ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52633.3— 2011

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

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 Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 684-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

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

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 2
5 Общие положения 2
5.1 Распределение взаимного доверия 2
5.2 Учет влияния структуры преобразователя «биометрия-код» при его тестировании на стойкость к атакам подбора 3
6 Тестирование средств высоконадежной биометрической аутентификации при высоком уровне взаимного доверия 3
6.1 Тестирование с использованием малых баз биометрических образов «Чужой» 3
6.2 Тестирование с использованием баз случайных биометрических образов «Чужой» среднего размера 5
7 Тестирование преобразователя «биометрия-код» при низком уровне взаимного доверия между донором биометрии и владельцем средства биометрической аутентификации 7
7.1 Тестирование стойкости к атакам подбора с использованием только кодов-откликов биометрического преобразователя, полученных на недоступной для проверяющего базе тестовых биометрических образов 7
7.2 Обнаружение факта модификации преобразователя «биометрия-код» 7
7.3 Обнаружение факта включения пользователем защитных механизмов связывания внутренних данных преобразователя «биометрия-код» 8
Приложение А (справочное) Пример направленного подбора параметров биометрического образа путем селекции наиболее близких образов и их морфинг-размножение в нескольких поколениях 9
Приложение Б (справочное) Результат оценки остаточной стойкости почти полностью скомпрометированного биометрического образа путем размножения образов «Свой» мутациями 10
Приложение В (справочное) Пример изменения плотности распределения значений критерия Хэмминга при включении/отключении защитных механизмов связывания внутренних данных в одном слое нейронов преобразователя «биометрия-код» 11

Введение

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

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

Тестирование средств биометрической аутентификации проводится с использованием баз биометрических образов «Свой» и «Чужой», размеры которых являются достаточными для подтверждения характеристик тестируемых средств.

Наиболее сложной частью задачи является тестирование стойкости обученных преобразователей «биометрия-код» к атакам подбора. Как правило, создать достаточно большой объем естественных биометрических образов по требованиям ГОСТ Р 52633.1 технически невозможно. По этой причине приходится многократно увеличивать размеры тестовой базы биометрических образов за счет синтетических биометрических образов, созданных по ГОСТ Р 52633.2.

В общем случае задача автоматизированного тестирования стойкости преобразователя «биометрия-код» требует формирования очень больших баз тестовых биометрических образов и применения высокопроизводительных вычислительных средств с большим объемом памяти. Областью применения настоящего стандарта не является общий случай перебора всех возможных биометрических образов, настоящий стандарт распространяется только на тестирование программных средств аутентификации, в которых предусмотрена возможность реализации специальных условий упрощения задачи тестирования, а также предусмотрены специальные тестовые режимы наблюдения внутренних данных преобразователя «биометрия-код». Для средств высоконадежной биометрической аутентификации, выполненных с аппаратной защитой внутренних данных, или для программных средств, не предоставляющих доступа к своим внутренним данным в специальных режимах тестирования, процедуры настоящего стандарта не могут дать численной оценки стойкости к атакам подбора.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора

Information protection. Information protection technology. The high reliability biometric protection means endurance testing from matching attacks

Дата введения — 2011—12—01

1 Область применения

Настоящий стандарт распространяется на автоматизированные системы тестирования средств высоконадежной биометрической аутентификации, выполненные по ГОСТ Р 52633.0, которые осуществляют имитацию атак подбора с использованием баз естественных биометрических образов, сформированных по ГОСТ Р 52633.1 и размноженных за счет синтетических биометрических образов, полученных по ГОСТ Р 52633.2. Настоящий стандарт распространяется на программные средства биометрической аутентификации или программные эмуляторы аппаратных средств аутентификации, предусматривающие доступность их внутренних данных в специальном тестовом режиме.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50779.10 Статистические методы. Вероятность и основы статистики. Термины и определения

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

ГОСТ Р 52633.1 Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 52633.0, ГОСТ Р 52633.1 и ГОСТ Р 52633.2, а также следующий термин с соответствующим определением:

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

4 Обозначения и сокращения

В настоящем стандарте использованы следующие обозначения и сокращения:

N — размер используемой для тестирования базы образов «Чужой»;

h — значение критерия Хэмминга;

n — длина выходного кода тестируемого преобразователя «биометрия-код»;

$E(.)$ — оператор вычисления математического ожидания по ГОСТ Р 50779.10;

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

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

ПБК — преобразователь «биометрия-код».

5 Общие положения

5.1 Распределение взаимного доверия

ПБК могут тестироваться при разном уровне доверия между донором биометрии, владельцем средства биометрической аутентификации (тестирования). Различают три уровня взаимного доверия:

- полное взаимное доверие между донором биометрии и владельцем средства биометрической аутентификации (тестирования);
- частичное доверие между донором биометрии и владельцем средства биометрической аутентификации (тестирования);
- отсутствие доверия донора биометрии к владельцу средства биометрической аутентификации (тестирования).

5.1.1 Полное доверие со стороны донора биометрии

Полное взаимное доверие возникает в случае, если донор биометрии одновременно является владельцем средства биометрической аутентификации со встроенным блоком самотестирования. Тогда донор биометрии способен после каждого обучения нейросетевого ПБК самостоятельно протестировать его уровень стойкости к атакам подбора. Однако при этом донор биометрии должен доверять встроенному в средство биометрической аутентификации блоку самотестирования. При полном доверии затраты на тестирование минимальны, так как все биометрические данные известны тестирующему.

5.1.2 Доверие к встроенному в средство аутентификации блоку самотестирования

Донор биометрии доверяет встроенному блоку самотестирования, если производитель средства аутентификации дает информацию о погрешности блока самотестирования. Заявленная производителем погрешность показаний блока самотестирования должна быть подтверждена внешним независимым тестированием с использованием тестовых баз биометрических образов достаточного размера.

5.1.3 Частичное доверие со стороны донора биометрии

Ситуация частичного доверия возникает в случае, если донор биометрии не является владельцем средства биометрической аутентификации (тестирования). В этом случае донор биометрии сохраняет за собой право на обеспечение конфиденциальности, анонимности, обезличенности своих биометрических данных и кода доступа. Тем не менее владелец средства биометрической аутентификации должен иметь возможность тестировать стойкость к атакам подбора ПБК донора биометрии (пользователей его средства). Средства тестирования должны быть способны работать в режиме сохранения анонимности, конфиденциальности, обезличенности персональных биометрических данных донора биометрии.

Частичное доверие со стороны донора биометрии к владельцу средства аутентификации (тестирования) существенно усложняет условия тестирования.

5.1.4 Тестирование при полном отсутствии доверия со стороны донора

Затраты на тестирование существенно зависят от начальной информации о биометрических данных и коде доступа. При полном отсутствии начальной информации о ПБК тестирующий должен перебрать множество биометрических образов, которые когда-либо могут быть предъявлены, и найти или синтезировать биометрический образ «Свой». Режим отсутствия доверия (полного отсутствия дополнительной информации о защищаемой биометрии и коде доступа) является наиболее сложным для тестирования. Этот режим требует значительных затрат материальных ресурсов на формирование больших баз биометрических образов по ГОСТ Р 52633.1, использование высокопроизводительных средств автоматизированного размножения биометрических образов по ГОСТ Р 52633.2 и последующего тестирования путем прямого перебора всех возможных вариантов биометрических образов. Этот режим тестирования в рамках настоящего стандарта не рассматривается, так как не позволяет получить достоверных численных результатов без привлечения высокопроизводительных вычислительных средств автоматизации подбора биометрических образов.

5.2 Учет влияния структуры преобразователя «биометрия-код» при его тестировании на стойкость к атакам подбора

5.2.1 Структура ПБК, использующего входные биометрические параметры высокого качества

Если ПБК использует прямое преобразование биометрических параметров в код через их сравнение с границами распределения параметров «Свой», то тестирование проводится без изменения его структуры. Тестирование проводится наблюдением выходных кодов, порождаемых входными биометрическими параметрами образов «Чужой».

5.2.2 Структура ПБК, использующего входные биометрические параметры среднего качества

Если ПБК осуществляет повышение качества биометрических параметров с помощью одного слоя искусственных нейронов или иного однослойного нечеткого механизма обогащения данных, то тестирование проводится без изменения его структуры. Тестирование проводится наблюдением выходных кодов ПБК, порождаемых входными биометрическими параметрами образов «Чужой».

5.2.3 Изменение структуры ПБК, использующего входные биометрические параметры низкого качества

Если ПБК осуществляет преобразование многослойной нейронной сетью или с помощью иных многослойных нечетких механизмов обогащения данных, то тестирование проводится с таким изменением его структуры, которое позволяет наблюдать коды на выходе каждого слоя. Тестовый режим должен обеспечивать контроль кодов на выходах нейронов или на выходах иных нечетких механизмов обогащения данных каждого слоя ПБК. При этом проводят тестирование выходных кодов каждого слоя ПБК. Итогом тестирования является наихудший показатель стойкости к атакам подбора.

5.2.4 Изменение структуры ПБК, использующего механизмы защиты от наблюдения внутренних данных

Если ПБК имеет сложную структуру, связывающую через дискретные операции (хэширования, битовые операции сложения по модулю два или иные операции) между собой внутренние данные, то его структура перед тестированием должна быть упрощена за счет отключения механизмов защиты от наблюдения внутренних данных. Тестовый режим должен обеспечить отсутствие влияния выходных кодов уже сработавших элементов ПБК на другие элементы ПБК через отключение соответствующих механизмов защиты от наблюдения внутренних данных.

6 Тестирование средств высоконадежной биометрической аутентификации при высоком уровне взаимного доверия

6.1 Тестирование с использованием малых баз биометрических образов «Чужой»

6.1.1 Требования к малым базам биометрических образов «Чужой»

Для тестирования обученного ПБК необходимо иметь не менее 128 примеров различных естественных биометрических образов «Чужой», которые ранее не были использованы при обучении тестируемого ПБК. Используемые при тестировании биометрические образы должны быть независимыми и формироваться по ГОСТ Р 52633.1.

Контроль уровня независимости образов «Чужой» осуществляется взаимным сравнением их кодов на выходе тестируемого преобразователя по критерию Хэмминга. Следует вычислять критерий Хэмминга между каждым из кодов-откликов «Чужой». В малой тестовой базе не должно быть пар биометрических образов, чьи выходные коды по критерию Хэмминга выпадают из интервала $\left[\frac{n-\sqrt{n}}{2}, \frac{n+\sqrt{n}}{2}\right]$, где n — число разрядов в выходном коде тестируемого ПБК.

6.1.2 Общая схема тестирования с использованием малой тестовой базы

При тестировании ПБК биометрические образы малой тестовой базы подаются на входы ПБК однократно в произвольном порядке. Блок-схема тестирования приведена на рисунке 1. В процессе тестирования кодовые отклики ПБК сравниваются с кодом «Свой», и строится распределение значений показателей критерия Хэмминга — $p(h)$.

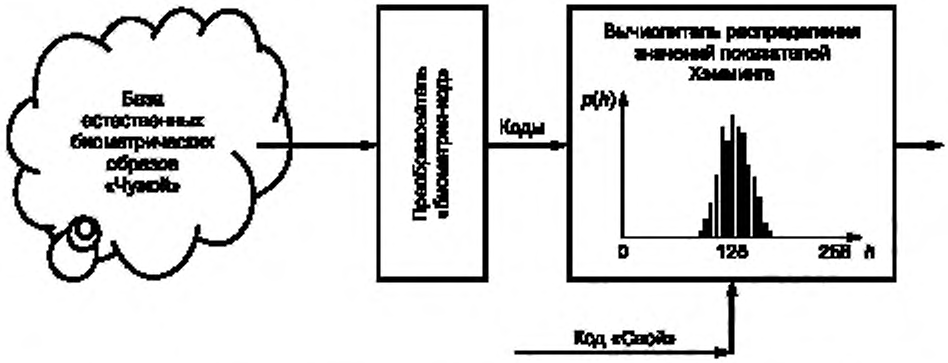


Рисунок 1 — Блок-схема тестирования с использованием базы естественных биометрических образов «Чужой»

По форме и параметрам распределения значений показателя критерия Хэмминга осуществляют прогнозирование появления нулевого значения. Вероятность появления нулевого значения критерия Хэмминга соответствует коллизии — ситуации появления кодового отклика «Свой» при предъявлении одного из образов «Чужой».

6.1.3 Вычисление статистических параметров распределения значений критерия близости Хэмминга

Распределение значений показателя Хэмминга является дискретным, однако при больших значениях длины выходного кода (для кодов длиной более 32 бит) эффектом дискретности следует пренебречь и рассматривать описывающую функцию дискретного распределения как непрерывное распределение с некоторыми статистическими моментами.

По полученной выборке кодов-откликов вычисляют математическое ожидание значений показателя — критерия Хэмминга — $E(h)$ и среднеквадратическое отклонение показателей критерия Хэмминга — $\sigma(h)$.

6.1.4 Оценка стойкости к атакам подбора при использовании малых тестовых баз

Приближенная оценка вероятности ошибки второго рода — P_2 тестируемого ПБК оценивается в рамках гипотезы нормальности закона распределения значений показателей критерия Хэмминга:

$$P_2 \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{E(h)/\sigma(h)} \exp(-t^2/2)dt. \qquad (1)$$

Стойкость к атакам подбора $P_{2,\text{Ост}}^{-1}$ оценивают как обратную величину вероятности ошибки второго рода.

Примечание — Реальное распределение значений показателей критерия Хэмминга может существенно отличаться от нормального распределения. В связи с этим прогноз, вычисленный по формуле (1), является приближенным и должен быть скорректирован соответствующей таблицей поправок, учитывающих показатели средней стабильности, уникальности, качества биометрических параметров тестируемого биометрического образа, а также среднее значение модуля парных корреляций.

6.2 Тестирование с использованием баз случайных биометрических образов «Чужой» среднего размера

6.2.1 Требования к средним тестовым базам случайных биометрических образов «Чужой»

Для тестирования средств высоконадежной биометрической аутентификации тестовые базы естественных биометрических образов среднего размера должны содержать от нескольких тысяч до нескольких десятков тысяч естественных биометрических образов. Создание таких баз биометрических образов вполне по силам производителям средств высоконадежной биометрической аутентификации, и это позволяет им самостоятельно тестировать свои средства биометрической аутентификации. Формирование тестовой базы естественных биометрических образов осуществляется по ГОСТ Р 52633.1.

6.2.2 Первый этап тестирования, селекция наиболее близких естественных образов «Чужой» исходного (нулевого) поколения

Первый этап тестирования проводят в соответствии с блок-схемой, представленной на рисунке 2. На первом этапе используют все образы «Чужой», содержащиеся в тестовой базе. Кодовые отклики этих образов упорядочивают по значению критерия расстояния Хэмминга, вычисленного по отношению к коду «Свой».

Из всех образов «Чужой» выбирают 1 % образов с наименьшим показателем критерия Хэмминга, используемых при дальнейшем тестировании.

6.2.3 Морфинг-размножение первого поколения потомков, наиболее близких биометрических образов «Чужой»

После селекции выявленного 1 % наиболее похожих на образ «Свой» образов «Чужой» их размножают через морфинг случайно выбранных пар образов. Морфинг пар образов-родителей выполняют в соответствии с ГОСТ Р 52633.2. Размножение осуществляют до момента, пока размер базы синтетических образов-потомков второго поколения не совпадет с размерами исходной базы естественных биометрических образов первого поколения.

6.2.4 Второй этап тестирования, селекция наиболее близких синтетических образов «Чужой» первого поколения потомков

Второй этап тестирования осуществляют путем предъявления всех синтетических биометрических образов первого поколения на входы тестируемого ПБК. Далее коды-отклики упорядочиваются по критерию Хэмминга, вычисленному по отношению к коду «Свой». Из всех синтетических биометрических образов-потомков первого поколения выделяют 1 % наиболее близких к образу «Свой» образов «Чужой».

6.2.5 Морфинг-размножение наиболее близких синтетических биометрических образов «Чужой» второго поколения потомков

После селекции выявленного 1 % наиболее похожих на образ «Свой» образов «Чужой» на втором этапе тестирования выявленные образы также размножают через морфинг их случайно выбранных пар. Морфинг пар образов-родителей выполняют в соответствии с ГОСТ Р 52633.2. Размножение осуществляют до момента, пока размер базы синтетических образов-потомков второго поколения не совпадет с размерами исходной базы естественных биометрических образов исходного (нулевого) поколения.

6.2.6 Прогнозирование предельных возможностей по подбору используемой базы естественных биометрических образов исходного (нулевого) поколения

Биометрические данные естественных биометрических образов исходного (нулевого) поколения для тестовых баз среднего размера, как правило, не содержат информации, достаточной для подбора входного биометрического образа «Свой» процедурами морфинга. Математическое ожидание критерия расстояния Хэмминга выходных кодов образов-потомков по отношению кода «Свой» уменьшается от поколения к поколению. Однако шаг движения в сторону точки $h = 0,0$ экспоненциально сокращается, сокращается также среднеквадратическое отклонение биометрических параметров образов-потомков в каждом следующем поколении.

Пользуясь экспоненциальной зависимостью снижения значения математического ожидания и среднеквадратического отклонения биометрических данных в последовательности поколений, необходимо спрогнозировать число поколений, позволяющих приблизиться одним из образов-потомков к образу «Свой» на расстояние $\min(h)$. Пример экспоненциальных кривых уменьшения статистических моментов, прогноза числа поколений, необходимых для достижения $\min(h)$, приведен в приложении А.

6.2.7 Первая приближенная оценка стойкости к атакам подбора

В том случае, если значение $\min(h)$ оказывается менее трех среднеквадратических отклонений критерия Хэмминга независимых кодов «белого шума» ($\min(h) \le 3\sigma_{шум}(h)$ бит), допустимо оценивать стойкость тестируемого преобразователя «биометрия-код» к атакам подбора по формуле

$$P_2^{\ 1} \approx N_0 \cdot 10^{2\ k+1}, \tag{2}$$

где N_0 — размер тестовой базы естественных биометрических образов исходного (нулевого) поколения;

k — номер поколения, в котором обнаружен (предсказан) образ-потомок «Чужой», отличающийся от образа «Свой» не более чем на $3\sigma_{шум}(h)$ бит по критерию Хэмминга.

Пример расчета оценки стойкости преобразователя «биометрия-код» при учете двух поколений подбора ($k = 2$) наиболее близкого образа-потомка «Чужой» приведен в приложении А.

Примечание — Для независимых выходных кодов длиной 256 бит «белый шум» имеет среднеквадратическое отклонение критерия Хэмминга 8 бит ($\sigma_{шум}(h) = 8$). Для других длин выходного кода n среднеквадратическое отклонение критерия Хэмминга идеального «белого шума» описывается соотношением $(\sigma_{шум}(h))^2 = n/4$. Для независимых кодов «белого шума» распределение значений критерия Хэмминга соответствует биномиальному закону плотности распределения значений независимых данных.

6.2.8 Размножение старших поколений образов-потомков «Чужой» с использованием мутаций

В том случае, если за два или три поколения образов потомков не удается достичь значения критерия Хэмминга меньше трех среднеквадратических отклонений независимых кодов «белого шума» ($\min(h) < 3\sigma_{шум}(h)$ бит), необходимо увеличение в два или три раза размера тестовой базы естественных биометрических образов исходного (нулевого) поколения N_0. Либо при том же размере N_0 необходимо применить размножение биометрических образов-потомков мутациями по ГОСТ Р 52633.2. Мутациями следует размножать старшие поколения образов-потомков. Соотношение числа образов-потомков, полученных на старших поколениях мутациями и морфингом, оптимизируется самим тестирующим. Критерием оптимальности является уменьшение достигнутого значения $\min(h)$.

6.2.9 Приближенная оценка остаточной стойкости через размножение мутациями образа «Свой»

В том случае, если $\min(h)$ не удается уменьшить менее чем до $3\sigma_{шум}(h)$ бит, следует вычислять оценку стойкости к атакам подбора по формуле

$$P_{2,\,Ост}^{\ 1} \approx N_0 \cdot 10^{2 \cdot k} \cdot P_{2,\,Ост}^{\ 1}, \tag{3}$$

где $P_{2,\,Ост}^{\ 1}$ — остаточная стойкость частично скомпрометированного биометрического образа «Свой», отличающегося от ближайшего синтезированного образа-потомка «Чужой» на величину $\min(h) >> 3\sigma_{шум}(n)$ бит.

Остаточная стойкость частично скомпрометированного биометрического образа «Свой» численно оценивается путем эксперимента, проводимого по блок-схеме, изображенной на рисунке 2.

Численный эксперимент проводят, изменяя значение a от 0,0 % до величины $\frac{\min(h)}{n}$ 100 %. Величину $\frac{\min(h)}{n}$ следует рассматривать как относительное значение уровня компрометации биометрических параметров во время подбора наиболее близкого образа-потомка «Чужой» в последнем поколении.

Если за приемлемое время численного эксперимента, проводимого по блок-схеме, представленной на рисунке 2, не удается обнаружить факт подбора биометрического образа, скомпрометированного на величину $\frac{\min(h)}{n}$, допускается использовать реальные данные, полученные при меньшем значении уровня компрометации биометрического образа «Свой». В этом случае пересчет данных проводят путем их линейной экстраполяции. Пример данных, полученных при численном тестировании стойкости к атакам подбора, приведен в приложении Б.

Вычисления стойкости к атакам подбора по формуле (3) существенно зависят от числа поколений-потомков k. Для исключения неоднозначности вычисления по формуле (3) следует проводить для избыточного числа поколений образов потомков $k = 1, 2, 3,\ldots$ Как результат окончательной оценки принимают результат оценки стойкости к атакам подбора одного из проанализированных поколений образов-потомков.

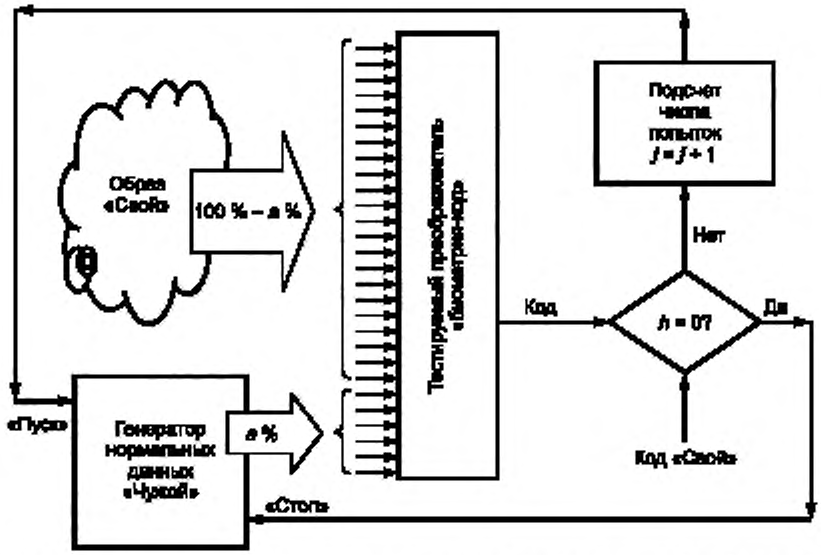


Рисунок 2 — Блок-схема проведения численного эксперимента по оценке остаточной стойкости образа «Свой», скомпрометированного на большую (100 % – *a* %) часть биометрических параметров

7 Тестирование преобразователя «биометрия-код» при низком уровне взаимного доверия между донором биометрии и владельцем средства биометрической аутентификации

7.1 Тестирование стойкости к атакам подбора с использованием только кодов-откликов биометрического преобразователя, полученных на недоступной для проверяющего базе тестовых биометрических образов

Размещение биометрических данных в параметрах обученных ПБК с простейшими структурами (см. 5.1.1, 5.1.2, 5.1.3) потенциально опасно, следовательно, передача ПБК с простейшими структурами сопряжена с риском компрометации биометрии донора и его кода доступа. Если донор биометрии не доверяет владельцу средства биометрической аутентификации, то он не должен предоставлять ему свой ПБК, преобразованный в одну из его простейших структур.

Если принятая политика обеспечения безопасности информационной системы требует от донора биометрии гарантий высокой надежности его биометрической аутентификации, то донор биометрии должен предоставить для внешнего тестирования кодовые отклики обученного ПБК на неизвестных проверяющему тестовых воздействиях. При этом донор биометрии должен переобучить ПБК на неиспользуемом случайном коде доступа «Свой».

Для исключения возможности частичной или полной компрометации биометрического образа «Свой» донор биометрии не предоставляет тестирующему самих тестовых воздействий «Чужой» и не дает информации о своем выходном коде.

Примечание — Переобучение нейросетевого ПБК на иной код или перепрограммирование его выходного кода не влияет на стойкость нейросетевого ПБК к атакам подбора. Переобучение проводят на той же обучающей выборке образов «Свой», но для иного выходного кода. Перепрограммирование проводят путем инвертирования некоторой части разрядов выходного кода без переобучения всего ПБК.

7.2 Обнаружение факта модификации преобразователя «биометрия-код»

7.2.1 Обнаружение факта модификации ПБК путем использования контрольных сумм

Сохраняя конфиденциальность, анонимность и обезличенность своего персонального биометрического образа, а так же конфиденциальность кода доступа «Свой», при необходимости донор биометрии имеет возможность заменить биометрический образ «Свой» или выходной код доступа. При любом из этих изменений изменяются данные ПБК.

Кроме того, донор биометрии может обеспечивать режим своей анонимности, изменяя при каждом сеансе аутентификации связи внутри своего ПБК. Подобные изменения могут быть осуществлены, например, за счет изменения связей нейронной сети и переобучения нового варианта нейронной сети, при этом биометрический образ и код доступа могут оставаться прежними.

Владелец средства биометрической аутентификации или сторонний наблюдатель обнаруживает факт модификации ПБК донора биометрии, например, вычисляя контрольную сумму двоичных данных ПБК и сравнивая ее с эталоном.

7.2.2 Подтверждение факта модификации ПБК, произведенной сменой только кодового отклика преобразователя «биометрия-код» или только сменой связей внутренних биометрических данных ПБК

При обнаружении факта модификации ПБК по 7.2.1 владелец средства биометрической аутентификации должен удостовериться в безопасности модификации. Для этой цели он должен запросить донора биометрии о характере осуществленных им изменений.

Для подтверждения того, что изменен только выходной код ПБК, или того, что код остался прежним, но изменены только связи ПБК, лояльный донор биометрии должен передать проверяющему новые кодовые отклики ПБК на неизвестных проверяющему тестовых образах «Чужой» в соответствии с 7.1.

Имея эту информацию, проверяющий должен убедиться в том, что стойкость ПБК осталась прежней (проверка проводится по 6.1.4), подтвердив, что донор биометрии сохранил образ «Свой», изменив лишь вид ПБК и/или код «Свой» на выходе ПБК.

7.2.3 Подтверждение факта модификации ПБК при изменении донором биометрического образа «Свой»

При изменении донором биометрического образа «Свой» и переобучении ПБК изменяется его стойкость к атакам подбора. Владелец средства биометрической аутентификации должен обнаружить факт изменения стойкости к атакам подбора модифицированного ПБК и, тем самым, сделать вывод о смене донором биометрии его конфиденциального биометрического образа аутентификации. Вывод делается только если донор биометрии предоставил владельцу средства биометрической аутентификации отклики нового ПБК по 7.1. Контроль стойкости к атакам подбора в этом случае проводится в соответствии с 6.1.4.

7.3 Обнаружение факта включения пользователем защитных механизмов связывания внутренних данных преобразователя «биометрия-код»

Так как действительная безопасность высоконадежной биометрической защиты информации связана с сохранением конфиденциальности (анонимности, обезличенности) персонального биометрического образа, то при его хранении необходимо использовать защищенные от наблюдения внутренних данных ПБК со сложной структурой, соответствующей 5.2.4. При этом внешний наблюдатель (например, владелец средства биометрической аутентификации) должен уметь выявлять факт перехода донора биометрии от ПБК с простой структурой к защищенному ПБК со сложной структурой.

Признаком тестирования защищенного ПБК является то, что при тестировании по блок-схеме, представленной на рисунке 1, среднеквадратическое отклонение распределения кодов критерия Хэмминга близко к среднеквадратическому отклонению распределения биномиального закона независимых данных (число степеней свободы у биномиального закона и число выходов преобразователя «биометрия-код» выбираются одинаковыми). При этом изменение кода, с которым сравниваются кодовые отклики защищенного ПБК, не должно приводить к значительному изменению $\sigma(h)$ по сравнению с $\sigma_{шум}(h)$.

Проверку рекомендуется проводить, используя не менее 64 вариантов случайных кодов с последующим усреднение результатов. ПБК относят к защищенным в случае, если выполняется условие

$$\sigma_{шум}(h) < E(\sigma(h)) < 1{,}5\sigma_{шум}(h). \quad (4)$$

Напротив, признаком тестирования открытого биометрического контейнера является то, что вычисленное значение $E(\sigma(h))$ не удовлетворяет условию (4). Для ПБК без защиты от наблюдения внутренних данных правая часть условий (4) не выполняется. Для ПБК с простейшими структурами (с однослойной нейронной сетью или с иным однослойным нечетким механизмом обогащения данных) среднеквадратические отклонения распределения критерия Хэмминга значительно больше, чем отклонения независимых кодов ($\sigma(h) >> 1{,}5\sigma_{шум}(h)$, подробнее см. в примечании к 6.2.7. Пример изменения показателя $\sigma(h)$ для включенного и отключенного механизма защиты приведен в приложении В.

Приложение А
(справочное)

Пример направленного подбора параметров биометрического образа путем селекции наиболее близких образов и их морфинг-размножение в нескольких поколениях

При использовании исходной тестовой базы, состоящей из 3000 естественных биометрических образов, ощутимое приближение синтетических образов к образу «Свой» по значению критерия Хэмминга наблюдается в первых двух поколениях. Кривые функции снижения значений критерия Хэмминга, построенные по экспериментальным данным, приведены на рисунке А.1.

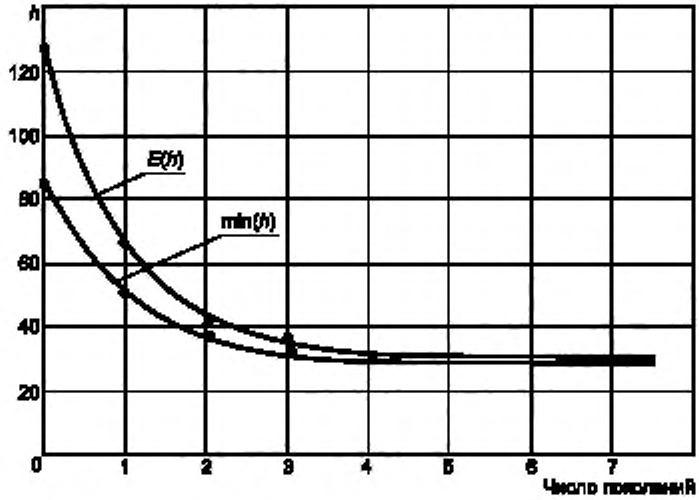


Рисунок А.1 — Экспоненциальные функции снижения значений показателей математического ожидания критерия Хэмминга E(h) и минимального значения критерия Хэмминга min(h) для нескольких поколений подбираемых образов-потомков

В соответствии с рисунком А.1, точки графика, соответствующие третьему и четвертому поколению, попадают на начало пологого участка первой и второй экспонент. Все поколения, попадающие на пологий участок, дают практически неразличимые результаты min(h). Оценка стойкости к атакам подбора производится вычислениями по формуле (4) 6.2.9, исходя из учета только двух поколений приближения, каждая из точек которых дает значительное снижение значения критерия Хэмминга:

$$P_2^{-1} \approx N_0 \cdot 10^{2k} \cdot P_{2,\text{Ост}}^{-1} = 3000 \cdot 10^4 \cdot 18 = 540000000.$$

Приложение Б
(справочное)

Результат оценки остаточной стойкости почти полностью скомпрометированного биометрического образа путем размножения образов «Свой» мутациями

Атака подбора частично скомпрометированного биометрического образа, реализованная по блок-схеме, представленной на рисунке 2, требует малых вычислительных ресурсов, если скомпрометирована большая часть биометрии. Результаты численной реализации атаки на нейросетевой ПБК с 416 входами и 256 выходами показаны на рисунке Б.1, где приведены две разметки оси абсцисс. Верхняя разметка отражает число подбираемых (не скомпрометированных) входов нейросетевого ПБК. Нижняя разметка отражает эквивалентное число подбираемых (не скомпрометированных) выходов нейросетевого преобразователя «биометрия-код».

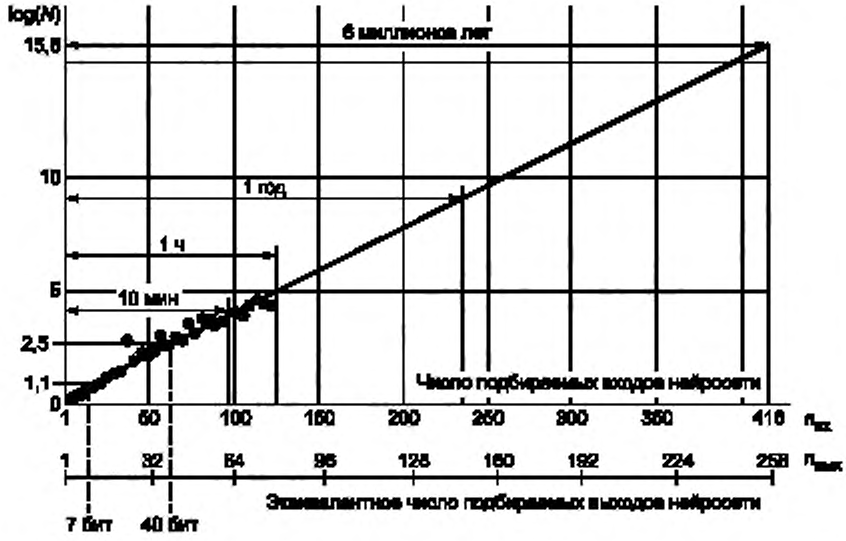


Рисунок Б.1 — Результаты численного эксперимента по подбору биометрических параметров почти полностью скомпрометированного биометрического образа

При почти полной компрометации биометрического образа (скомпрометировано 97 % биометрических параметров, не скомпрометированный остаток ключа 7 бит), на реализацию тестирования требуется менее 10 мин (использовалась обычная персональная вычислительная техника). Во время тестирования осуществлялось 100-кратное повторение подбора 3 % оставшихся неизвестными параметров (каждый подбор проводился для разных входов нейронной сети ПБК, результаты подборов усреднялись).

Приложение В
(справочное)

Пример изменения плотности распределения значений критерия Хэмминга при включении/отключении защитных механизмов связывания внутренних данных в одном слое нейронов преобразователя «биометрия-код»

При переходе к сложной структуре защищенного от наблюдения внутренних данных ПБК график плотности распределения значений критерия Хэмминга сжимается (см. рисунок В.1).

При отключенных защитных механизмах связывания внутренних данных ПБК среднеквадратическое отклонение кодов Хэмминга должно быть использовано для численной оценки стойкости к атакам подбора тестируемого преобразователя. При включенных механизмах связывания данных ПБК среднеквадратическое отклонение кодов Хэмминга не отражает стойкости преобразователя «биометрия-код» и совпадает со среднеквадратическим отклонением биномиального закона распределения независимых значений той же размерности, что и выходная размерность тестируемого ПБК.

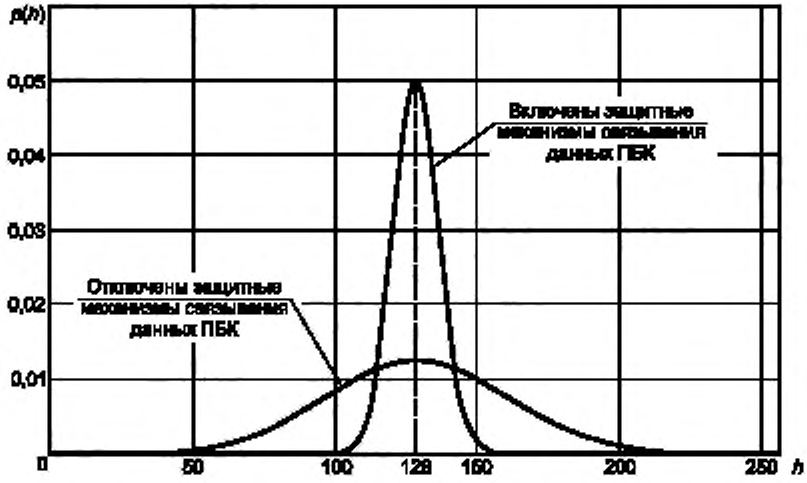


Рисунок В.1 — Две описывающие функции распределения значений критерия Хэмминга при тестировании ПБК с примитивной структурой и защищенного ПБК с 256 выходами

Для биномиального закона распределения 256 независимых данных $\sigma(h) = 8,0$. Если тестирование преобразователя «биометрия-код» на 128 тестовых образах «Чужой» дает для кода «Свой» и N случайных кодов близкие значения: $\sigma_1(h) = 8,14$; $\sigma_2(h) = 7,84$; $\sigma_3(h) = 8,07$;…., то такой ПБК является защищенным.

УДК 681.18:006.354 ОКС 01.040.01

Ключевые слова: защита информации, техника защиты информации, тестирование стойкости, средства высоконадежной биометрической защиты, атаки подбора, биометрические образы естественные и синтетические, поколение образов-потомков

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 08.10.2018. Подписано в печать 12.11.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,50.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru