
ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р .1-202
(проект, первая редакция)

Информационные технологии
БИОМЕТРИЯ
Обнаружение инъекционной атаки
Часть 1
Общие требования

Москва
Российский институт стандартизации

202

ГОСТ Р
(проект, первая редакция)

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.rst.gov.ru)

© Оформление. ФГБУ «Институт стандартизации», 202_

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.....	
2	Нормативные ссылки	
3	Термины и определения	
4	Обозначения и сокращения.....	
5	Характеристики инъекционной атаки.....	
5.1	МИА.....	
5.2	ИИА	
6	Структура методов ОИА	
6.1	Типы методов ОИА	
6.2	МЗМИА.....	
6.3	МЗИИА.....	
6.4	Комбинация нескольких методов ОИА.....	
6.5	Компромисс между безопасностью и удобством использования.....	
	Приложение А (справочное) Противодействие инъекционным атакам в биометрической системе.....	
	Библиография.....	

Введение

Существует девять точек атаки на биометрическую систему общего вида, как показано на рисунке 1. Область применения серии стандартов ГОСТ Р 58624 распространяется только на атаки типа 1, т. е. на атаки, предъявляемые подсистеме сбора биометрических данных с целью вмешательства в работу биометрической системы. Область применения серии стандартов ГОСТ Р 58624 не распространяется на те атаки, которые применяются за пределами интерфейса подсистемы сбора биометрических данных и которые физически не предъявляются встроенному устройству сбора биометрических данных.

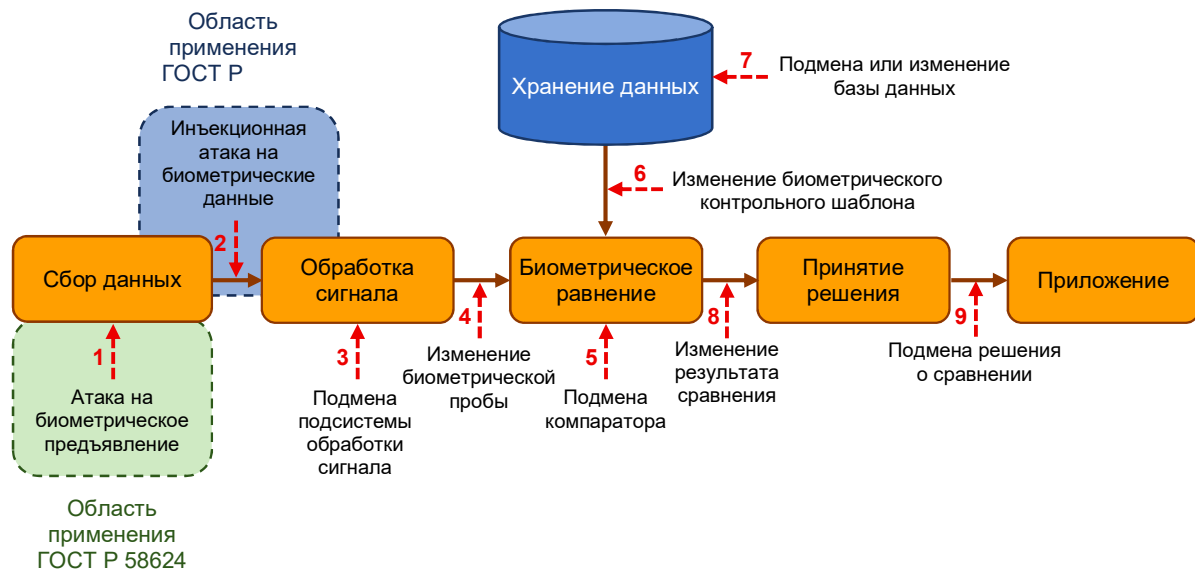


Рисунок 1 – Примеры точек атаки в биометрической системе [1]

Появление средств для удаленной идентификации, основанных на биометрических технологиях и использовании мобильных приложений или приложений веб-браузера, предоставило новые возможности атаки на биометрическую систему. Одной из таких атак является атака типа 2 (см. рисунок 1), которая основана на изменении злоумышленником потока данных.

Серия национальных стандартов «Информационные технологии. Биометрия. Обнаружение инъекционной атаки» посвящена атакам типа 2, которые называются инъекционными атаками. Инъекционная атака заключается во вмешательстве в работу биометрической системы путем подмены исходного биометрического образца, полученного от пользователя с помощью устройства сбора биометрических данных,

другим биометрическим образцом перед выполнением процесса извлечения признаков.

На рисунке 2 показана одна из возможных реализаций подсистемы обнаружения инъекционной атаки в структуре биометрической системы общего вида.

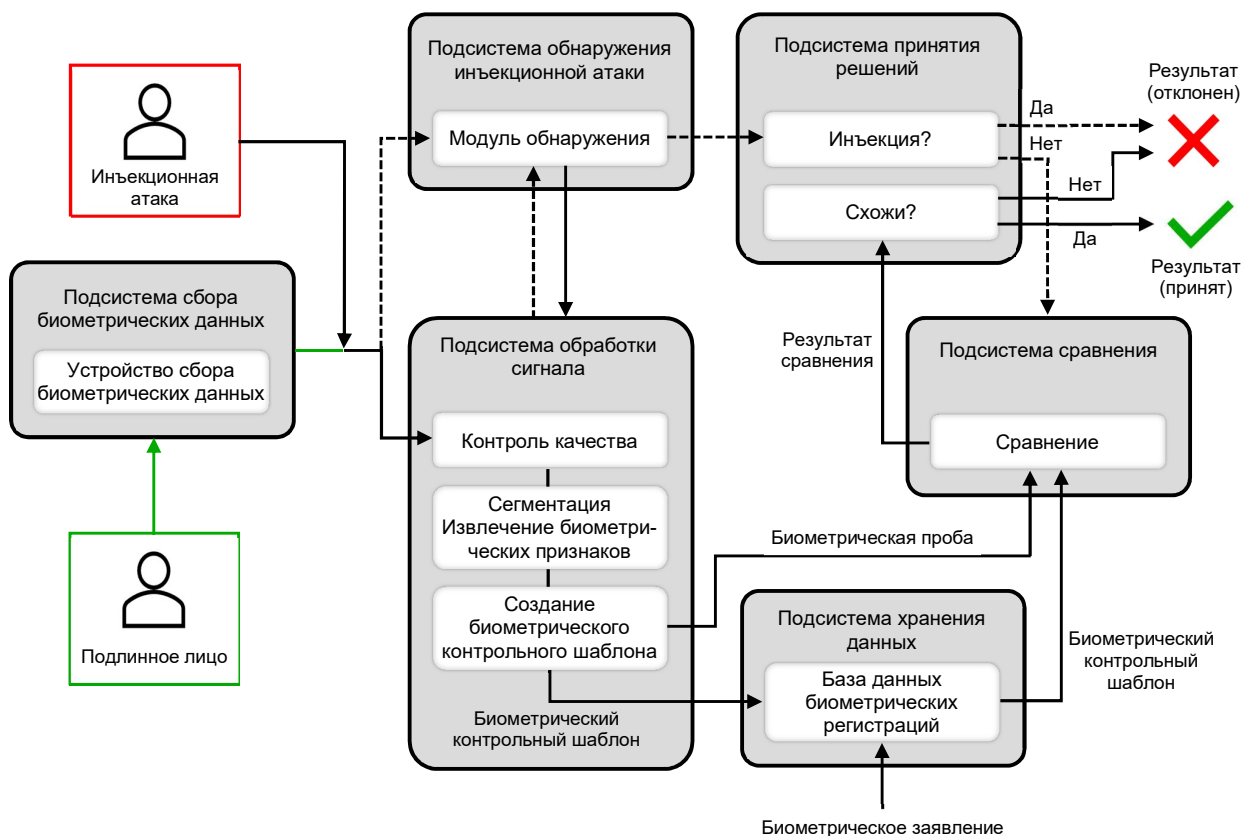


Рисунок 2 – Структура биометрической системы общего вида с подсистемой обнаружения инъекционной атаки

Настоящий стандарт определяет терминологию и структуру для обнаружения инъекционных атак, а также для их классификации, детализации и передачи соответствующих данных для последующего принятия решения биометрической системой и оценки ее эксплуатационных характеристик.

Область применения настоящего стандарта не распространяется на элементы безопасности и любые другие криптографические функции безопасности.

В серию стандартов «Информационные технологии. Биометрия. Обнаружение инъекционной атаки» также входят следующие стандарты:

- Информационные технологии. Биометрия. Обнаружение инъекционной атаки.

Часть 2. Методология оценки эксплуатационных характеристик программного обеспечения»;

- Информационные технологии. Биометрия. Обнаружение инъекционной атаки.

Часть 3. Расширенная классификация атак»;

- Информационные технологии. Биометрия. Обнаружение инъекционной атаки.

Часть 4. Оценка потенциала атаки».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Обнаружение инъекционной атаки

Часть 1

Общие требования

Information technology. Biometrics. Injection attack detection. Part 1. General requirements

Дата введения – 202 – –

1 Область применения

Настоящий стандарт устанавливает термины и определения, используемые для описания, а также структуру методов обнаружения инъекционных атак с целью обнаружения, классификации и детального описания инъекционных атак.

Настоящий стандарт содержит:

- рекомендации по снижению рисков инъекционной атаки;
- примеры противодействия инъекционным атакам в биометрической системе на этапах биометрической регистрации и биометрической верификации.

Настоящий стандарт распространяется только на те подсистемы обнаружения атаки на биометрическое предъявление, которые могут быть использованы в качестве механизма защиты от инструментов и/или методов инъекционной атаки. При этом испытание подсистемы обнаружения атаки на биометрическое предъявление не входит в область применения настоящего стандарта.

Настоящий стандарт не распространяется:

- на любые другие виды атак кроме атак типа 2 (см. рисунок 1);
- шифровальные (криптографические) средства защиты информации (СКЗИ).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р ИСО/МЭК 71414.1 (ИСО/МЭК 19795-1:2021) Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура

ГОСТ Р 58624.1 (ИСО/МЭК 30107-1:2016) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура

ГОСТ Р 58624.3 (ИСО/МЭК 30107-3:2017) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний

П р и м е ч а н и е – 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 ссылку этого стандарта с учетом всех внесенных в данную версию изменений. Если изменен 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.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ ISO/IEC 2382-37, ГОСТ Р 71414.1, ГОСТ Р 58624.1 и ГОСТ Р 58624.3, а также следующие термины с соответствующими определениями:

3.1 **тип атаки:** Сочетание метода инъекционной атаки и вида инструмента инъекционной атаки.

3.2 **инъекция:** Изменение потока данных путем изменения источника данных или перезаписи данных.

3.3 **перехват:** Операция, при которой вызов функции перехватывается программой для изменения ее поведения.

3.4 **инъекционная атака:** Использование метода инъекционной атаки для вмешательства в работу биометрической системы путем подмены исходного биометрического образца, полученного с помощью устройства сбора биометрических данных, на инструмент инъекционной атаки перед выполнением процесса извлечения признаков.

Пример – Инъекционная атака может представлять собой инъекцию через виртуальную веб-камеру поддельного видео, которое создается путем накладывания изображения лица жертвы поверх изображения лица злоумышленника с целью выдать себя за личность жертвы во время удаленной транзакции биометрической верификации по изображению лица.

3.5 **обнаружение инъекционной атаки;** ОИА: Автоматизированное определение инъекционной атаки.

Примечание – Обнаружение инъекционной атаки может включать в себя механизмы защиты от методов инъекционной атаки и механизмы защиты от инструментов инъекционной атаки.

3.6 **подсистема обнаружения инъекционной атаки;** подсистема ОИА: Аппаратное и/или программное обеспечение, которое реализует механизм ОИА и в явном виде сообщает о факте ОИА.

3.7 **инструмент инъекционной атаки;** ИИА: Биометрический образец, используемый в инъекционной атаке.

Примечание – Инструмент инъекционной атаки может быть модифицированным биометрическим образцом.

ГОСТ Р

(проект, первая редакция)

3.8 механизм защиты от инструментов инъекционной атаки; МЗИИА: Защитный механизм, направленный на создание биометрической системы, устойчивой к ИИА.

3.9 вид инструмента инъекционной атаки; ВИИА: Класс ИИА, созданных с использованием общего метода производства и на основе различных биометрических характеристик.

Пример – Набор поддельных видео с изображением лица, созданных с использованием одного и того же программного обеспечения.

3.10 метод инъекционной атаки; МИА: Метод вмешательства в работу биометрической системы путем подмены исходного биометрического образца, полученного с помощью устройства сбора биометрических данных.

3.11 механизм защиты от методов инъекционной атаки; МЗМИА: Защитный механизм, направленный на создание биометрической системы, устойчивой к МИА.

3.12 модифицированный биометрический образец: Биометрический образец, измененный злоумышленником путем редактирования или модификации с целью выдачи себя за жертву или сокрытия исходных характеристик биометрического образца.

3.13 учетная запись с неограниченными правами: Тип учетной записи, которая имеет неограниченный доступ ко всем файлам, директориям и функциям системы.

3.14 устройство с учетной записью с неограниченными правами: Устройство, в котором получен доступ к учетной записи с неограниченными правами.

3.15 прокси (сервер): Компьютерный процесс, который перенаправляет протокол между клиентской и серверной компьютерными системами, представляясь клиенту от имени сервера, а серверу — от имени клиента.

3.16 эмулятор: Программное средство или аппаратный комплекс, который имитирует работу другого устройства или системы.

4 Обозначения и сокращения

В настоящем стандарте использованы следующие обозначения и сокращения:

API – прикладной программный интерфейс (application programming interface);

ИТ – информационные технологии;

ОАБП – обнаружение атаки на биометрическое предъявление;

ПЗУ – постоянное запоминающее устройство.

5 Характеристики инъекционной атаки

5.1 МИА

Инъекционные атаки как правило осуществляют самозванцы, которые намереваются быть распознанными как определенное лицо, зарегистрированное в биометрической системе.

Чтобы осуществить инъекционную атаку, злоумышленнику необходимо иметь частичный контроль над устройством для выполнения подмены, так как для осуществления подмены может потребоваться подготовка устройства или использование определенного программного обеспечения, установленного на устройстве. Это означает, что контроль над устройством, используемым для выполнения атаки, (большую часть времени) отсутствует.

Таким образом, существуют различные типы устройств, на которых возможно осуществить инъекционную атаку:

- компьютер;
- мобильное устройство;
- другие устройства, оснащенные подсистемой сбора данных (например, устройство ИВ, оснащенное камерой).

На рисунке 3 показана схема выполнения инъекционной атаки на биометрическую систему с использованием сетевого или компьютерного приложения. На рисунке 4 показана схема выполнения инъекционной атаки с использованием перехвата.

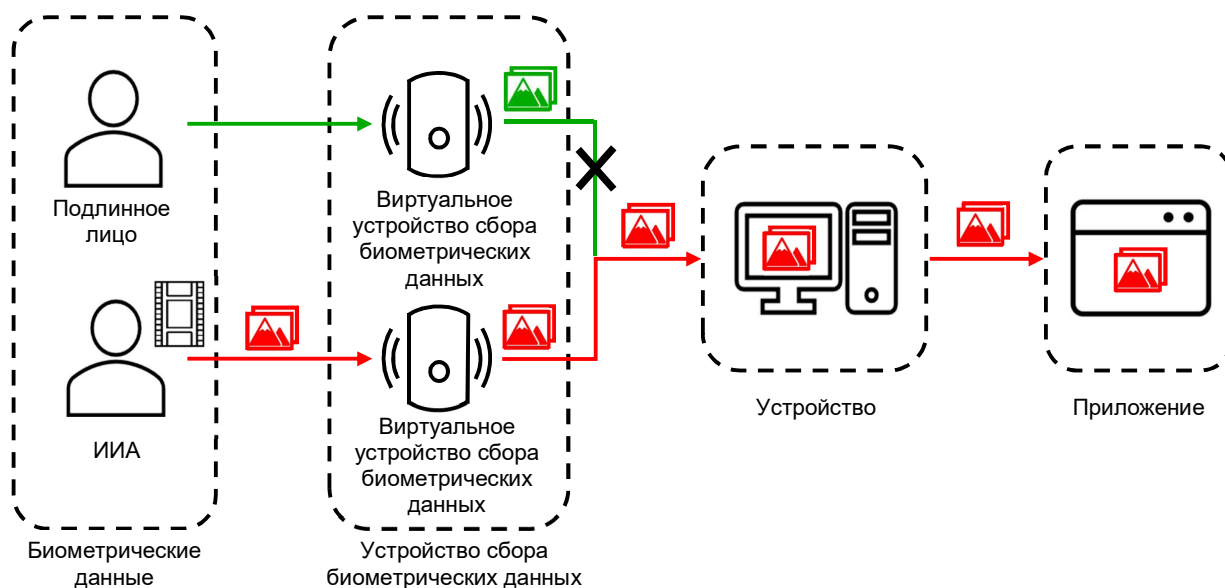


Рисунок 3 – Схема инъекционной атаки через виртуальное устройство сбора биометрических данных, используемое в стандартном устройстве

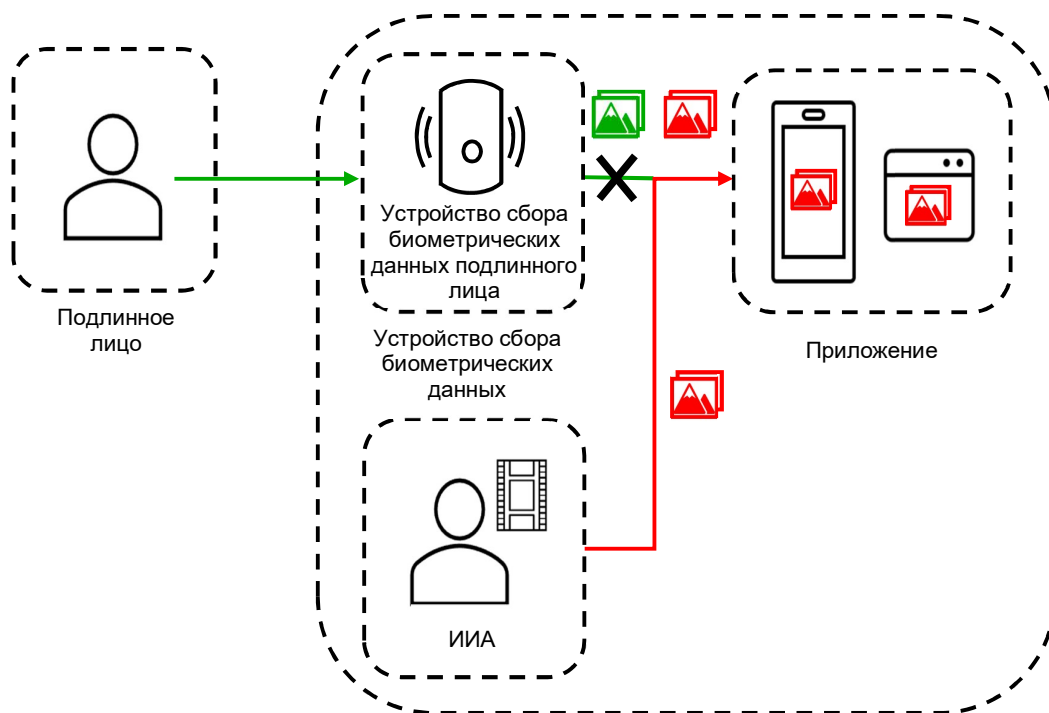


Рисунок 4 – Схема инъекционной атаки с использованием перехвата

Сложность осуществления инъекционной атаки зависит от устройства, которое используется для ее выполнения, и от способа использования данного устройства. Использование компьютера может дать доступ к большому количеству различного

программного обеспечения, позволяющего самозванцу имитировать устройство сбора биометрических данных (например, виртуальную камеру для распознавания лица или виртуальный микрофон для распознавания голоса) или перехватывать данные, отправленные устройством сбора биометрических данных. Установить виртуальное устройство сбора биометрических данных на мобильное устройство сложнее. В данном случае для выполнения инъекционной атаки может потребоваться устройство с учетной записью с неограниченными правами и наличие опыта в обратном проектировании мобильных приложений и тестировании на проникновение, чтобы сделать перехват API устройства сбора биометрических данных, вызываемого мобильным приложением, и заменить подлинные биометрические данные вредоносными данными.

Примечание – Для некоторых устройств злоумышленник может найти в сети Интернет пользовательское ПЗУ с виртуальной камерой, затем настроить учетную запись с неограниченными правами на своем смартфоне, установить пользовательское ПЗУ и выполнить инъекционную атаку.

На рисунке 5 приведен пример процесса перехвата.

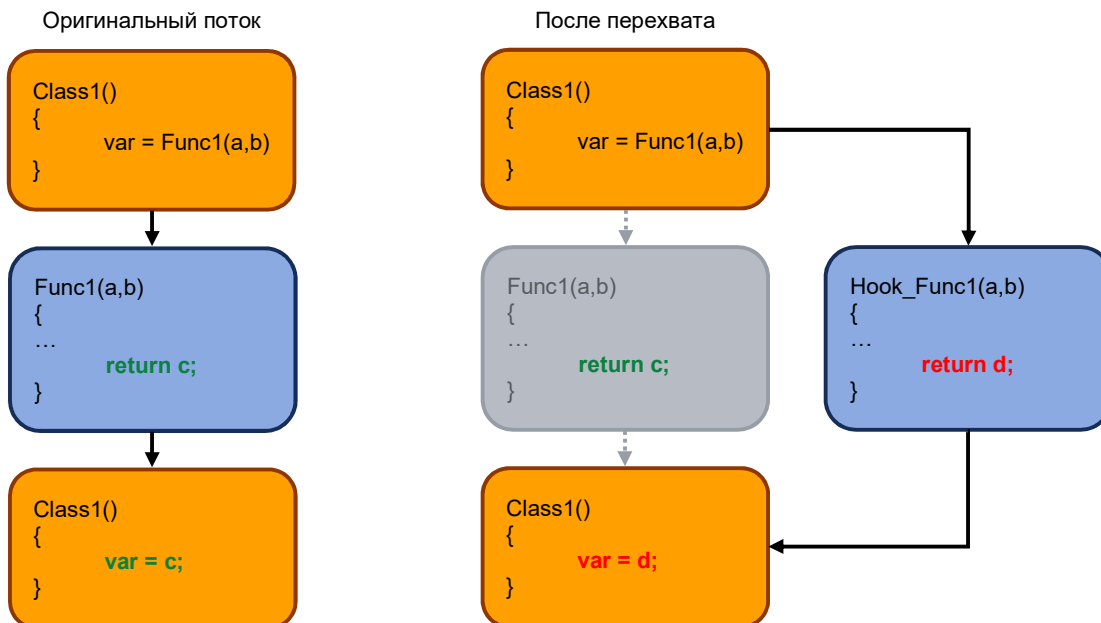


Рисунок 5 – Процесс перехвата

Возможность осуществления инъекционной атаки зависит от среды ее выполнения. Если над биометрической системой осуществляется контроль или обслуживание, злоумышленнику может быть труднее осуществить инъекционную атаку.

Успешное выполнение инъекционной атаки тесно связано с ИИА, который использует злоумышленник. Создание высококачественного ИИА может зависеть от опыта злоумышленника и/или качества источника биометрических данных.

5.2 ИИА

ИИА — это полностью синтетический, модифицированный или неизменный биометрический образец, используемый злоумышленником для замены подлинного биометрического образца с целью обмана биометрической системы. Данные, используемые для инъекционной атаки, разделяют на три категории: неизменные, модифицированные и искусственные данные (рисунок 6).

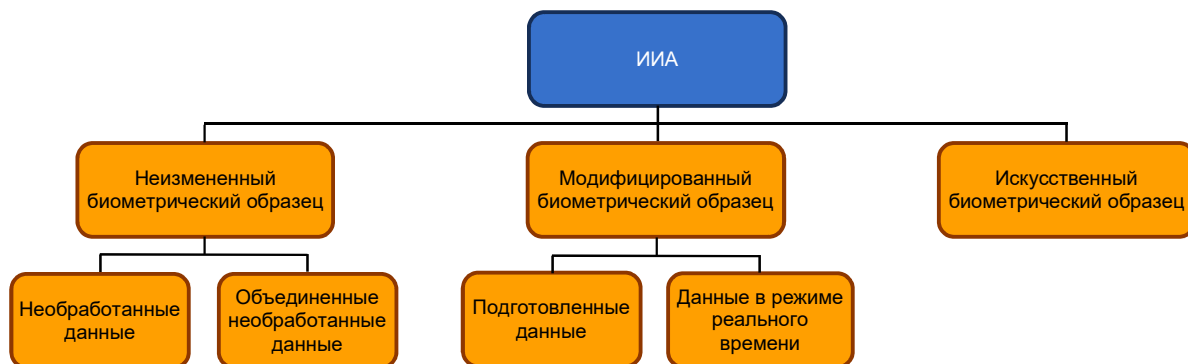


Рисунок 6 – Типы ИИА

Примеры для каждого типа ИИА приведены в таблице 1.

Таблица 1 – Примеры ИИА

Неизмененный биометрический образец	Необработанные данные	Видеоизображение лица, фотография радужной оболочки глаза
	Объединенные необработанные данные	Объединение нескольких видео или аудиозаписей голоса
Модифицированный биометрический образец	Подготовленные данные	Поддельное видео, синтезированная запись голоса или их комбинация
	Данные в режиме реального времени	Поддельное видео в режиме реального времени, синтезированный голос в режиме реального времени или их комбинация
Искусственный биометрический образец	Созданные искусственные данные	Фотография лица или отпечатка пальца, сгенерированная с помощью ИИ

6 Структура методов ОИА

6.1 Типы методов ОИА

Метод инъекционной атаки не зависит от того, является ли устройство сбора биометрических данных встроенным или внешним (например, встроенная веб-камера или USB-веб-камера на компьютере), и инъекционная атака может быть выполнена на обеих архитектурах.

Существуют следующие типы методов ОИА:

- МЗМИА, предназначенный для противодействия МИА;
- МЗИИА, предназначенный для обнаружения ИИА.

Рекомендуется разрабатывать подсистему ОИА таким образом, чтобы в ней были реализованы оба типа механизмов ОИА.

Так как невозможно гарантировать, что биометрические данные, переданные в приложение (мобильное или компьютерное), получены от доверенного устройства сбора биометрических данных, механизмы противодействия МИА обычно зависят от криптографических решений безопасности. Механизмы противодействия ИИА могут

ГОСТ Р

(проект, первая редакция)

быть похожи на механизмы ОАБП или могут использовать фактор случайности во время процесса сбора биометрических данных (см. 6.3.1 и 6.3.2).

Технологии МЗМИА могут быть основаны на обнаружении изменений в системе, обнаружении инъекций, контрмерах ИТ или аутентификации устройства. Технологии МЗИИА могут быть основаны на методе «запрос-ответ» или обнаружении артефактов.

В таблице 2 приведены различные методы ОИА и примеры их реализации.

Т а б л и ц а 2 – Примеры методов обнаружения и защиты от инъекционных атак

МЗМИА	Обнаружение изменений в системе	Обнаружение изменений в системе при обычном ее использовании злоумышленником. Например, обнаружение прокси, учетной записи с неограниченными правами или эмулятора для мобильных устройств
	Обнаружение инъекции	Обнаружение инъекционной атаки во время использования устройства. Например, обнаружение виртуальной камеры
	Контрмеры ИТ	Меры безопасности, реализованные разработчиком для сокрытия конфиденциальной информации и/или для того, чтобы злоумышленник потратил больше времени при попытках обмануть биометрическую систему. Например, использование счетчиков или обфускация кода
МЗИИА	Аутентификация устройства и безопасный обмен сообщениями	Биометрический образец, переданный в подсистему обработки сигнала, защищается с точки зрения подлинности и целостности путем применения соответствующих криптографических примитивов [2].
	Запрос-ответ	Обнаружение ожидаемого ответа после определенного запроса от подсистемы ОИА. Ответ на запрос может быть выполнен самим пользователем или устройством сбора биометрических данных, и его можно наблюдать на биометрическом образце. Например, подсистема ОИА может попросить пользователя выполнить определенные действия (активный запрос-

		<p>ответ), такие как движение головы в биометрических системах распознавания лица или считывание некоторого случайного кода для биометрических систем распознавания голоса, или она может дать команду подсистеме сбора данных выполнить определенные инструкции (пассивный запрос-ответ).</p> <p>Можно использовать и другую полезную информацию, непосредственно извлеченную из устройства сбора биометрических данных и собранных данных, для обнаружения обычного использования. Например, использовать акселерометр мобильного телефона для проверки того, находится ли устройство в движении</p>
	Обнаружение артефактов	Обнаружение признаков, указывающих на артефакт. Например, обнаружение аномальных срезов в голосовом потоке в синтетическом голосе, созданном путем копирования и вставки или конкатенации речи; обнаружение аномального размытия вокруг рта или глаз в синтетических видео

6.2 МЗМИА

6.2.1 Обнаружение виртуального устройства сбора биометрических данных

Злоумышленник может использовать виртуальную камеру, которую можно настроить для отображения предварительно записанных видео или видеопотока подлинного лица, и которая будет функционировать аналогично реальной камере. Аналогичным образом, использование симулятора или эмулятора смартфона позволяет злоумышленнику использовать среду рабочего стола и имитировать или эмулировать смартфон. На имитируемую камеру смартфона можно, например, подавать предварительно записанное видео подлинного лица или динамическое поддельное видео.

В подсистеме ОИА должны быть предусмотрены механизмы, снижающие риск использования таких виртуальных устройств сбора биометрических данных.

6.2.2 Механизмы защищенных каналов

Злоумышленник не должен иметь возможности перехвата и изменения фото-, видеоизображений, результата проверки витальности или любых инструкций во время их передачи. Для защиты всего цифрового канала между устройством сбора биометрических данных и подсистемой обработки сигнала следует использовать СКЗИ. Они могут включать в себя цифровое шифрование, цифровую подпись или любые другие механизмы обеспечения целостности и подлинности.

6.3 МЗИИА

6.3.1 Запрос-ответ

Метод «запрос-ответ» широко используется в системах распознавания, основанных как на биометрических, так и на небιοметрических характеристиках.

В таблице 3 приведен принцип ОИА с использованием метода «запрос-ответ».

Таблица 3 – ОИА с использованием метода «запрос-ответ»

	Пассивный ответ	Активный ответ
Запрос	Конкретные команды подсистеме сбора данных, влияние которых можно наблюдать на биометрическом образце	Сигналы (вербальные, визуальные и т. д.), направленные на выполнение конкретного действия, результат которого должен быть получен биометрической системой
Ответ	Естественные, произвольные реакции, не контролируемые субъектом	Произвольные реакции, основанные на восприятии субъекта и контролируемые им
Примеры	Изменения фокуса на изображении лица в соответствии с шаблоном, заданным системой	Изменение угла наклона головы меняется в ответ на просьбу повернуть голову Субъект произносит определенное слово в ответ на сигнал к прочтению данного слова

Использование метода «запрос-ответ» для ОИА может снизить риск инъекционных атак, основанных на неизменных биометрических образцах, так как в зависимости от типа запроса злоумышленнику может быть сложно (а иногда и невозможно) получить неизменный биометрический образец, соответствующий данному запросу. Чем более неожиданный тип запроса, тем сложнее получить неизменный биометрический образец, соответствующий данному запросу. Запрос-ответ для ОИА также может затруднить создание инъекционных атак, основанных на модифицированных данных, в частности, если запросы к устройству или пользователю основаны на «экстремальных данных» (например, данных, которые сложно синтезировать), таких как необычные ракурсы лица или вымышленные слова. Более того, если запрос основан на известных уязвимостях инъекционной атаки, для проведения такой атаки достаточно высокого качества злоумышленнику может потребоваться большее количество времени и/или более высокий уровень знаний.

В контексте ОИА метод «запрос-ответ», основанный как на активных, так и на пассивных ответах, особенно интересен в том случае, если присутствует фактор случайности появления запроса, так как это усложняет подготовку инъекционной атаки (см. 6.3.2).

6.3.2 Случайность

Информация, приведенная в настоящем пункте, распространяется только на биометрические системы, основанные на архитектуре «сервер-клиент». Для эффективного предотвращения инъекционных атак рекомендуется, чтобы биометрическая система выполняла анализ различных запросов на стороне сервера. Поскольку клиентская сторона должна получать необходимую информацию от пользователя, любой запрос, отправляемый системе или пользователю, должен быть зашифрован, чтобы злоумышленник не мог заранее узнать запросы.

Включение фактора случайности в подсистемы ОИА с запросом-ответом для предотвращения инъекционной атаки может усложнить злоумышленнику обман биометрической системы. Системы со случайным запросом-ответом основаны на наборе различных запросов или их последовательностей, которые могут быть заданы любому пользователю в любой момент времени. Чем больше возможных запросов или их последовательностей, тем надёжнее биометрическая система. Например, в биометрической системе распознавания лица с активным ответом подсистема ОИА может сделать к пользователю запрос повернуть голову направо, затем налево или в

ГОСТ Р

(проект, первая редакция)

обратном порядке: это создаст два возможных варианта, которые для каждой проверки могут быть выбраны случайным образом. Чем больше энтропия, тем больше времени требуется для создания различных последовательностей запросов для проведения инъекционной атаки. Это означает, что наличие большой энтропии (например, более сотни возможных последовательностей запросов) может предотвратить заранее подготовленные инъекционные атаки, которые при этом являются инъекционными атаками наилучшего качества, так как в случае предварительной подготовки у злоумышленника есть достаточно времени, чтобы устранить или, по крайней мере, уменьшить недостатки подготовленной инъекционной атаки.

Если биометрическая система построена на архитектуре «сервер-клиент», создание запроса должно происходить на стороне сервера, чтобы предотвратить его изменение злоумышленником. Кроме того, конфиденциальность инструкций, содержащих запрос, должна быть защищена в канале между сервером и клиентом (см. 6.2.2).

Важно отметить, что особенности устройства влияют на возможности разработчика. Например, разработчик имеет доступ к большему количеству параметров управления камерой в мобильном приложении по сравнению с параметрами, доступными для веб-камеры в веб-приложении.

Примеры

1 На мобильном устройстве разработчик имеет доступ к необработанным изображениям (без применения каких-либо алгоритмов для обработки изображений).

2 На мобильном устройстве можно получить доступ к данным других датчиков, например, акселерометра.

6.3.3 Обнаружение артефактов

Реализация обнаружения артефактов в МЗИИА способствует противодействию инъекционным атакам с использованием синтезированных видео, с наложением лица на заданное исходное видео, с использованием синтезированного голоса.

Пример – В некоторых случаях получение изображения с разрешением, отличным от ожидаемого, может быть свидетельством инъекционной атаки.

Подобные методы автоматического ОИА могут быть эффективны для защиты биометрических систем от инъекционных атак, реализуемых в режиме реального времени, так как такие атаки обычно имеют множество артефактов, которые могут быть обнаружены.

Пример – Для увеличения вероятности появления артефактов может быть использован запрос, требующий движения некоторого объекта перед источником биометрических данных.

6.4 Комбинация нескольких методов ОИА

Каждый метод ОИА предназначен для защиты от определённого типа инъекционной атаки, поэтому наилучшим способом защиты биометрической системы является комбинирование различных методов ОИА. Так, например, подсистема ОИА, сочетающая МЗМИА (например, счетчик попыток входа) с МЗИИА (например, запрос-ответ и обнаружение артефактов), поможет обнаружить большинство инъекционных атак.

6.5 Компромисс между безопасностью и удобством использования

Следует комбинировать различные методы обеспечения безопасности таким образом, чтобы они оставались просты и понятны пользователю. Обеспечение высокого уровня безопасности может повлиять на удобство использования биометрической системы. Для поиска компромисса между уровнем безопасности и удобством использования важно проводить испытания для оценки эксплуатационных характеристик подсистемы ОИА.

Приложение А

(справочное)

Противодействие инъекционным атакам в биометрической системе

А.1 Инъекционная атака на этапе биометрической регистрации

Для проведения успешной инъекционной атаки на этапе биометрической регистрации в биометрической системе:

- 1) подлинный биометрический образец должен быть заменен на ИИА;
- 2) биометрический образец ИИА должен быть успешно обработан для создания биометрического контрольного шаблона;
- 3) проведение инъекционной атаки должно быть реализовано при соблюдении мер безопасности на системном уровне;
- 4) подсистема ОИА, при ее наличии в системе, не должна классифицировать предъявленный ИИА как инъекционную атаку.

Инъекционная атака может быть предотвращена на любом из этих этапов в зависимости от типа биометрической системы и качества атаки. Например (в соответствии с порядком этапов проведения атаки, представленным выше):

- 1) может быть получен отказ в биометрической регистрации ИИА, если подсистема ОИА классифицировала полученный биометрический образец ИИА как атаку;
- 2) подсистема обработки сигнала может отклонить биометрический образец ИИА ввиду неудовлетворительного качества.

А.2 Инъекционная атака на этапе биометрической верификации

Для проведения успешной инъекционной атаки на этапе биометрической верификации в биометрической системе:

- 1) подлинный биометрический образец должен быть заменен на ИИА;
- 2) биометрический образец ИИА должен быть успешно обработан;
- 3) решение о сравнении биометрического образца ИИА и биометрического контрольного шаблона должно быть положительным;
- 4) проведение инъекционной атаки должно быть реализовано при соблюдении мер безопасности на системном уровне;
- 5) подсистема ОИА, при ее наличии в системе, не должна классифицировать предъявленный ИИА как инъекционную атаку.

Инъекционная атака может быть предотвращена на любом из этих этапов в зависимости от типа биометрической системы и качества атаки. Например (в соответствии с порядком этапов проведения атаки, представленным выше):

1) может быть получен отказ в биометрической регистрации ИИА, если подсистема ОИА классифицировала полученный биометрический образец ИИА как атаку;

Пример – Подсистема ОИА может классифицировать биометрический образец как инъекционную атаку, если записанный голос не соответствует ожидаемому ответу на запрос или в биометрическом образце обнаружены соответствующие артефакты.

2) подсистема обработки сигнала может отклонить биометрический образец ИИА ввиду неудовлетворительного качества для извлечения признаков;

3) результат сравнения может не превышать установленный порог принятия решений ввиду использования для сравнения биометрического образца ИИА неудовлетворительного качества.

Библиография

- [1] Ratha N.K., Connell J.H., Bolle R.M. «Enhancing security and privacy in biometrics-based authentication systems» // IBM Syst. J., 2001, 40 (3)
- [2] Waldmann, U., Scheuermann, D., Eckert, C., «Protected transmission of biometric user authentication data for oncard-matching» // ACM Symposium on Applied Computing, 2004

УДК

ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, инъекционная атака, обнаружение инъекционной атаки, инструмент инъекционной атаки
