и множество входных образов «Чужой» в случайный «белый шум» на каждом из выходов искусственной нейронной сети. Для обучения используется N_1 примеров образов «Свой» и N_2 примеров образов «Чужой». Структурная схема процедуры обучения искусственной нейронной сети приведена на рисунке 2.

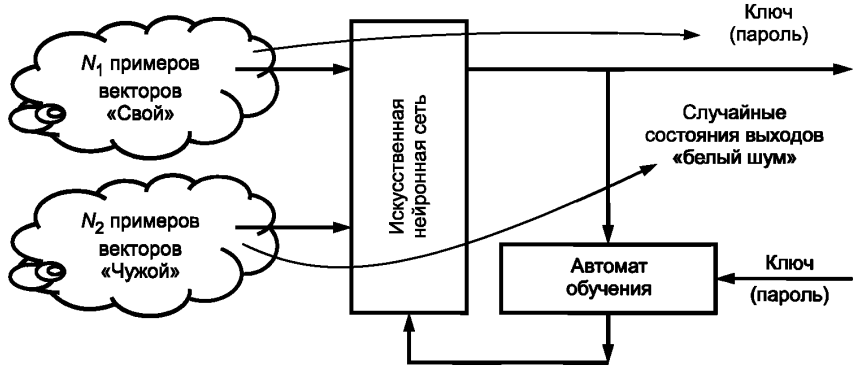

Рисунок 2 — Структурная схема процедуры обучения нейросетевого преобразователя векторов биометрических параметров в код ключа (пароля)

6.2 Алгоритм обучения искусственной нейронной сети и реализующий его автомат могут быть любыми, однако время обучения и потребляемые вычислительные ресурсы на обучение должны быть приемлемыми для потребителей. Из-за потенциальной опасности процедуры обучения время ее осуществления не должно превышать нескольких минут. При обучении искусственной сети нейронов пользователь или администратор безопасности должны лично контролировать зону, в которой осуществляется процесс обучения (зону расположения обучающего нейросеть вычислительного средства) и использовать при обучении только доверенную вычислительную среду (без закладок и иных неконтролируемых вычислительных процессов).

6.3 После процедуры обучения средства высоконадежной биометрико-нейросетевой аутентификации потребитель или администратор безопасности должны оценить качество обучения. Оцениваются достигнутые искусственной нейронной сетью вероятность ошибки первого рода — P_1 (ошибочного отказа в аутентификации «Своему») и вероятность ошибки второго рода — P_2 (ошибочной аутентификации «Чужого»). Это необходимо в силу того, что пользователи на практике стараются облегчить себе процедуру биометрической аутентификации, например необоснованно сократить длину своего рукописного пароля. Это необходимо в силу того, что пользователи имеют разную стабильность воспроизведения их биометрического образа. Кроме того, уникальность (информативность) биометрических образов разных людей различна. Стойкость конкретного биометрического образа пользователя является функцией его длины, стабильности, уникальности. Пользователь и администратор безопасности должны знать реальные оценки стойкости к атакам подбора конкретной реализации биометрической защиты после ее обучения, построенной на воспроизведении конкретного тайного биометрического образа. Тестирование осуществляют, используя n_1-тестовый пример векторов образов «Свой» и n_2-тестовых примера векторов образов «Чужой». Структурная схема процедуры тестирования приведена на рисунке 3. Примеры для тестирования системы не должны использоваться ранее при ее обучении.

6.4 Так как процедуры тестирования и обучения нейросетевой защиты предполагают использование конфиденциальных биометрических образов «Свой» и ключа (пароля) пользователя, они являются потенциально опасными. Тестирование и обучение следует проводить в условиях повышенных требо-

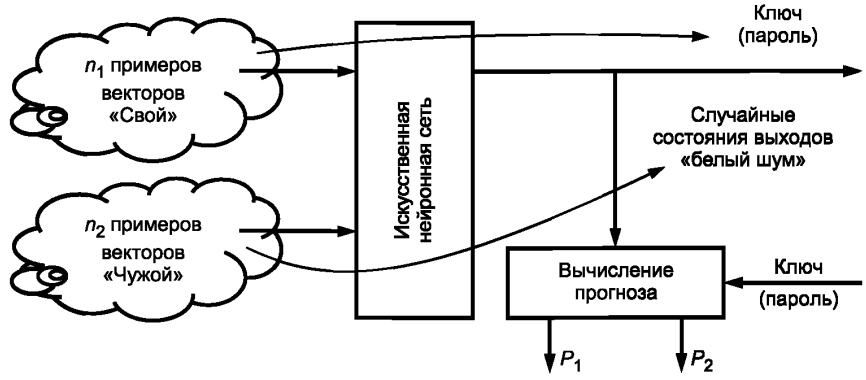

Рисунок 3 — Структурная схема процедуры тестирования биометрико-нейросетевой защиты, проводимой после процедуры обучения

ваний к чистоте вычислительной среды и малому времени вычислений при обучении. После тестирования и обучения конфиденциальная информация в форме ключа (пароля), а также биометрических образов «Свой» должна быть гарантированно уничтожена. Кроме того, должны быть предусмотрены организационно-технические мероприятия, исключающие перехват конфиденциальной информации через каналы визуального наблюдения, акустического прослушивания, побочных электромагнитных излучений и наводок.

6.5 Ключ, используемый при обучении, должен иметь длину в соответствии с требованиями используемого механизма криптографической аутентификации. Например, при использовании для аутентификации механизма электронной цифровой подписи (ЭЦП) длину ключа и требования к нему выбирают в соответствии с ГОСТ Р 34.10. Рекомендации по выбору длин ключей (фрагментов ключей) для мультибиометрических систем приведены в таблицах А.1—А.3 (приложение А).

6.6 При выборе длины пароля, используемого при обучении, следует руководствоваться требованиями соответствующего механизма парольной аутентификации. Рекомендуется выбирать длину случайного пароля, близкую к максимальному значению длины пароля, допустимую для каждого конкретного механизма парольной аутентификации. Недопустимо использовать короткие случайные пароли, код которых менее 40 бит.

6.6.1 Рекомендуется использование средствами высоконадежной биометрической аутентификации программ автоматического синтеза случайных паролей с качественным генератором случайных чисел.

6.6.1.1 Необходимо проверять число нулевых и единичных разрядов в случайном коде сгенерированного пароля. Число нулевых и единичных значений кода должно быть примерно одинаковым. Допускается 10 %-ное различие чисел «0» и «1» в случайном двоичном коде.

6.6.1.2 Серии из одинаковых знаков должны иметь длину не более 7 % длины двоичного кода сгенерированного случайного пароля при округлении длины серии до целого числа в меньшую сторону.

6.7 При использовании статических биометрических образов длина вектора биометрических параметров и их качество зависят от алгоритма предварительной обработки биометрических образов и информативности самого биометрического образа. Длина векторов биометрических параметров статических биометрических образов и их информативность не могут быть изменены по желанию пользователей. Интервалы возможных значений вероятностей ошибок второго рода для различных статических биометрических образов приведены в таблицах А.1 и А.3 (приложение А). Использование статических биометрических образов потенциально опасно, так как обеспечить анонимность пользователя не всегда возможно. Без обеспечения анонимности пользователя его статические биометрические образы могут быть скомпрометированы (перехвачены), что резко снижает уровень защищенности. Даже зная, что его статический биометрический образ скомпрометирован, пользователь не может изменить свой статический биометрический образ, данный ему от рождения.

6.8 При использовании динамических биометрических образов:

- паролей, воспроизведенных рукописным почерком;
- парольных фраз, воспроизведенных голосом;

- парольных фраз с контролем клавиатурного почерка при их наборе появляются дополнительные возможности по сохранению используемого биометрического образа в тайне. При компрометации динамического биометрического образа он может быть изменен пользователем. Информативность таких биометрических образов может быть изменена пользователем по его усмотрению. Пользователь может увеличивать длину своего рукописного пароля или число слов в рукописной парольной фразе до момента, пока прогноз стойкости его личной биометрической защиты к атакам подбора не достигнет приемлемого значения. Интервалы возможных значений вероятностей ошибок второго рода для различных динамических биометрических образов приведены в таблице А.2 (приложение А).

6.8.1 При выборе рукописного пароля в средствах высоконадежной биометрической аутентификации нет необходимости использовать плохо запоминаемые комбинации из случайных символов. Рекомендуется использовать легко запоминаемые слова родного языка пользователя, которые могут быть усилены:

- увеличением числа букв в слове;
- использованием сочетаний слов;
- изменением порядка воспроизведения букв, цифр, знаков;
- введением обратных росчерков;
- изменением, пропуском, добавлением одного из знаков;
- написанием коротких цифровых кодов через рукописную запись буквами.

Пример — Код 213 можно записать прописью: «двести тринадцать», содержащей 16 букв.

Эффективность мер усиления рукописного пароля проверяется средствами встроенного тестирования и прогнозирования.

6.8.2 При выборе голосового пароля в высоконадежных средствах биометрической аутентификации рекомендуется использовать сочетания легко запоминаемых слов родного языка пользователя, которые могут быть усилены:

- увеличением числа букв в словах голосового пароля;
- увеличением числа слов в голосовом пароле;
- короткими цифровыми кодами, воспроизводимыми в соответствии с правилами произнесения цифр на языке пользователя.

Эффективность мер усиления голосового пароля (парольной фразы) проверяется средствами встроенного тестирования и прогнозирования.

6.8.3 При выборе клавиатурного пароля рекомендуется использовать фрагмент текста, случайно выбранный из книги, журнала, статьи. Оценка стойкости парольной фразы в сочетании с контролем клавиатурного почерка проверяется встроенными в СВБА средствами тестирования и прогнозирования.

7 Требования к средствам высоконадежной биометрической аутентификации, принимающим решение путем анализа нескольких разнородных биометрических образов

7.1 Одним из эффективных путей усиления уровня защищенности биометрических средств аутентификации и ограничения доступа является использование совокупности разных биометрических механизмов. При этом разные биометрические механизмы имеют разный уровень стойкости к атакам подбора, и соответственно используемые механизмы их объединения должны исключать возможность обхода мультибиометрической защиты через наиболее слабый механизм. Возможны два способа решения задачи и их комбинации.

7.2 Безопасное объединение двух и более биометрических механизмов может быть осуществлено по выходам нескольких преобразователей биометрии в ключ. Рекомендуется осуществлять объединение путем формирования общего (составного) ключа, каждый из фрагментов которого формируется своим преобразователем «биометрия-код». Взаимная балансировка различных биометрических механизмов осуществляется выбором длины ключевого фрагмента для каждого механизма пропорционально его стойкости к атакам подбора. Рекомендации по выбору сбалансированных длин ключей приведены в таблицах А.1—А.3 (приложение А).

7.3 Безопасное объединение двух и более биометрических механизмов допустимо осуществлять по входам одного общего преобразователя биометрии в код. По этому способу вектора биометрических параметров разных биометрических механизмов объединяются в один длинный вектор, который и подается на входы единственного преобразователя «биометрия-код».

7.4 Допускается использование комбинаций объединения биометрических механизмов по входам и выходам преобразователей.

7.5 При формировании биометрического ключа с длиной, существенно превышающей необходимую длину криптографического ключа аутентификации (например, при объединении разнородных биометрических механизмов), рекомендуется осуществлять сокращение длины биометрического ключа до требуемого размера через вычисление хэш-функции по ГОСТ 34.311 и использование части хэшированной информации.

7.6 Недопустимо снабжать средства высоконадежной биометрической аутентификации однозначными показателями (индикаторами) правильности формирования фрагментов ключа. Допустимо однозначно отображать только появление всего составного верного ключа. Допустимо использование только неоднозначных косвенных индикаторов контроля фрагментов составного ключа.

8 Основные показатели и характеристики для средств высоконадежной биометрической аутентификации

8.1 СВБА должны сообщать пользователю следующие параметры, отражающие их способность осуществлять положительную аутентификацию:

- вероятность ошибочного отказа «Своему» для среднестатистического пользователя;
- прогноз вероятности ошибочного отказа «Своему» на конкретном биометрическом образе пользователя.

8.2 СВБА должно сообщать пользователю следующие параметры, отражающие способность противостоять попыткам его обхода:

- вероятность ошибочного пропуска «Чужого» при предъявлении им случайного биометрического образа для среднестатистического пользователя при отсутствии компрометации биометрического образа;
- прогноз значения вероятности пропуска «Чужого» при предъявлении им случайного биометрического образа для конкретного нескомпрометированного биометрического образа пользователя;
- вероятность пропуска «Чужого» для скомпрометированного биометрического образа среднестатистического пользователя;
- вероятность удачи подбора ключа (пароля) с первой попытки (величина, обратная размерам ключевого поля);
- вероятность удачи подбора биометрического образа среднестатистического пользователя с первой попытки при атаке подбора нормальным белым шумом (величина, обратная размерам поля возможных некоррелированных состояний биометрических образов);
- прогноз значения вероятности удачи подбора биометрического образа конкретного пользователя с первой попытки при атаке подбора нормальным «белым шумом» (прогноз величины, обратной размерам поля возможных некоррелированных состояний конкретного биометрического образа);
- вероятность удачи подбора биометрического образа среднестатистического пользователя с первой попытки при атаке коррелированным нормальным шумом, воспроизводящим корреляционные связи реальных биометрических образов (величина, обратная размерам поля возможных коррелированных состояний биометрических образов);
- прогноз значения вероятности удачи подбора биометрического образа конкретного пользователя с первой попытки при атаке подбора коррелированным нормальным шумом, воспроизводящим корреляционные связи реальных биометрических образов (прогноз величины, обратной размерам поля возможных коррелированных состояний конкретного биометрического образа).

8.3 Производителям средств высоконадежной биометрической аутентификации предписывается сообщать пользователям о материальных затратах и затратах времени на преодоление их биометрической защиты от несанкционированного доступа (НСД) через подбор биометрических параметров, подбор ключа (пароля), изготовление муляжей биометрических образов на физическом уровне.

9 Требования к индикации режимов работы (конфигурации) и индикации критических переключателей режимов для средств высоконадежной биометрической аутентификации

9.1 Предоставленное пользователю СВБА должно иметь средства управления своей конфигурацией.

9.1.1 Программный или аппаратно-программный продукт высоконадежной биометрической аутентификации должен быть авторизован (инсталлироваться только с диска производителя, отвечающего за его действия и содержание), а также быть обеспечен средствами контроля авторизации. Авторизация действующего программного продукта должна быть двухсторонней (со стороны производителя и со стороны потребителя). После обучения биометрической защиты пользователь должен иметь средства контроля за отсутствием каких-либо модификаций системы. Авторизация со стороны производителя должна осуществляться в виде уникального номера и ЭЦП производителя поставляемого программного продукта. Авторизация со стороны потребителя должна осуществляться в виде уникального имени пользователя средства биометрической защиты и даты его обучения, а также в виде ЭЦП потребителя (пользователя). Биометрическая защита должна автоматически проверять последнюю авторизацию (цепь событий авторизации контролируется в ручном режиме).

9.1.2 СВБА должно иметь конкретную конфигурацию или быть оснащено средствами управления настройками конфигурации. Единственная конфигурация средства высоконадежной биометрической аутентификации или все возможные ее комбинации должны быть описаны в технической документации. После изменения конфигурации, как и после переобучения, средства должны отслеживать все изменения в настройках. В СВБА должен присутствовать механизм контроля целостности заданной пользователем конфигурации средства высоконадежной биометрической аутентификации.

9.1.3 СВБА должно работать в строго заданной конфигурации аппаратно-программных средств обработки информации и конкретных параметрах вычислительной среды. Изменения конфигурации средств обработки информации и характеристик вычислительной среды должны отслеживаться средствами контроля конфигурации и параметров внешней вычислительной среды.

9.1.4 Система управления конфигурацией должна быть обеспечена документацией разработчика со списком возможных комбинаций управления конфигурацией. Изменения настроек конфигурации системы должны осуществляться строго в соответствии с документацией производителя, содержащей перечень планов последовательного изменения конфигурации.

9.1.5 Система управления конфигурацией должна предусматривать такие меры (в том числе и организационно-технические), при которых могут быть осуществлены только санкционированные изменения настроек конфигурации.

9.2 СВБА должны однозначно отражать режимы своей работы и оповещать пользователей об уровне опасности этих режимов и последствиях их переключения.

9.2.1 Режимы повышенной опасности, такие как:

- режим переобучения системы на новый биометрический образ;
- режим переобучения системы для смены ключа (длинного пароля);
- режим уничтожения старого ключа (пароля) и ввода нового ключа (пароля);
- режим генерирования новых длинных паролей и замены старых длинных паролей;
- режимы уничтожения конфиденциальной биометрической информации должны однозначно отображаться так, чтобы пользователь не мог их спутать с другими, менее опасными режимами работы.

9.2.2 Критические переключатели режимов должны быть выполнены с дублированием, требованием подтверждения переключения, исключающим случайную инициализацию опасных режимов.

10 Перечень угроз и способов обеспечения информационной безопасности при применении средств высоконадежной биометрической аутентификации

10.1 Угрозы информационной безопасности для средств высоконадежной биометрической аутентификации

10.1.1 Компрометация тайного биометрического образа человека на физическом уровне.

Например, малогабаритные средства подслушивания могут перехватить голосовой пароль пользователя или миниатюрные средства наблюдения могут перехватить тайный рукописный пароль пользователя.

10.1.2 Перехват тайного электронного образа человека в виде его биометрических данных или в виде вектора его биометрических параметров.

Подмена или модификация ПО обработки биометрической информации позволяет злоумышленнику получить (скомпрометировать) тайный электронный биометрический образ человека. Человек не может почувствовать подмену, если он не обеспечен специальными механизмами контроля целостности ПО и функций вычислительных процессов, идущих параллельно с биометрической аутентификацией.

10.1.3 Перехват криптографического ключа или длинного пароля.

10.1.4 Случайный подбор тайного биометрического образа на физическом уровне.

10.1.5 Случайный подбор электронного тайного биометрического образа.

10.1.6 Случайный подбор криптографического ключа или длинного пароля.

10.1.7 Извлечение конфиденциальной информации из структуры и параметров преобразователя «биометрия-код».

10.1.8 Саботаж и нелояльность пользователя при обучении биометрической системы.

10.1.9 Сговор.

10.1.10 Некорректное поведение администратора безопасности системы.

10.1.11 Неадекватная оценка уровня защищенности, обеспечиваемого биометрическим средством высоконадежной аутентификации.

10.1.12 Потеря доступности в случае утраты и существенного искажения биометрического образа легального пользователя из-за травмы, болезни, приема лекарств, опьянения, стресса.

10.2 Для каждой типовой угрозы информационной безопасности средств высоконадежной биометрической аутентификации может быть противопоставлена типовая политика безопасности, снижающая эффективность атак, реализующих соответствующую угрозу.

10.2.1 Компрометация физического биометрического образа человека может быть снижена за счет проведения биометрической аутентификации только в контролируемой зоне и в зоне проведения специализированных организационно-технических мероприятий.

Примеры

1 Вероятность реализации угрозы компрометации рукописного пароля может быть снижена за счет гашения экрана карманного компьютера при воспроизведении рукописного пароля.

2 За счет использования ларингофона с сохранением в тайне места его контакта с телом при аутентификации по голосу может быть снижена вероятность реализации угрозы компрометации голосового пароля.

3 Вероятность реализации угрозы компрометации тайного биометрического физического образа человека может быть снижена за счет периодической смены тайного биометрического образа (биометрического пароля) пользователя по аналогии со сменой обычных паролей.

10.2.2 Компрометация электронного биометрического образа может быть снижена путем контроля целостности используемого ПО и действий (аудита) вычислительных процессов, идущих параллельно процедурам биометрической аутентификации. Возможен частичный или полный перенос всех биометрических и криптографических операций в специализированную вычислительную среду (чип-брелок с флеш-памятью и собственным процессором). Компрометация тайного биометрического образа человека может быть снижена за счет периодической смены тайного биометрического образа (биометрического пароля) пользователя по аналогии со сменой обычных паролей.

10.2.3 Перехват криптографического ключа (длинного пароля) может быть снижен или исключен путем использования специализированной вычислительной среды, контроля целостности программ, контроля характеристик и действий параллельных вычислительных процессов. При дистанционной биометрико-криптографической аутентификации, осуществляемой по открытым каналам связи, необходимо использовать специальные криптопротоколы, осуществляющие аутентификацию с участием секрета (ключа, пароля), но без их прямого предъявления.

10.2.4 Случайный подбор тайного биометрического образа на физическом уровне может быть уменьшен за счет ограничения числа предоставляемых пользователю попыток аутентификации и за счет увеличения информативности биометрического образа (увеличения числа слов рукописного пароля и числа букв в слове, введения обратных росчерков, тренировок по стабильному написанию рукописного пароля).

10.2.5 Случайный подбор электронного биометрического образа может быть уменьшен путем увеличения сложности преобразователя «биометрия-код», например увеличением числа входов и выходов искусственной нейронной сети преобразователя, увеличением числа слоев нейронов и числа связей у каждого нейрона преобразователя. Это эквивалентно росту сложности алгоритма защиты и появлению соответствующих гарантий стойкости защиты. Кроме того, сам нейросетевой преобразователь может

быть сделан недоступным для злоумышленников, например может быть введен запрет на вынос средств биометрико-нейросетевой аутентификации с защищенной территории.

10.2.6 Случайный подбор криптографического ключа или длинного пароля может быть уменьшен до заданного значения за счет увеличения длины ключа (пароля) с соблюдением правил их генерации.

10.2.7 Извлечение конфиденциальной информации из таблиц описания нейронной сети преобразователя «биометрия-код» может быть уменьшен за счет:

- ограничения доступа к таблицам;
- увеличения размерности таблиц;
- генерирования уникальной конфигурации связей нейросети преобразователя для каждого пользователя.

10.2.8 Саботаж и нелояльность пользователя при обучении биометрического средства (искусственной нейронной сети) могут быть снижены, если средство имеет ПО автоматизированного самотестирования и предсказания ожидаемой стойкости защиты. Тогда попытки нелояльных пользователей скомпрометировать средство будут выявлены на этапе ее обучения и тестирования. Средство не должно позволять себя скомпрометировать при обучении, сообщая администратору безопасности о неспособности пользователя или его нежелании иметь биометрическую защиту заданного политикой безопасности уровня.

10.2.9 Угроза сговора (намеренная передача своей биометрии злоумышленникам) может быть снижена при аутентификации по длинному составному ключу (паролю), каждая часть которого связана своей искусственной нейронной сетью с разными пользователями. Группа пользователей и администратор безопасности могут создать общий ключ только совместными усилиями, контролируя друг друга.

10.2.10 Некорректное поведение администратора безопасности уменьшается при отсутствии централизованного хранения тайных биометрических образов конкретных пользователей и использовании при аутентификации протоколов, построенных на асимметричной аутентификации (например, с использованием ЭЦП, когда открытый ключ пользователя известен администратору, личный ключ пользователя администратору неизвестен).

10.2.11 Неадекватная оценка уровня защищенности, обеспечиваемого биометрическим средством защиты, уменьшается путем статистического тестирования средства, его сертификации, профилирования по ГОСТ Р ИСО/МЭК 15408-3. Кроме того, необходимо контролировать уровень ошибок подсистемы тестирования и прогнозирования.

10.2.12 Потеря доступности из-за утраты и существенного искажения биометрического образа легального пользователя может быть ослаблена или снижена за счет дублирования биометрической аутентификации классическими процедурами аутентификации через обладание ключом или знанием длинного пароля. При этом ключ или пароль хранятся в сейфе, а доступ через них является нештатным. Нештатный доступ осуществляется при травмах пользователя, нахождении его в стрессовом состоянии, опьянении, под воздействием психотропных препаратов. Рекомендуется введение в штатные средства аутентификации выходных проверок на соответствие полученного ключа действительному ключу, исключающих компрометацию ключа (например, через контроль значения эталонной хэш-функции полученного ключа). Допускается введение в штатные средства биометрической аутентификации средств индикации близости полученного ключа к действительному ключу, не содержащих информации о самом ключе. Допускается введение в штатные средства аутентификации автоматических средств перебора кодов, близких к ключу (паролю), способных проверять ограниченную часть ключевого поля за приемлемые для пользователя интервалы времени (например, 10^{-12} часть реального ключевого поля за один час рабочего времени).

10.3 Меры для обеспечения безопасного использования средств высоконадежной биометрической аутентификации

10.3.1 Программное и аппаратное обеспечение средств биометрической аутентификации должно быть физически защищено или находиться на контролируемой территории или должна регулярно осуществляться проверка целостности их ПО. Целостность программного и аппаратного обеспечения может быть обеспечена дублированием стандартных аппаратных средств ввода информации и дублированием программных средств биометрико-нейросетевой обработки. Дубликаты следует использовать при обнаружении нарушений целостности программных средств или обнаружении неисправности стандартных аппаратных средств ввода биометрической информации и ее обработки.

10.3.1.1 Использование механизмов высоконадежной биометрико-нейросетевой аутентификации без физической защиты вне контролируемой зоны возможно только при условии обеспечения гарантий целостности программных и аппаратных фрагментов средств защиты и условии сохранения в тайне предъявляемого биометрического образа.

10.3.1.2 Использование механизмов высоконадежной биометрико-нейросетевой аутентификации в рамках контролируемой зоны предпочтительно, так как повышает уровень безопасности из-за снижения вероятности компрометации биометрического образа пользователя и снижения вероятности подмены подлинного ПО на модифицированное.

10.3.2 Предполагается, что в отношении персонала справедливо следующее: для управления должен быть назначен компетентный администратор, пользователи лояльно относятся к биометрической защите и добросовестно выполняют инструкции. У пользователей и администратора безопасности нет личной неприязни. Пользователи находятся в нормальном психологическом и физическом состоянии.

11 Правила приемки (поставки)

11.1 Производитель СВБА должен документировать процедуры поставки средств высоконадежной биометрической защиты от НСД или ее части, а также вести строгий учет поставок, рекламаций, атак, обнаруженных пользователями.

11.2 Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при легальном распространении ПО средств высоконадежной биометрической защиты от НСД.

11.2.1 Производитель должен предоставить руководство администратора.

Руководство администратора должно содержать:

- описание функций администрирования и интерфейсов ВБА, доступных администратору безопасности;
- описание безопасного способа управления СВБА;
- предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации;
- описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, их безопасные значения;
- описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности и сущностей, контролируемых биометрико-криптографическими механизмами аутентификации.

11.2.1.1 Руководство администратора должно быть согласовано со всей технической документацией, поставляемой производителем.

11.2.2 Производитель должен предоставить руководство пользователя.

Руководство пользователя должно содержать:

- описание функций и интерфейсов, доступных пользователям СВБА, не связанным с администрированием;
- описание применения всех потенциально доступных пользователям функций СВБА (обучения, переобучения, тестирования, предсказания ожидаемого качества, смены ключа или длинного пароля, проверки целостности ПО, контроля близости выработанного ключа к действительному его значению);
- все предупреждения относительно доступных для пользователя функций и привилегий, которые следует контролировать в безопасной среде (нарушение целостности, низкое качество обучения, низкий уровень стойкости биометрической защиты).

11.2.2.1 В руководстве пользователя должны быть четко определены все обязанности пользователя, необходимые для безопасной эксплуатации СВБА, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности СВБА.

11.2.2.2 Руководство пользователя должно быть согласовано со всей иной документацией, поставляемой разработчиком.

11.2.2.3 Руководство пользователя может быть снабжено описанием типовых ошибок пользователей СВБА и последствий этих ошибок.

11.3 Процедуры установки, генерации, запуска, процедуры обучения

11.3.1 Производитель должен документировать процедуры, необходимые для безопасной установки, генерации и запуска ПО средства высоконадежной биометрической аутентификации.

Документация в обязательном порядке должна содержать:

- описание последовательности действий, необходимых для безопасной установки, генерации, запуска, обучения ПО средства высоконадежной биометрической аутентификации;

- описание процедур аварийного входа в систему из-за временной или полной утраты пользователем своего тайного биометрического образа (стресс, травмы, болезнь);

- описание процедур, позволяющих пользователю самостоятельно оценивать стойкость средства высоконадежной биометрической защиты на образах «Чужой»;

- описание процедур, позволяющих пользователю самостоятельно оценивать стойкость средства высоконадежной биометрической аутентификации при его обучении на примерах личных биометрических образов пользователя.

12 Требования к тестированию (испытаниям)

12.1 Разработчик должен представлять планы тестирования средств высоконадежной биометрической аутентификации пользователей во всех режимах ее эксплуатации при привлечении всех состояний переключателей интерфейсов управления. План или планы тестирования должны обеспечивать полноту покрытия всех возможных состояний продукта СВБА. Комментарии к планам тестирования должны содержать обоснование необходимости проведения каждого теста с вариантами интерпретации итоговых результатов тестирования.

12.2 Проверка вероятности ошибочного отвержения «Своего» осуществляется пользователем самостоятельно на собственных данных в соответствии с ГОСТ Р 50779.10. Вычисление вероятности ошибок первого рода осуществляется на выборке не менее чем из 50 различных образов «Свой».

12.3 Проверка качества выходного «белого шума» преобразователя «биометрия-код»

Проверка качества выходного белого шума преобразователя «биометрия-код» осуществляется через контроль:

- близости к равновероятным состояний «0» и «1» во всех разрядах выходного кода при подаче на вход преобразователя случайных биометрических образов «Чужой»; допустимые отклонения вероятностей должны находиться в пределах $(0,5 \pm 0,1)$;

- значений парных коэффициентов корреляции, которые должны иметь наиболее вероятное нулевое значение, допустимо среднее значение модулей коэффициентов парной корреляции — не более 0,15 при статистической выборке в 300 примеров образов «Чужой», не знающий пароля; рекомендуется проверять не менее 100 выбранных случайно пар разрядов выходных кодов;

- значений групповых коэффициентов корреляции. Коэффициенты групповой корреляции должны иметь нулевое значение, допустимое среднее значение модулей коэффициентов групповой корреляции не более 0,15 при статистической выборке в 300 примеров образов «Чужой», не знающий пароля; рекомендуется проверять не менее 100 выбранных случайно групп из 3, 4, 5 разрядов выходных кодов;

- математического ожидания значений меры Хемминга расхождения случайных кодов от случайных образов «Чужой» и кода ключа «Свой». Математическое ожидание должно быть близко к половине длины ключа (пароля); допускается не более чем 5 % отклонение математического ожидания расстояния меры Хемминга от половины длин выходных кодов на статистической выборке не менее 300 случайных входных биометрических образов «Чужой», не знающий пароля.

12.4 Проверка стойкости средств высоконадежной биометрической защиты от НСД к атакам подбора (вероятностей ошибок второго рода)

12.4.1 Стойкость средств высоконадежной биометрической защиты от НСД к атакам подбора проверяют путем ввода случайных данных на входы обученного преобразователя «биометрия-код» до первого совпадения выходного кода преобразователя с ключом (паролем) пользователя. Подсчитывают число осуществленных попыток подбора. При тестировании допускается ослабление биометрической защиты через подстановки на часть входов преобразователя «биометрия-код» биометрических данных подлинного пользователя «Свой». Полученную оценку вероятности ошибки второго рода ослабленной системы рекомендуется скорректировать, возведя в степень отношение числа всех входов преобразователя к числу тестируемых (подбираемых) входов. При ослаблении средства в k раз рекомендуется осуществлять k^2 тестирований, каждое из которых проверяет различные комбинации входов. Полученные результаты усредняют.

12.4.2 Ускоренную проверку стойкости средств высоконадежной биометрикой защиты от НСД к атакам подбора проводят путем подстановки случайных входных биометрических образов «Чужой» на все входы обученного преобразователя биометрии в код ключа (пароля). При этом рекомендуется контролировать значение среднеквадратического отклонения и математического ожидания меры Хемминга расхождения случайных выходных кодов «Чужой» и кода ключа (пароля) пользователя «Свой».

12.4.2.1 При значительных отклонениях математического ожидания меры Хемминга расхождения случайных выходных кодов «Чужой» и кода ключа (пароля) пользователя «Свой» от половины длин этих кодов, для прогноза стойкости средства защиты от НСД рекомендуется использовать гипотезу о биномиальном распределении значений меры Хемминга.

12.4.2.2 При незначительных (менее 5 %) отклонениях математического ожидания меры Хемминга расхождения случайных выходных кодов «Чужой» и кода ключа (пароля) пользователя «Свой» от половины длин этих кодов для прогноза стойкости средства защиты от НСД рекомендуется использовать гипотезу о нормальном законе распределения значений меры Хемминга.

12.5 Проверка остаточной стойкости средств высоконадежной биометрической защиты от НСД при скомпрометированном биометрическом образе осуществляется подготовленными людьми, которым предоставлены технические средства для изучения и имитации биометрических образов «Свой». Результаты тестирования обрабатывают в соответствии с требованиями ГОСТ Р 50779.21 или исходя из гипотезы биномиального распределения значений выходных кодов преобразователя «биометрия-код».

Приложение А
(справочное)

Таблицы рекомендуемых длин кодов ключей (паролей), используемых при совмещении нескольких биометрических технологий

Таблица А.1 — Рекомендуемые интервалы выбора длины ключей (паролей) при совместном использовании разнотипных биометрических образов

Наименование биометрической технологии	Стойкость к атакам подбора	Минимальная длина ключа или пароля, бит	Максимальная длина ключа или пароля, бит
Анализ кровеносных сосудов глазного дна	От 10^8 до 10^{12}	27	40
Анализ радужной оболочки глаза	От 10^6 до 10^9	20	30
Двухмерный и трехмерный анализ геометрических особенностей лица в видимом и инфракрасном спектрах света	От 10^2 до 10^4	7	14
Анализ особенностей геометрии ушных раковин	От 10^2 до 10^3	7	10
Анализ особенностей голоса	От 10^2 до	7	Нет ограничений
Анализ особенностей папиллярного рисунка одного пальца	От 10^4 до 10^{13}	12	39
Анализ геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони	От 10^2 до 10^5	7	17
Анализ рисунка кровеносных сосудов, складок кожи тыльной стороны ладони	От 10^2 до 10^3	7	10
Анализ рукописного почерка	От 10^2 до	7	Нет ограничений
Анализ клавиатурного почерка	От 10^2 до	7	Нет ограничений
Анализ геометрических соотношений частей тела	От 10^3 до 10^6	10	20
Анализ особенностей походки	От 10^1 до 10^3	4	10

Таблица А.2 — Рекомендуемые длины ключей (паролей) для среднестатистического пользователя в зависимости от числа букв биометрического пароля или от информативности тайного биометрического образа (данные ФГУП «ПНИЭИ» 2006 г.)

Число букв (цифр) в пароле, образующем биометрический образ без учета пробелов между словами	Длина ключа (пароля), получаемого из рукописного пароля, бит	Длина ключа (пароля), полученного из голосового пароля, бит	Длина ключа (пароля), полученного из динамических параметров клавиатурного почерка, бит
4	32	10	------
5	40	13	------
6	48	16	------
7	56	18	------
8	64	21	------
9	72	23	------
10	80	26	------
12	96	31	------

Окончание таблицы А.2

Число букв (цифр) в пароле, образующем биометрический образ без учета пробелов между словами	Длина ключа (пароля), получаемого из рукописного пароля, бит	Длина ключа (пароля), полученного из голосового пароля, бит	Длина ключа (пароля), полученного из динамических параметров клавиатурного почерка, бит
14	112	36	-----
16	128	42	7
18	144	47	8
20	160	52	10
24	192	64	11
26	224	76	14
32	256	88	17
36	288	100	20
40	320	112	23

Примечания

1 В зависимости от стабильности и уникальности биометрического образа конкретного человека длина его ключа может сокращаться в три раза или увеличиваться до трех раз. Рекомендуется уточнять приведенные цифры для каждого конкретного биометрического образа через использование встроенного в биометрическое приложение механизмов тестирования и прогнозирования ожидаемой стойкости.

2 Для преобразователей «биометрия-код» эффективная длина ключа может составлять от 10 % до 30 % реальной длины выходного биометрического ключа на выходах нейронной сети.

Таблица А.3 — Рекомендуемые длины ключей (паролей) для среднестатистического анонимного пользователя в зависимости от числа особых точек в учитываемом фрагменте рисунка отпечатка пальца (данные ФГУП «ПНИЭИ» 2005 г.)

Число особенностей в учитываемом фрагменте рисунка отпечатка	Вероятность удачи при подборе с первой попытки	Рекомендуемая длина бинарного кода ключа, бит
16	$10^{-5,6}$	17
18	$10^{-6,3}$	19
20	10^{-7}	21
22	$10^{-7,7}$	23
24	$10^{-8,4}$	25
26	$10^{-9,1}$	27
28	$10^{-9,8}$	29
30	$10^{-10,5}$	31
32	$10^{-11,2}$	33
34	$10^{-11,9}$	35
36	$10^{-12,6}$	37
38	$10^{-13,3}$	39

УДК 001.4:025.4:006.354 ОКС 01.040.01 Т00

Ключевые слова: техническая защита информации, биометрическая аутентификация, преобразование биометрии в ключ (пароль) доступа

Редактор *О.В. Гелемеева*
Технический редактор *Л.А. Гусева*
Корректор *М.С. Кабашова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 08.02.2007. Подписано в печать 05.03.2007. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 2,79. Уч.-изд. л. 2,50. Тираж 350 экз. Зак. 171. С 3759.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.

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

Набрано во ФГУП «Стандартинформ» на ПЭВМ.
Отпечатано в филиале ФГУП «Стандартинформ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru