

Date: 5th June-2025

НОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АБОНЕНТОВ СОТОВОЙ СВЯЗИ

Жолдасова Ферида Икрамовна

Ташкентский университет информационных технологий
студент магистратуры

Абдурахмонов Рустам Паттохвич

Профессор Ташкентского университета информационных технологий

Аннотация. Операторы сотовой мобильной связи (СМС) помимо стандартных услуг голосовой связи, используя мощности сетей и оборудования, реализуют услуги с добавленной стоимостью (VAS-услуги). Операторами связи обслуживаются сервисы и услуги, требующие идентификации абонента и телефонного аппарата (ТА). Это продиктовано тем, что в настоящее время на сетях СС реализуются сервисы, которые позволяют с использованием ТА производить различного рода финансовые действия со счетом абонента, а также взаимодействовать с банковскими системами, получать отчетность и совершать операции по банковским картам. Так, например, абонент, оплативший услуги, должен получить единоличный доступ к ней. Но в случае утери телефона и несвоевременного сообщения об утере в службу поддержки оператора, или завладение телефоном сторонними лицами мошенническим путем нарушается право абонента, что может привести к финансовым потерям.

Ключевые слова: Идентификация абонента, Голосовая биометрия, Информационная безопасность, Сотовая подвижная связь (СПС), Голосовой ключ, Биометрические параметры, Нейронные сети, Речевая идентификация, Защита от несанкционированного доступа, Шифрование в GSM

Постановка задачи:

В ряде случаев необходимо внедрение новых механизмов обеспечения информационной безопасности (ИБ), работающих совместно со стандартными алгоритмами шифрования, реализованными в сетях СМС (здесь и далее будем рассматривать сети операторов СПС стандарта GSM, хотя все сказанное применимо и к сетям СПС других стандартов).

В рекомендациях GSM для предотвращения несанкционированного доступа к информации абонентов, передаваемой по сетям операторов СМС, предусмотрены алгоритмы шифрования речевого канала. Однако, как показано в [2], если речь идет о необходимости обеспечить максимальную конфиденциальность информации, передаваемой по каналам связи, необходимо реализовывать дополнительные средства защиты информации (ЗИ) такие как: ввод числового кода, идентификация ТА абонента, использование биометрических данных об абоненте.

Способ идентификации абонента с использованием кода, вводимого с клавиатуры ТА, уже стало обыденным явлением, используемым операторами СПС для проведения дополнительной верификации абонента. Альтернативным или



Date: 5th June-2025

дополнительным вариантом защиты может являться проверка личности абонента по его биометрическим параметрам.

Классификация биометрических параметров человека

Рассмотрим существующие технологии биометрической идентификации.

Идентифицировать человека возможно по признакам связанным с его физиологическими особенностями, которые для него являются персонализированными. К таким признакам можно отнести:

- геометрическое строение руки,
- почерк,
- отпечатки пальцев (дактилоскопия),
- особенности рисунка сетчатки глаза,
- радужная оболочка глаза,
- тепловой портрет (например, инфракрасная карта лица),
- характеристики и особенности речи,
- клавиатурный почерк,
- и др. физиологические особенности человека, делающим его «особенным».

Особенность идентификации по биометрическим параметрам является их исключительность. Вероятность того, что найдутся два человека с одинаковыми признаками, очень мала (например, вероятность того, что у двух различных людей на одинаковых пальцах одной руки совпадут отпечатки пальцев, равна 1/24 млн., то есть, практический нуль).

Представим основные характеристики, перечисленных выше методов биометрической идентификации, в виде таблицы 1. [1]

Таблица 1

Метод получения биометрических параметров	Отказ в доступе %	Ошибочная идентификация «чужого» (без муляжа) %	Ошибочная идентификация «чужого» (с использованием муляжа) %	Сохранение тайны образа при процессе идентификации абонента	Стоимость технической реализации денежном эквиваленте у.е.
геометрическое строение руки	0,2...4	0,2...1	10...75	нельзя скрыть	От 600 до 3000
отпечатки пальцев	2...6	0,0001	10...70	нельзя скрыть	От 60 до 600
особенности рисунка сетчатки глаза	0,4	6...10	_____	нельзя скрыть	примерно 4000
радужная оболочка глаза	0,2...2	0,0001	_____	нельзя скрыть	От 500 до 6000
тепловой	1...9	_____	_____	нельзя	55000

Date: 5th June-2025

портрет				скрыть	
почерк	0,5...5	0,5...5	0,5...5	8-10...10-40	_____
клавиатурный почерк	3...9	3...9	_____	6-10...10-12	_____
характеристи ки и особенности речи	0,5...5	0,5...5	25...90 (запись)	10-16...10-30	1...60

Выбор технологии идентификации абонента по биометрическим параметрам в сетях СМС.

Реализация технологии идентификации абонента по биометрическим параметрам в сетях СМС должно удовлетворять следующим требованиям:

- целесообразностью использования;
- реализация технического решения должна быть решена на платформе ТА абонента;
- ТА с возможностью считывания биометрических параметров должен быть доступным;
- должен использоваться метод, обеспечивающий высокую стойкость системы к внешним атакам.

В 2005 г. в Китае компанией Bird был анонсирован мобильный телефон, позволяющий идентифицировать его обладателя по отпечаткам пальцев от контактного дисплея [3].

Такое решение обеспечивает локализованную защиту от НСД к данным злоумышленником, получившему доступ к ТА. Время стойкости такого решения равно времени, необходимого для физического доступа к информации (взлом корпуса телефона и т.д.).

Альтернативным решением может являться использование в мобильном телефоне механизма идентификации абонента по голосу. Как видно из таблицы 1 голосовая идентификация имеет низкий уровень ложного срабатывания, обеспечивает сохранность голосового ключа, во время его использования, обладает высокой степенью стойкости к подлогу ключа, а также приемлемой ценой.

Определение параметров речи, необходимых для идентификации абонента по голосу

Для того чтобы идентифицировать абонента по голосу, необходимо иметь речевой шаблон, с которым будет сравниваться вводимый в систему голосовой ключ. Сравнение ключа и шаблона может проводиться по одному или нескольким ниже перечисленным характеристикам речевого сигнала (здесь, мы говорим о

Date: 5th June-2025

цифровом речевом сигнале, прошедшем обработку и адаптированном под поставленную задачу) [1]:

- амплитудные и мощностные (громкость);
- временные;
- частотные (тембр);
- энергетические;
- фазовые.

Для обеспечения простоты анализа речевого сигнала, его предварительно подвергают дискретизации с использованием частотного или Вейвлет преобразования. Оптимальным вариантом при реализации ИКМ является использование частоты дискретизации 11 кГц и размер отчетов равно 16 бит [3].

Идентификация абонента может проводиться по следующим показателям, определяемым при обработке речевого сигнала:

- кратковременная энергия сигнала (определяется функции кратковременной энергии с использованием окон Хемминга [3]);
- автокорреляционная функция (автокорреляционная функция позволяет определять энергию и периодические свойства сигнала);
- число переходов сигнала через ноль (т.к. высокие частоты приводят к большому числу переходов через ноль, а низкие - к малому, то существует жесткая связь между числом нулевых пересечений и распределением энергии по частотам [3]);
- спектр сигнала;
- коэффициенты линейного предсказания [3];
- кепстральные коэффициенты;
- кепстральные коэффициенты, вычисленные на основе линейного предсказания.

При обработке речи необходимо учитывать следующие речевые признаки сигнала:

- детерминированные – определенные для рассматриваемого объекта;
- вероятностные – признаки распределены по всем классам объектов с какой-то вероятностью;
- логические – признаки, которые можно описать элементарными логическими функциями с достаточной определенностью;
- структурные - к ним относятся лингвистические и синтаксические.

Требования, предъявляемые к ТА (считывателю биометрических параметров) и процедуре обработки речевого сигнала

ТА должен обеспечивать:

- адекватного отображения входного биометрического параметра в данные.
- низкого уровня помех. Конкретные значения соотношения сигнал/шум имеют смысл только для конкретных биометрических признаков

ТА, используемые в сетях СПС, удовлетворяют обоим требованиям.



Date: 5th June-2025

Процедура выделения биометрических параметров из речевого сигнала должна обеспечить обработку большого потока входящей, избыточной информации и произвести подбор необходимого набора признаков. При выборе биометрических параметров необходимо руководствоваться следующими принципами:

- наборы параметров биометрических признаков для различных абонентов не должны пересекаться;
- персонализированные параметры для каждого абонента должны быть как можно более устойчивы. Под устойчивостью будем понимать дисперсию параметров внутри класса параметров для определенного пользователя, следовательно, чем меньше внутриклассовая дисперсия параметров, тем более устойчивы параметры;
- параметры для различных абонентов должны быть весьма неустойчивы, т.е. межклассовая дисперсия для различных дикторов должна быть наибольшей.

Очевидно, что параметры, соответствующие данным принципам являются идеальным вариантом, в большинстве случаев получить параметры, обладающие этими свойствами – невозможно, поэтому необходимо выбирать компромиссные решения.

Объем выходных биометрических параметров должен быть небольшим (в среднем до 200 байт). Время вычисления параметров должно быть незначительным для пользователя.

Сложность перебора параметров должна быть больше сложности перебора ключа, поскольку в противном случае более эффективной становится атака перебора на биометрические параметры. Таким образом, алгоритм должен обеспечивать преобразование больших массивов биометрической информации в компактные параметры, устойчивые в пределах образцов одного абонента и значительно отличающиеся для разных абонентов.

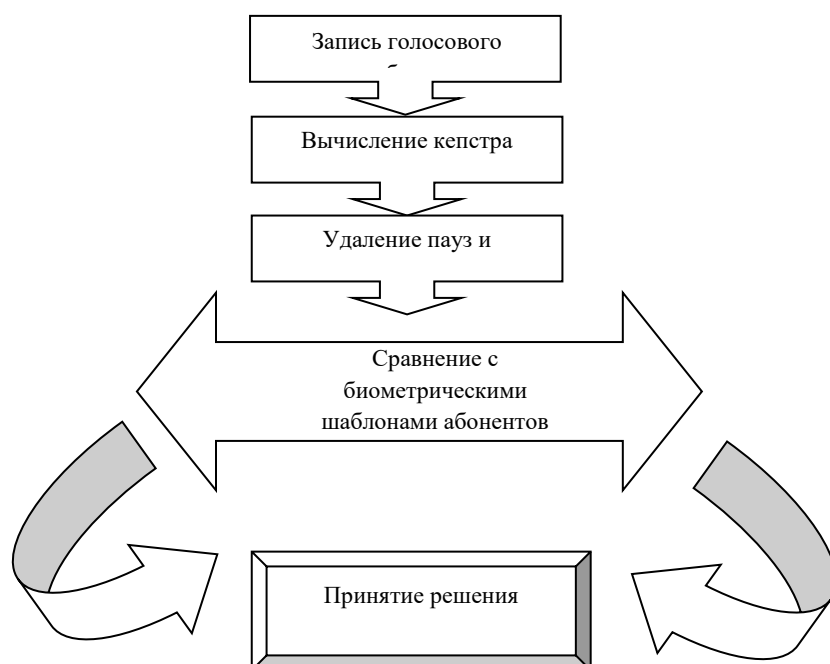


Рисунок 1.

Структурная схема идентификации пользователя



Важной функциональной особенностью системы идентификации абонента по голосу, показанной на рисунке 1, является механизм обучения системы, которые реализуется на базе нейронных сетей распознавание образа.

В настоящее время искусственные нейронные сети являются классическим средством для распознавания образов различной природы. Для реализации системы речевой идентификации абонента, нейронная обучаемая сеть должна обладать следующими свойствами:

- нейронные сети строятся из множества простых элементов, выполняющих элементарные действия и соединённых между собой различными связями;
- нейронные сети должны обладать высокой способностью к обучению и адаптации;
- нейронные сети должны обладать способностью обобщать информацию, полученную в процессе обучения. Таким образом, правильное распознавание объекта будет достигнуто даже в случае изменения его характеристик, например, потери или искажения части информации.

Передача речевого ключа в сетях СПС происходит по стандартным речевым каналам, защита от НСД к информации в которых обеспечивается алгоритмами шифрования, предусмотренными в стандарте GSM. Однако, существует возможность записи информации, передаваемой в зашифрованном виде с целью проведения криптоанализа и выявления голосового ключа. Для исключения такой возможности в системе голосовой идентификации абонента могут быть заложены алгоритмы смены голосового ключа. Временные интервалы и принципы реализации процедур смены голосового ключа выбираются в зависимости от важности информации.

Реализация механизма идентификации абонента по голосу в сетях СМС

Возможность идентификации абонента по голосовому ключу технически может реализовываться либо с использованием ресурсов оператора СМС, либо у контент-провайдера, организующего контроль доступа к своим услугам (рисунки 2 и 3).

Date: 5th June-2025

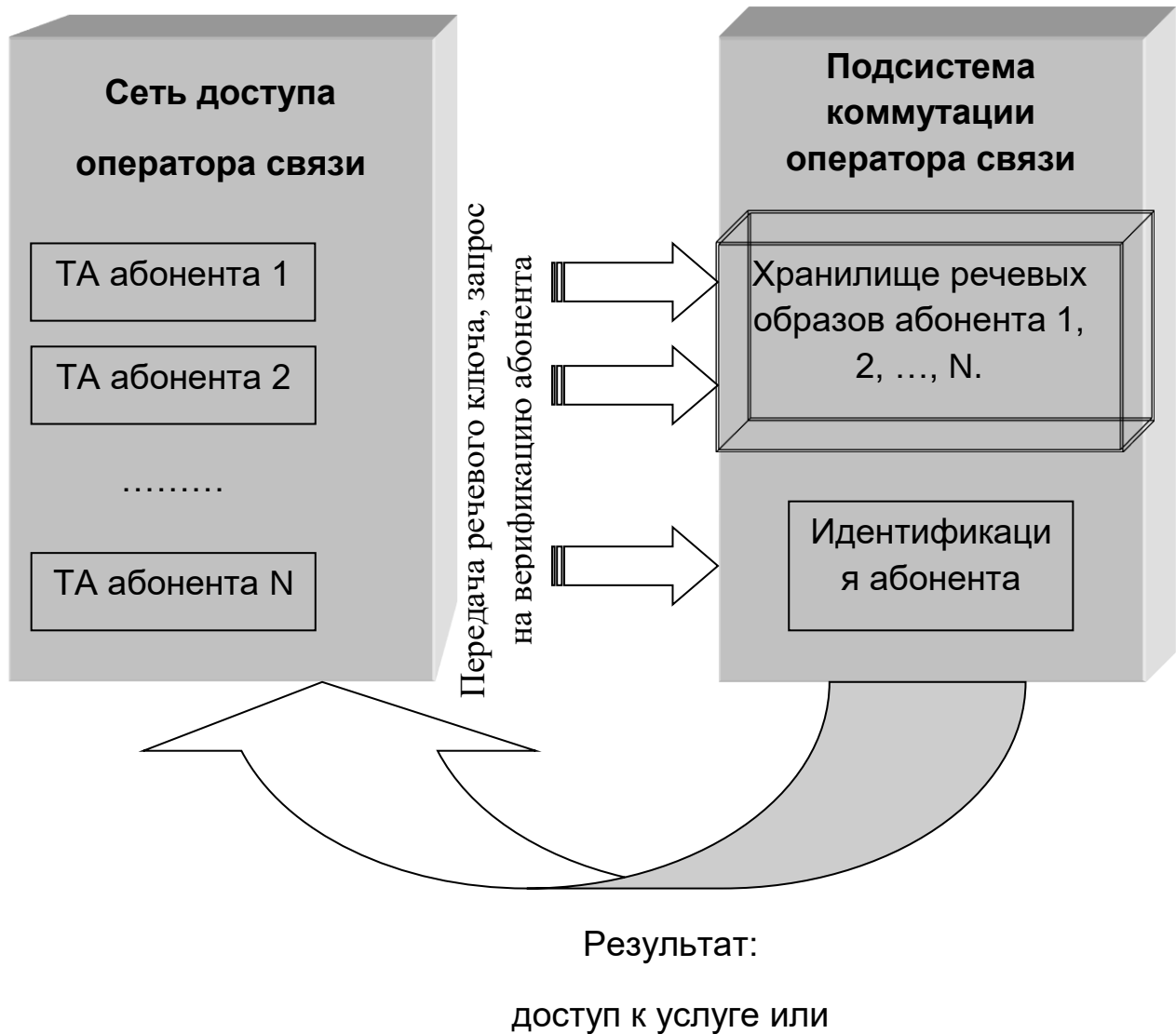


Рисунок 2. Идентификации абонента по голосовому ключу у оператора СПС

Со стороны абонента достаточно обычного ТА, работающего в сети оператора СМС стандарта GSM, и являющимся в данном случае микрофоном.

На сети оператора или контент-провайдера услуг должно реализовываться:

- хранилище речевых образов абонентов;
- механизм сравнения речевого ключа с хранящимися речевыми образами и принятие решения;
- алгоритм реализации смены речевого ключа.

В первом случае (рисунок 2) решение о доступе к ресурсам по результатам обработки речевого ключа принимается в сети оператора СМС. Во втором (рисунок 3), силами контент-провайдера, сеть оператора СПС в этом случае выполняет свое прямое назначение – передача речи.

Date: 5th June-2025

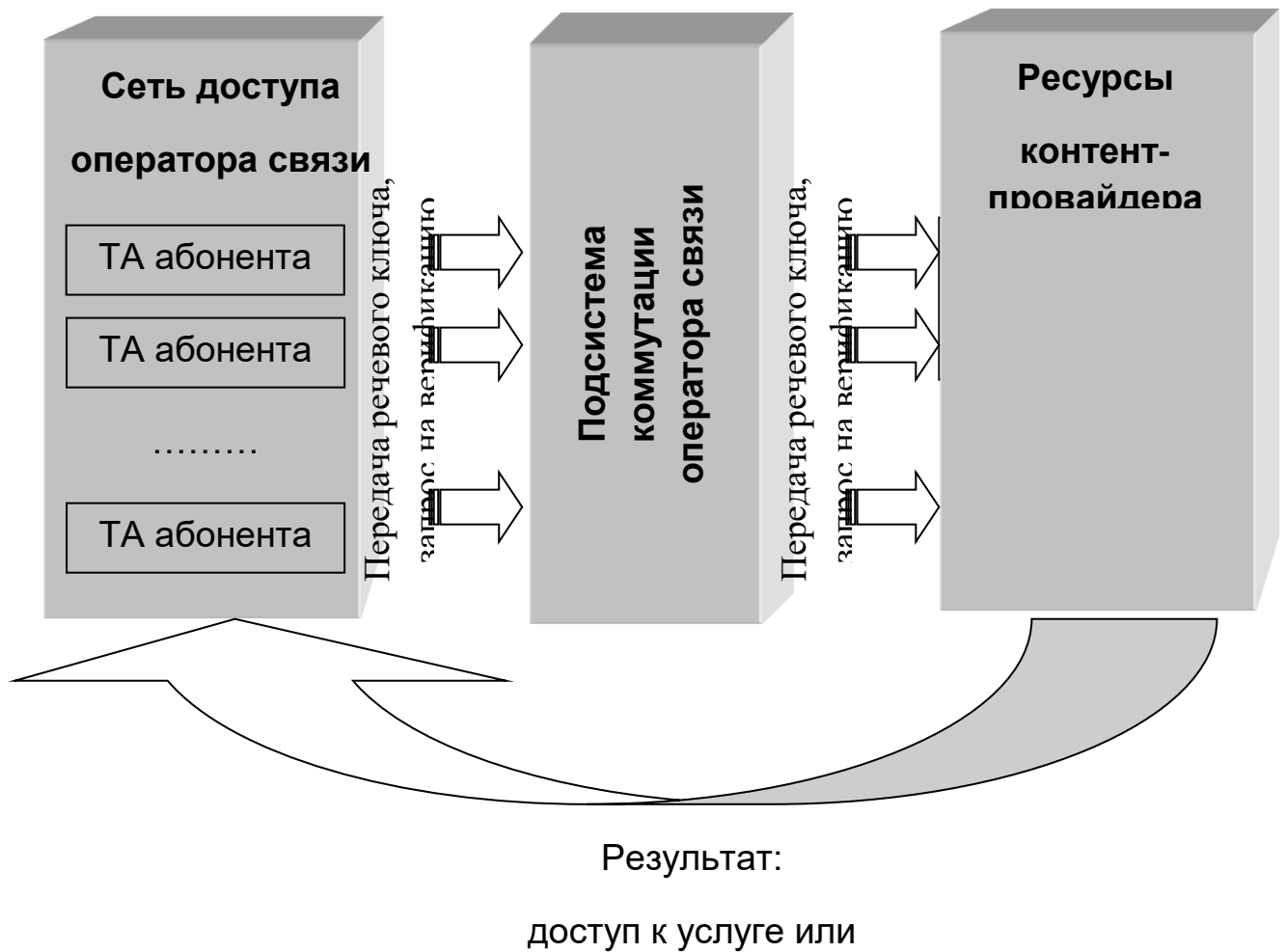


Рисунок 2. Идентификации абонента по голосовому ключу у контент-провайдера

Заключение

Реализация возможности идентификации абонента по голосу в сетях СМС для доступа к услугам, на взгляд авторов является интересной с теоретической и практической точки зрения.

Возможности современных сетей СМС позволяют реализовать такой механизм в полной мере.

Целесообразность использования такого метода идентификации абонентов может быть оправдана целями и задачами, которые необходимо решить. Ведь подбор речевого ключа, намного сложнее подбора пин-кода вводимого с клавиатуры ТА. А совместное использование механизмов своевременной смены ключа и алгоритмов шифрования, реализованных в сетях GSM, позволяет говорить с высокой долей уверенности о невозможности перехвата ключа в реальном времени.

Date: 5th June-2025

СПИСОК ЛИТЕРАТУРЫ:

1. Дворянкин С.В. Речевая подпись / Под ред. заслуженного деятеля науки РФ, д.т.н., проф. А.В. Петракова. – М.: РИО МТУСИ, 2003 – 184 с.
2. Отчет по НИР «Методы защиты сетей СПС стандарта GSM от несанкционированного доступа», ЗАО «Институт сотовой связи», 2004 г.
3. Рабинер Л.Р., Шафер Р.В. Цифровая обработка речевых сигналов: Пер. с англ./Под ред. М.В. Назарова, Ю.Н. Прохорова.– М.: Радио и связь, 1981.– 495 с
4. www.cnews.ru

