Biometric methods of information protection

Mukapil K.– Beketova G. – Zhumagalieva N. – Tulemisova V. – Kultan J.

Abstract

Considers biometric methods of information protection. The comparative analysis of technologies to protect the information using „fuzzy extractors" and high dimensional neural network converters biometrics code. A description of threats of biometrics systems, neural network authentication.

The aim of the article is the analysis of identity authentication methods on the basis of three basic methods: by ownership of knowledge and biometrics. It is also considered the separation of biometrics on the physiological and behavioral resorting to their basic properties – universality, uniqueness, consistency and measurability. Given these factors make the analysis of identity authentication methods and systems using these parameters. The following provides an overview of the technology of information security and personal identification. The last part of the article focused on the analysis of some of the threats to the biometric authentication systems.

The article is an analysis of the current status and new opportunities for the development of information security systems

Keywords:

biometrics, biometric identification, biometric authentication systems, biometric technology, information security, a neural network.

ACM Computing Classification System:

Security and privacy – Security services – Authentication -Biometrics

Введение

Сегодня все большее число организаций переходят на электронный документооборот. Используются централизованное и распределенное хранение данных, облачные технологии. Наблюдается резкая активизация граждан в использовании услуг электронного правительства. Все это приводит, с одной стороны, к увеличению объема информации, в том числе и конфиденциальной. С другой стороны растет число потенциальных нарушителей, стремящихся получить доступ к ней. Поэтому еще большую актуальность приобретает проблема надежной защиты информации организаций и граждан, циркулирующей в сети Интернет [1-4].

К сожалению, до сих пор Интернет остается анонимной, обезличенной средой с низким доверием к ней. Это, с одной стороны, является питательной средой для разного рода мошенников, а с другой стороны подрывает доверие обычных граждан к электронному правительству. На рисунке (Рисунок 1) приведены данные аналитического центра InfoWatch [5], который ведет мониторинг официально опубликованных утечек информации в различных структурах по всему миру и

выпускает ежегодный аналитический отчет, включающий статистический анализ зафиксированных случаев утечки информации с комментариями экспертов. Например, только по вине медицинских учреждений в мире скомпрометировано 54,1 миллиона записей.

Рисунок 1 Утечка данных в различных структурах

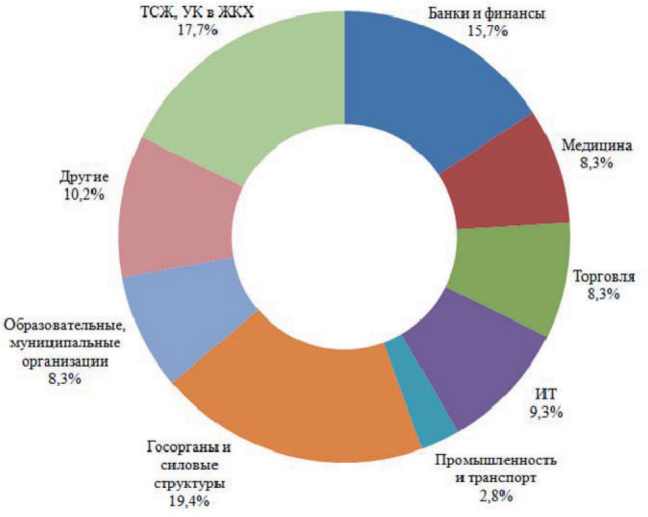

Рисунок 1: *Утечка данных в различных структурах [5]*

Поэтому следует создавать новые технологии, которые с одной стороны гарантировано обеспечивают надежную аутентификацию граждан при доступе к услугам Интернет, а с другой стороны обеспечивают высокий уровень доверия к ней.

1 Методы аутентификации личности

В настоящее время используется три традиционных способа аутентификации личности (Рисунок 2) [6]:

- по собственности – физическим предметам, таким, как ключ, паспорт, смарт-карта;
- по знаниям – информация, которая хранится в секрете и которую знает только определенный человек, например пароль;
- по биометрическим параметрам – физиологическим или поведенческим характеристикам личности. Это индивидуальные особенности строения органов и частей человеческого тела или действия, характерные для конкретного человека, по которым можно отличить людей друг от друга.

На сегодня основным способом аутентификации личности при доступе к информационным системам остается парольная защита. Основной проблемой па-

рольной аутентификации является то, что большинство пользователей не в состоянии держать в памяти длинные пароли из случайных символов. Поэтому, как правило, используются пароли, состоящие из 5-8 символов. Стойкость защиты к атакам подбора пароля составляет 10^{10}-10^{16} попыток подбора при условии, что символы пароля случайны.

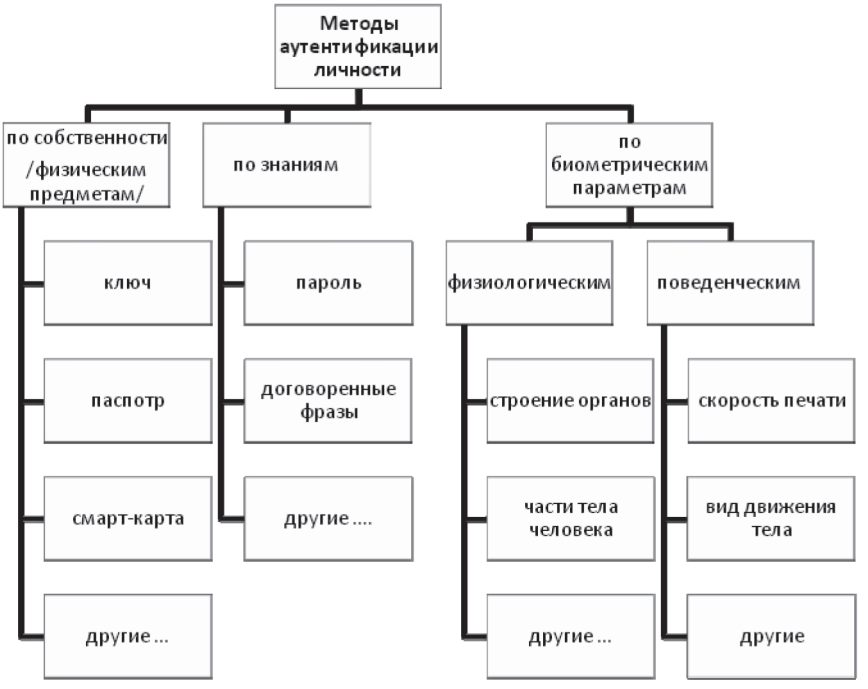

Рисунок 2: *Разделение методов аутентификации*

Стандартный компьютер Pentium 4 – 3 ГГц позволяет перебирать 10^7 вариантов паролей за одну секунду. Это означает, что по извлеченной из системы аутентификации хэш-функции пароля злоумышленник подберет нужный пароль примерно за 12 минут (проверив 10^{10} вариантов для пароля из 5 символов), одни сутки (проверив 10^{12} вариантов для пароля из 6 символов), три месяца (проверив 10^{14} вариантов для пароля из 7 символов), 21 год (проверив 10^{16} вариантов для пароля из 8 символов).

В связи со сложностью запоминания случайных символов пароля пользователи стараются применять в качестве пароля слова родного языка. При этом отмечается резкое снижение стойкости парольной защиты. Для слова из 8 символов стойкость составит только 10^5 попыток, подбор такого пароля займет несколько минут машинного времени современного компьютера.

Проблемой парольной защиты является обезличенность пароля при его вводе. Одним из путей решения данной проблемы является использование биометрических параметров самого пользователя в качестве пароля. Биометрические параметры делятся на физиологические и поведенческие, а также обладают и другими свойствами, без которых невозможно их практическое применение [6]:

Всеобщность: каждый человек имеет биометрические характеристики.

Уникальность: не существует двух людей, обладающих полностью одинаковыми биометрическими характеристиками.

Постоянство: биометрические характеристики должны быть стабильны во времени.

Измеряемость: биометрические характеристики должны быть измеряемы каким-либо физическим считывающим устройством.

Также очень важным свойством является *приемлемость*. Оно менее всего связано с каким-либо определенным биометрическим параметром, однако без его учета нельзя создать полную картину эффективности использования биометрических систем. Комбинация всех перечисленных выше свойств определяет эффективность биометрических систем аутентификации [6, 7].

В настоящее время не существует биометрических параметров, которые сочетали бы в себе все эти свойства одновременно, особенно если учитывать приемлемость. Поэтому, любой метод биометрической аутентификации является результатом многих компромиссов [6, 7].

2 Биометрические методы аутентификации личности

Существующие в настоящее время средства аутентификации, использующие биометрию человека, можно разделить на три ветви (Рисунок 3), учитывающие его статические (неизменяемые) характеристики, динамические (изменяемые) характеристики и их комбинации [6-7, 9-19].

К первой ветви относится большая группа биометрических систем, построенных на анализе статических (неизменяемых) образов личности, данных ей от рождения. Основным преимуществом статической биометрии является ее относительная независимость от психофизиологического состояния пользователей, малые временные затраты на регистрацию биометрических характеристик пользователей, относительно высокая стойкость подбора биометрического образа от 10^2 до 10^{13} попыток [6].

Существует множество механизмов анализа статических биометрических характеристик личности, из которых мы рассмотрим следующие:

– Анализ кровеносных сосудов глазного дна. Суть метода заключается в сканировании через зрачок сетчатки глаза. Пользователь должен приблизить глаз к регистрирующему устройству на расстояние в 1-1,5 см. Рисунок сетчатки измеряется в 400 точках.

Достоинства. Считается одним из самых надежных в настоящее время методов идентификации. По данным Сандийской национальной лаборатории (США), ошибки первого рода составляют 0,4 %. Ошибки второго рода не указаны.

Недостатки. Согласно статистическим данным лишь 80-90% пользователей могут с первого раза пройти процедуру регистрации.

Устройства распознавания по сетчатке глаза являются одними из самых дорогих - порядка 4000 долларов. Также данный метод имеет довольно сложную процедуру регистрации [6, 9].

Производством данных систем занимаются Iridian Technologies, Inc (США), Visionics FaceIt (США), Panasonic (CIS) OY (Япония).

Информации по хорошо подготовленным специальным атакам на этот тип биометрических устройств в настоящее время нет;

– Индивидуальные особенности геометрии лица. Суть метода заключается в создании двух- или трехмерного электронного образца, учитывающего индивидуальные особенности геометрии лица [6, 9].

Двухмерный электронный образ создается на основе набора биометрических данных и их обработки в виде определенного кода, относящегося к конкретной личности.

Недостатки. Идентификация ненадежна и изготовление муляжа-фотографии не является сложной технической проблемой.

Создание трехмерного образа близко к человеческому видению проблемы распознавания. Система самообучаема в отношении изменчивости лица – таких факторов, как возраст, наличие усов или бороды, очков.

Достоинства. Сложность изготовления муляжа. Обмануть данный класс систем можно только объемной маской, точно воспроизводящей трехмерную геометрию лица-оригинала [6, 9].

Стоимость видеокамер для проведения видеоконференций составляет от 20 до 200 долларов. Стоимость программного обеспечения для идентификации пользователей по лицу колеблется от 40 до 200 долларов.

На производстве подобных систем специализируются компании FaceKey TMCorporation (США), Iritech Inc. (США), Identix Inc. (США), AcSys Biometrics (США), A4Vision (Швейцария) Cognitec Systems GmbH (Германия), ZN Vision Technologies AG (Германия), Vicar Vision (Голландия);

– Папиллярный рисунок пальцев руки. Суть метода заключается в регистрации с помощью специального устройства папиллярного узора с одного из пальцев пользователя и его сравнение с эталонным шаблоном базы [6-9, 12-14].

Достоинства. Самые массовые системы аутентификации – более 52% от всего количества производимых систем биометрической аутентификации. По оценкам производителей ошибки первого рода ≈ 2%, а ошибки второго рода на уровне 0,0001%.

Недостатки. Возможность изготовления муляжа [6, 9].

Стоимость биометрических систем данного класса снижается и в настоящее время составляет от 60 до 300 долларов [6].

Основные компании-разработчики: США – ATMEL, DigitalPersona Inc., Cross Match Technologies, Ethentica by Security First Corp., BioLink Technologies, Iridian Technologies Inc., Identix Inc., Sagem Morpho, Veridicom, Infineon, BioScrypt, SecuGen Corporation, Швейцария – Biometric Security AG, Швеция – Precise Biometrics, Венгрия – Guardware Systems Ltd., Россия – ЦентрИнвест Софт SCANTI-RUS, „Системы Папилон“;

Ко второй ветви относится группа биометрических продуктов, построенных на *анализе динамических биометрических образов личности*: из которых мы рассмотрим идентификации личности по голосу, рукописному почерку, клавиатурному почерку.

– Идентификация личности по рукописной подписи и динамике ее воспроизведения. Суть метода – идентификация личности по подписи, которую автор сам вырабатывает и закрепляет повседневной тренировкой. Подпись должна иметь существенные отличия по форме от классического написания букв в виде дополнительных элементов (росчерков, возвратов, наложения букв) [6, 15-17, 23].

Выделяют два способа обработки данных о подписи: простое сравнение с образцом и динамическую аутентификацию [6, 9, 15-16]. Первый способ прост, но ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Известные на сегодня технические решения по вероятностным характеристикам существенно хуже, чем статистика работы экспертов. Именно по этой причине фирмы-производители не дают статистических данных об ошибках первого и второго рода для идентификации автора по „мертвому“ статическому образу его подписи.

Достоинства. Простота и доступность использования.

Второй способ динамической аутентификации требует более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие, как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи.

Достоинства:

Динамическую подпись сложно подделать. Практически никто не в состоянии в точности скопировать и воспроизвести динамику движения руки истинного владельца подписи, так как эти навыки вырабатываются у человека в течение достаточно длительного времени и после этого долго остаются неизменными.

Приемлемая для требований сегодняшнего дня ошибка первого рода – 0,01.

Защита от визуального наблюдения образ начертания подписи, воспроизводимого на графическом планшете, сенсорном экране коммуникатора или карманного персонального компьютера в режиме скрытого ввода подписи.

Доступная процедура аутентификации. Пользователь, используя стандартный графический планшет с электронным пером, воспроизводит свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных. При совпадении образа подписи с биометрическим шаблоном (эталоном) система прикрепляет к подписываемому документу информацию, включающую имя пользователя, адрес его электронной почты, должность, текущее время и дату, параметры шаблона подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение) и др. Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал. Впервые данную технологию использовала компания PenOp.

Низкая стоимость и простота реализации. Стоимость графических планшетов уменьшается и в настоящее время составляет от 40 до 70 долларов. Все коммуникаторы и карманные компьютеры уже сегодня имеют возможность рукописного ввода на сенсорнНедостатки:

Вероятность ошибки второго рода – 0,01 для отдельных приложений является неприемлемо большой величиной. Для снижения этой ошибки используют идентификацию по динамике воспроизведения биометрического слова-пароля. Автором сохраняется в секрете, как сам пароль, так и его особенности написания. В этом случае главной оказывается не сама биометрия, а тайна пользователя – пароль. Увеличивая длину воспроизводимого слова-пароля, можно добиться малой вероятности ошибки второго рода.

Зависимость параметров динамического ввода подписи от психофизиологического состояния людей и стабильности их почерка.

В настоящее время разработкой данных систем занимаются компании PenOp, Cybersign, Communication Intelligence Corporation.

– Аутентификация личности по клавиатурному почерку. Суть метода – идентификация личности по клавиатурному вводу информации всеми пальцами обеих рук. Только при выполнении этого условия, у каждого человека появляется свой уникальный клавиатурный почерк. При вводе парольной фразы биометрическая система фиксирует время нажатия каждой клавиши и интервал времени между нажатием очередной клавиши и отпусканием предыдущей клавиши [6, 23].
– Весьма важной характеристикой этой технологии биометрической аутентификации является длина парольной фразы. Практика показывает, что парольная фраза должна быть легко запоминаемой и содержать от 21 до 42 нажатий на клавиши. При синтезе парольной фразы допустимо использование слов со смыслом из некоторого словаря. В отличие от классических паролей, при наборе длинной парольной фразы допустимы ошибки в одном или двух символах, что несколько ухудшает стойкость парольной фразы к статическому подбору, но зато значительно снижает вероятность ошибки первого рода.

Биометрический эталон ввода парольной фразы получают вычислением математических ожиданий и дисперсий контролируемых параметров. При вычислениях крайне важным является исключение из обучающей выборки аномальных выбросов [6].

Недостатки. Обычные пользователи, как правило, не имеют достаточно устойчивого клавиатурного почерка, пригодного для аутентификации личности, поэтому данный способ биометрической аутентификации малопригоден для подавляющего большинства пользователей.

Компания Net Nanny Software International разрабатывает программный продукт под названием BioPassword, расширяющим защитные свойства обычных парольных систем, задача которого состоит в анализе динамики ввода текста.

Компании, специализирующиеся на производстве и продвижении подобных биометрических систем: Cyber-SIGN Incorporated (США), Communication Intelligence Corporation (США), BioPassword Security Software, Inc. (США).

– Аутентификации личности по особенностям голоса. Метод аутентификации личности по особенности голоса строится на частотных методах или линейных предсказателях речевого сигнала.

В основу частотного метода положены различная тембральная окраска голосов и индивидуальная неравномерность распределения мощности произносимой фразы

по частотному спектру [6, 16, 23]. Базовыми процедурами для этого класса устройств являются узкополосная фильтрация сигнала и восстановление его огибающей.

Недостаток частотного метода. Фрагменты кривых $A_k(t)$, соответствующих шипящим звукам, должны обязательно исключаться из данных, по которым принимается решение, так как их учет может только ухудшить качество идентификации.

Системы аутентификации с линейными предсказателями речевого сигнала используют описание сигнала во временной области. В основу кодирования речи методом линейного предсказания положена волновая структура речевого сигнала, особенно хорошо наблюдаемая при произношении гласных. Метод линейного предсказания построен на аппроксимации соседних волн в звуковой пачке переходным процессом некоторого линейного цифрового фильтра. Исходный сигнал разбивается на отдельные интервалы анализа фиксированной длины – обычно 20 мс. Далее осуществляют определение типа звука внутри интервала анализа (шум или тональный звук). Если внутри интервала находится шумовой участок, то определяются только его энергетические параметры $A_0(t)$. Если внутри интервала анализа присутствует тональный фрагмент, то сигнал дополнительно описывают путем задания коэффициентов линейного предсказателя (линейного цифрового фильтра) и задания периода импульсов основного тона, возбуждающих переходные процессы на выходе линейного предсказателя.

Основным недостатком использования линейных предсказателей с рекурсивной структурой является их потенциальная неустойчивость из-за наличия обратной связи.

Еще одним подходом к решению задачи является использование устойчивого линейного предсказателя с нерекурсивной структурой. В этом случае его коэффициенты $\{a_1, a_2, a_3,\ldots, a_k\}$ повторяют импульсную переходную функцию h(t), но для точного описания импульсной переходной функции h(t) число коэффициентов существенно увеличивается. Формально вектор коэффициентов линейного предсказателя может быть получен непосредственно из параметров звуковой волны без решения системы линейных уравнений, однако для этого требуется знать период импульсов основного тона и моменты прихода импульсов основного тона на вход линейного предсказателя. В первом приближении моменты времени прихода импульсов возбуждения основного тона могут быть найдены как левое пересечение нулевого уровня максимальным по модулю импульсом.

Независимо от типа используемых процедур предварительной обработки, после дробления парольной фразы на последовательные интервалы наблюдения и их обработки получают описание особенностей голоса личности в виде характерных функций $T_0(t)$, $A_0(t)$ и системы функций коэффициентов линейного предсказателя $\{a_1(t), a_2(t), a_3(t),\ldots, a_k(t)\}$. Все эти данные обладают существенной индивидуальностью, но они должны быть правильно фрагментированы на отдельные фонемы и приведены к единому масштабу времени и амплитуды.

При обучении система идентификации личности по голосу анализирует несколько произношений парольной фразы и создает биометрический эталон, определяя наиболее вероятные значения функций $T_0(t)$, $A_0(t)$, $a_1(t),\ldots, a_k(t)$ для регистрируемого пользователя и допустимые для него отклонения этих функций от средних значений.

Достоинства. Аутентификация по голосу является традиционной для людей и не вызывает психологической неприязни. Для отдельных граждан аутентификация по голосу является основным способом узнавания личности [6, 17].

В качестве недостатка биометрических систем аутентификации личности по голосу необходимо отметить то, что парольную фразу трудно сохранить в тайне. Современные средства акустического прослушивания позволяют достаточно успешно осуществлять несанкционированное копирование парольной фразы. Ожидается, что исключение опасности использования злоумышленниками „магнитофонов" произойдет при переходе к идентификации личности на произвольных фразах.

По данным независимого тестирования Сандийской национальной лабораторией (США) ошибки первого и второго рода составляют для голосовых систем от 2 до 1% [6]. Эта технология рассматривается как наиболее часто используемая по динамическим (поведенческим) параметрам.

Разработкой и продвижением такого рода систем занимаются T-Netix (США), Lone Wolf Software (США), Veritel (США), ITT Nuance (США), SPIRIT Corp. (Россия).

На сегодняшний день биометрические системы аутентификации личности по голосу слабее аналогичных систем аутентификации по динамике почерка. Тайна парольной фразы оказывается много сильнее уникальности биометрических параметров. Парольную фразу, произнесенную голосом, труднее сохранить в тайне.

Описанные выше три метода динамической биометрии являются достаточно хорошо изученными. Эти методы со временем могут быть дополнены другими, которые в настоящее время находятся в процессе исследований:

– метод аутентификации личности по походке, которая считается одной из стабильных поведенческих характеристик человека [6];
– метод идентификации по движению губ. Аутентификация по движению губ имеет такие же разновидности, что и метод распознавания говорящего: с фиксированным текстом, зависимая от текста и не зависимая от текста. Исследования в этой области проводятся компанией «Biold». Достоинство метода заключается в возможности совмещения его с идентификацией говорящего и распознаванием по геометрии лица. Любое рассогласование речи и изображения может быть признаком атаки воспроизведения [6];
– метод идентификации по уникальности движений глаз. Система, разработанная компанией ID-U Biometrics (Израиль), отслеживает уникальные образцы движения глаз человека, которые являются сугубо индивидуальной чертой [6]. Система работает с компьютером и обычной видеокамерой, которая следит за движением глаз. Человек должен отследить глазами движение символа на экране, при этом траектории движения могут выбираться в случайном порядке, что существенно повышает безопасность всей системы.

Данные, полученные с помощью камеры, проходят обработку специализированным программным обеспечением, которое на основании занесенных в базу данных движений производит точную идентификацию личности человека. Данная система является первой системой биометрической идентификации, использующей уникальность реакций на внешние раздражители. Достоинством системы является ее простота использования и дешевизна благодаря использованию обычного компьютера и

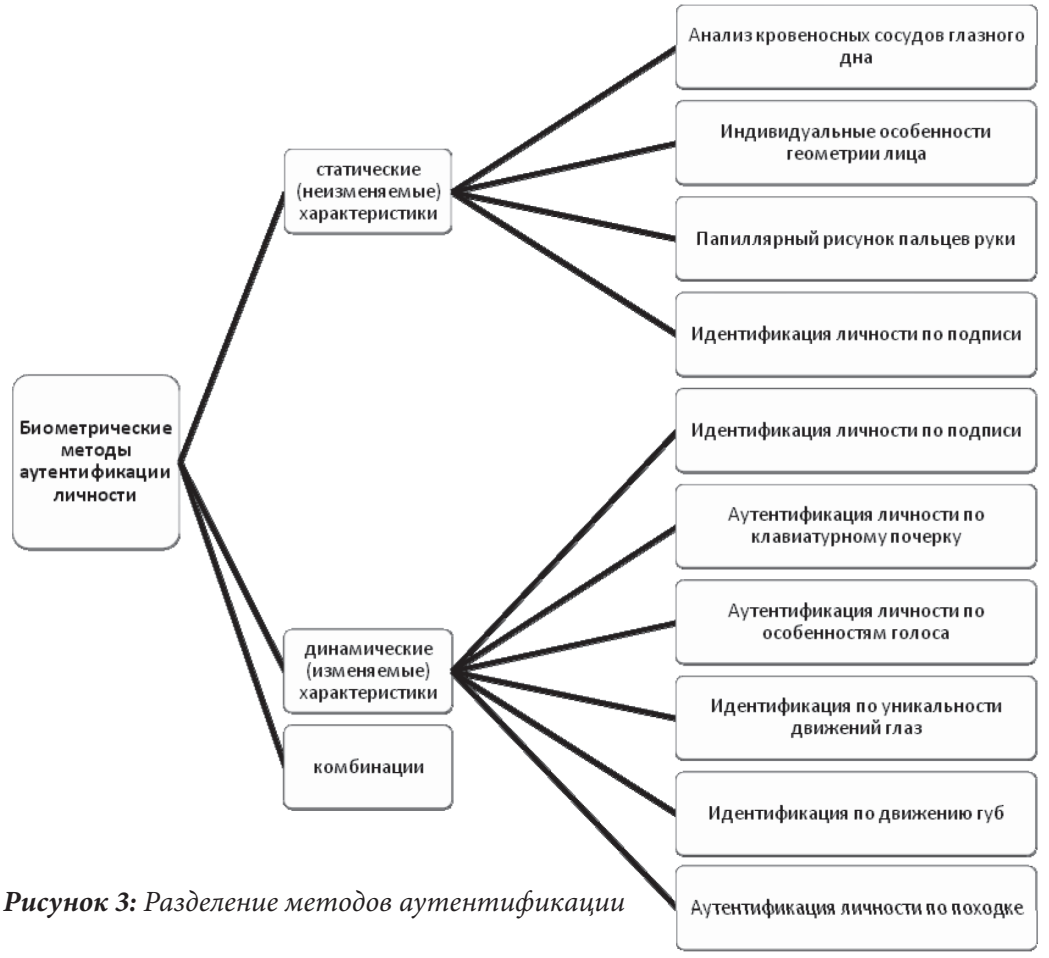

Рисунок 3: *Разделение методов аутентификации*

камеры. Так же программное обеспечение системы может работать на большинстве мобильных телефонов, оборудованных фронтальными видеокамерами.

К третьей ветви относятся биометрические системы, использующие несколько биометрических параметров человека, причем одновременно могут использоваться как статические, так и динамические характеристики. Например, системы аутентификации, использующие одновременно распознавание по отпечатку пальца, радужной оболочке глаза и рукописному паролю [19].

Основной целью построения мультибиометрических систем является уменьшение вероятности ложного доступа.

3 Технологии защиты информации и идентификации личности с использованием биометрии личности

На сегодняшний день исследованиями по преобразованию неоднозначных нечетких биометрических образов личности в полноценный ключ или длинный пароль занимаются в России, Белоруссии, Казахстане, США, Канаде, странах Ев-

росоюза и Южной Корее. Все преобразователи биометрии в код делятся на «нечеткие экстракторы» [30-41] и нейросетевые преобразователи биометрия-код [24-29]. Основной вклад в развитие технологии «нечетких экстракторов» внесли исследователи США, Канады, стран Евросоюза и Южной Кореи. Нейросетевые преобразователи биометрия-код разрабатываются усилиями исследователей России, Белоруссии и Казахстана. Отличие между этими двумя технологиями только в положении квантователя непрерывных биометрических данных.

3.1 Нечеткие экстракторы

В США, Канаде, странах Евросоюза и Южной Корее для решения вопроса идентификации предлагается использовать аппарат нечетких множеств. Основным преимуществом «нечетких экстракторов» англоязычная криптографическая общественность считала их относительно высокий уровень защищенности и простоту (прозрачность) используемой защиты. Принцип защиты данных «нечетких экстракторов» иллюстрируется рисунком (Рисунок 4) [29].

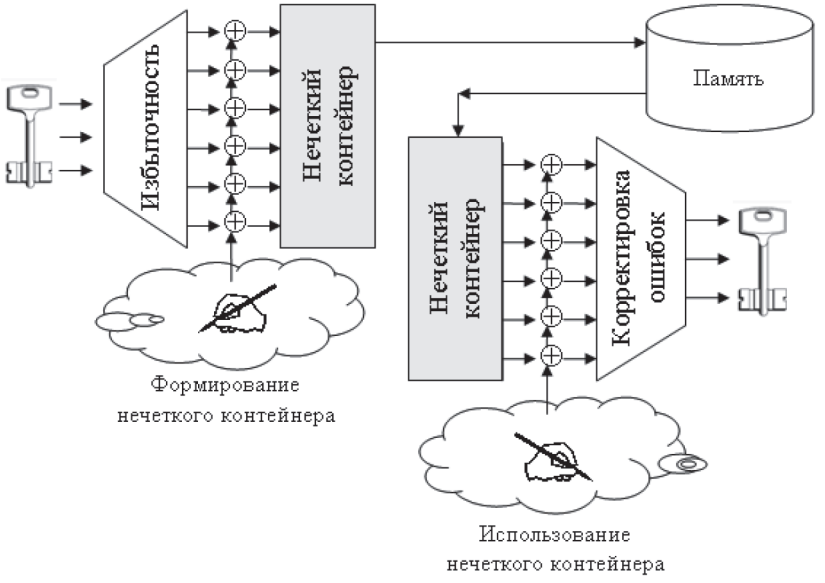

Рисунок 4: *Формирование и использование нечетких контейнеров*

Для защиты «сырых» био-кодов используют секретный ключ. Этот ключ накрывают избыточным самокорректирующимся кодом. Это может любой классический код, способный обнаруживать и исправлять ошибки. Обычно используются коды БЧХ (Боуза-Чоудхури-Хоквингема) и тем самым получают гамму в 10 раз длиннее кода секретного ключа. Далее накрывают «сырой» био-код гаммой, получая тем самым «нечеткий контейнер». «Нечеткий контейнер» хранят в памяти средств биометрической аутентификации. В США и странах НАТО такой способ считается

относительно безопасным, и именно эта ветвь технологий за рубежом активно развивается. Конструкции «нечетких экстракторов» даны в ряде англоязычных публикаций [30-41], в работах [20-22] отражены усилия русскоязычных исследователей этого технологического направления.

В процессе аутентификации «нечеткий контейнер» извлекают из памяти и складывают его данные по модулю два с введенным и оцифрованным биометрическим образом. При этом восстанавливается избыточный самокорректирующийся код криптографического ключа, содержащий ошибки, унаследованные от двух биокодов (био-коде формирования нечеткого контейнера и био-коде аутентификации). Если таких ошибок меньше, исправляющей способности самокорректирующегося кода, то они правятся.

Схема предлагаемой обработки информации показана на рисунке (Рисунок 5).

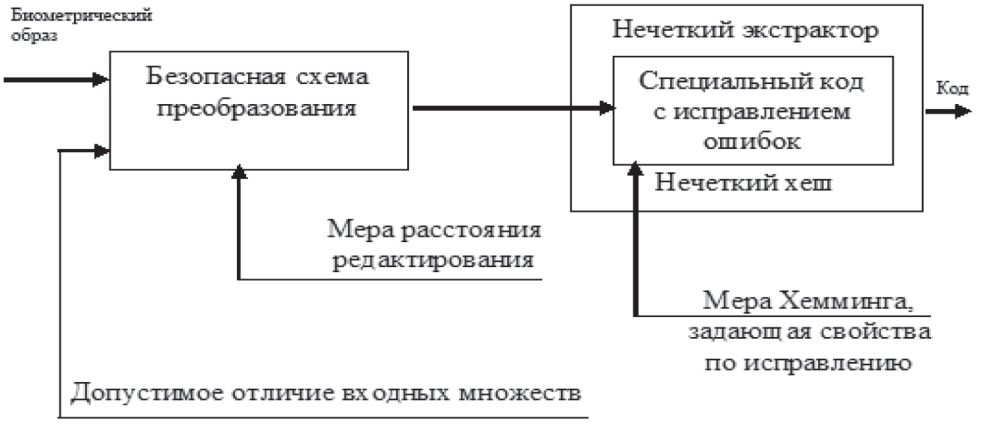

Рисунок 5: *Структурная схема преобразования нечетких биометрических данных личности в код*

Она начинается с использования некоторой безопасной схемы преобразования. Необходимо задать допустимую разность множеств, в рамках которой можно осуществлять преобразования. Если входное биометрическое воздействие не слишком сильно отличается от эталонного множества, то нечеткие преобразования могут быть осуществлены только при условии их безопасности.

Фактически эту технологию можно интерпретировать как синтез некоторой нечеткой хэш-функции с предварительной коррекцией входной последовательности заданной длины некоторым линейно взвешенным кодом с обнаружением и исправлением ошибок.

3.2 Биометрико-нейросетевая аутентификация

Исследования, проведенные в Казахстане, России и Белоруссии в последние годы показали, что существующие биометрические технологии могут быть значительно усилены за счет использования искусственных нейронных сетей [23, 25, 30-43]. Они

осуществляют обогащение данных в непрерывной форме и обычно для корректировки всех входных ошибок оказывается достаточно двукратной избыточности, то есть 512 входных биопараметров нейронная сеть преобразует в 256 бит выходного кода практически без ошибок.

С точки получения биометрических свойств нейросетевые преобразователи биометрия-код всегда лучше «нечетких экстракторов». Этот тезис никто не оспаривает. Это легко продемонстрировать на примере плохих биометрических данных, дающих ошибки в 50% и более разрядах био-кода. Скорректировать больше 50% ошибок классические самокорректирующиеся коды не способны, нейронные сети с этой проблемой справляются, если избыточность их становится трехкратной (входов в три раза больше, чем выходов).

Переход к использованию больших нейронных сетей позволяет учитывать наряду с «хорошими» биометрическими данными «плохие» биометрические данные и «очень плохие» биометрические данные. При этом чем «хуже» используемые биометрические данные, тем больше должна быть сеть искусственных нейронов и тем сложнее ее обучать. Общая структура системы биометрико-нейросетевой аутентификации показана на рисунке (Рисунок 6).

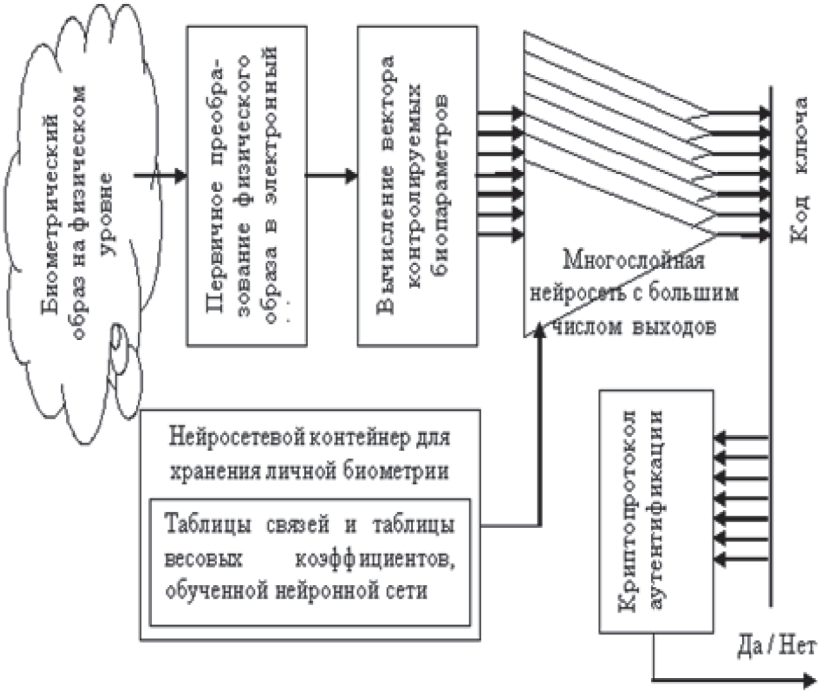

Рисунок 6: *Общая структура системы биометрико-нейросетевой аутентификации*

При этом необходимо отметить, что для решения подобной задачи искусственные нейронные сети низкой размерности непригодны [25-26].

Процесс преобразования входного биометрического образа в выходной длинный пароль (ключ) можно представить в виде схемы на рисунке (Рисунок 7) [44].

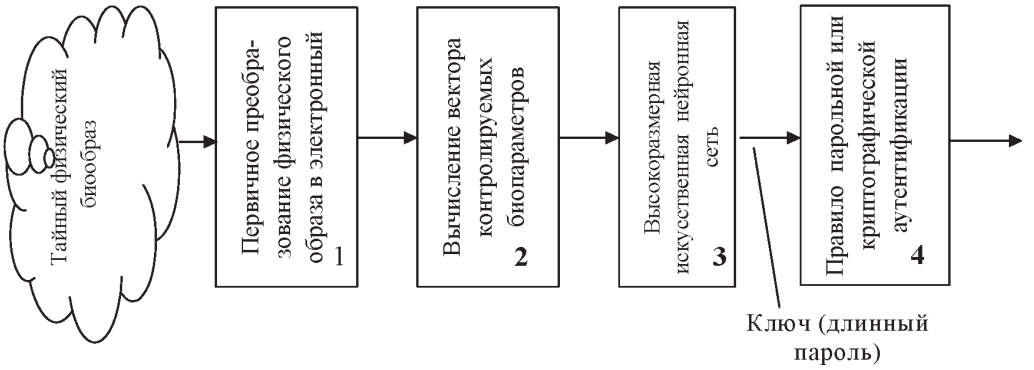

Рисунок 7: *Структурная схема обработки информации в системах биометрико-нейросетевой аутентификации*

Схема обучения нейросетевого преобразователя векторов биометрических параметров в код ключа (пароля) представлена схемой на рисунке (рис. 8) [25, 44].

Обучение искусственной нейронной сети должно осуществляться автоматически (без вмешательства человека в процесс подбора параметров искусственной нейронной сети), пользователь должен иметь гарантии того, что его длинный пароль (ключ), участвующий в обучении, не будет скомпрометирован.

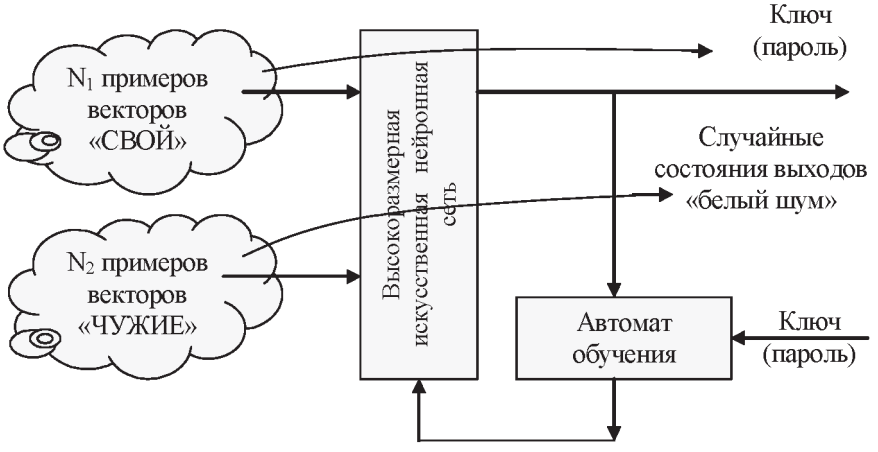

Рисунок 8: *Структурная схема обучения нейросетевого преобразователя*

При обучении весовые коэффициенты искусственной нейронной сети должны подбираться автоматом обучения таким образом, чтобы при появлении на входах искусственной нейронной сети элементов вектора «Свой» на выходах искусственной нейронной сети появлялся длинный пароль (ключ). При появлении на входах искусственной нейронной сети векторов данных, соответствующих образам «Чужой», на выходах искусственной нейронной сети должны появляться случайные состояния – «белый шум». Обучение осуществляется путем поочередного предъявления образов «Свой» и «Чужие» с промежуточным подбором коэффициентов.

Для обучения искусственной нейронной сети были разработаны быстрые алгоритмы обучения [24-25, 44]. Их особенностью является послойное обучение нейронов искусственной нейронной сети. При этом решается только линейная часть задачи (нахождение только оптимальных весовых коэффициентов сумматоров). Нелинейную модификацию найденного нейросетевого линейного решения предложено осуществлять по заранее построенным таблицам оптимизации параметров нелинейных элементов искусственных нейронов. В этом случае сложность задачи обучения искусственных нейронных сетей оказывается квадратичной. Вычислительная сложность оказывается не выше кубической при наихудшем по быстродействию алгоритме определения оптимальных весовых коэффициентов через обращение ковариационных матриц.

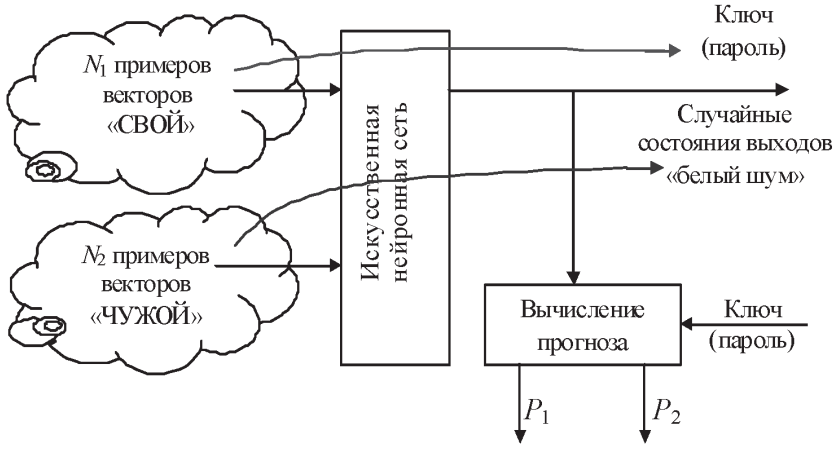

Рисунок 9: *Структурная схема тестирования системы биометрико-нейросетевой аутентификации после обучения*

После обучения системы биометрико-нейросетевой аутентификации необходимо оценить качество обучения. Оцениваются вероятность ошибки первого рода P_1 и вероятность ошибки второго рода P_2.

Пользователь должен знать реальные оценки стойкости к атакам подбора конкретной реализации биометрической аутентификации после ее обучения, построенной на воспроизведении конкретного тайного биометрического образа. Тестирование осуществляют, используя N_1 – тестовых примера векторов образов «Свой» и N_2 – тестовых примера векторов образов «Чужой». Структурная схема тестирования приведена на рисунке [44].

4 Угрозы для систем биометрико-нейросетевой аутентификации

Для систем биометрико-нейросетевой аутентификации существует ряд угроз (Рисунок 10) [23, 25, 44]. К ним относятся:

– *компрометация тайного биометрического образа человека на физическом уровне.* Угроза компрометации тайного биометрического образа является самой существенной. Может быть снижена за счет проведения биометрической аутентификации только в контролируемой зоне; за счет гашения экрана карманного компьютера при воспроизведении рукописного пароля; за счет периодической смены тайного биометрического образа (биометрического пароля) пользователя по аналогии со сменой обычных паролей;
– *перехват тайного электронного образа человека в виде его биометрических данных или в виде вектора его биометрических параметров.* Подмена или модификация программного обеспечения обработки биометрической информации позволяет получить (скомпрометировать) тайный электронный биометрический образ человека. Человек не чувствует подмену, если не обеспечен системой специального контроля целостности программного обеспечения и контроля функций вычислительных процессов, идущих параллельно с биометрической аутентификацией. Реализация этой угрозы через соответствующую атаку подмены программного обеспечения или его модификации – это один из самых простых и вместе с тем эффективных путей. Данная угроза снижается путем контроля целостности используемого программного обеспечения и контроля действий (аудита) вычислительных процессов, идущих параллельно процедурам биометрико-нейросетевой аутентификации. Возможен частичный или полный перенос всех операций в специализированную вычислительную среду.

Если биометрическое программное обеспечение имеет чеки целостности и перед запуском идет их проверка, то исключается возможность подмены. При этом необходимо обеспечить надежное хранение чеков целостности, так как их могут подменить вместе с программным обеспечением. Поэтому чеки целостности необходимо хранить отдельно от программного обеспечения. Пользователь может иметь свой носитель информации с чеками целостности, подключение этого носителя и сравнение с его чеками целостности проверок будут являться гарантией того, что программное обеспечение биометрической системы не искажено.

При обнаружении факта перехвата или при выявлении условий, с высокой вероятностью приводящих к перехвату электронного биометрического образа пользователя, рекомендуется изменить биометрический образ и далее его менять периодически так же, как в случае использования обычных парол*случайный подбор тайного биометрического образа на физическом уровне.* Эта новая угроза, и может быть реализована путем хищения у человека образцов его рукописного почерка. Естественно, что для этого должны быть собраны значительные объемы биометрической информации (несколько страниц рукописного текста, воспроизведенного на графическом планшете легальным пользователем). Появляется возможность построить имитатор конкретного человека, например, использующий подстановки фрагментов подлинной биометрии в их разных комбинациях. Тогда, даже не зная биометрического пароля, но, зная, что этот пароль является коротким словом языка пользователя или его модификацией, можно попытаться перебирать варианты биометрических паролей с учетом их модификации и проверки близлежащих комбинаций континуумов биометрических образов.

Угроза может быть уменьшена за счет ограничения числа предоставляемых пользователю попыток аутентификации и за счет увеличения качества рукописного пароля (увеличения числа слов рукописного пароля и числа букв в слове, введения обратных росчерков, тренировок по стабильному написанию рукописного пароля).

Гарантией снижения вероятности подбора тайного биометрического образа на физическом уровне является наличие в биометрическом продукте защиты системы контроля качества биометрических паролей. Такая система исключает использование слишком слабых паролей. Подбор сильных биометрических паролей технически очень сложен из-за трудностей автоматического синтеза комбинаций биометрических данных, воспроизводящих рукописный почерк пользователя;

– *случайный подбор электронного тайного биометрического образа (вектора биометрического параметра образа).* Для синтеза случайных входных данных достаточно задать их возможный динамический диапазон и в этом диапазоне синтезировать случайные независимые данные, с последующей их подстановкой на входы искусственной нейронной сети. Поэтому наличие внутреннего контроля качества обучения искусственной нейронной сети в системах биометрико-нейросетевой аутентификации является обязательным элементом [44-46].

Еще одним важным моментом является частичная компрометация тайны биометрического образа (например, средства перехвата дали только половину биометрического образа), тогда атака случайного подбора оставшейся части биометрического электронного образа также может оказаться эффективной.

Угроза случайного подбора электронного тайного биометрического образа может быть уменьшена путем увеличения числа входов и выходов искусственной нейронной сети, увеличения числа слоев нейронов и числа связей у каждого нейрона.

Кроме того, сама искусственная нейронная сеть может быть сделана недоступной для злоумышленников, например, может быть введен запрет на вынос систем биометрико-нейросетевой аутентификации с защищенной территории;

– *извлечение конфиденциальной информации из структуры и параметров искусственной нейронной сети.* На данный момент пока не создано систем, позволяющих проводить анализ и извлекать конфиденциальную информацию из структуры и параметров искусственных нейронных сетей. В случае их появления потребуется увеличить сложность обратного преобразования за счет соответствующего увеличения числа слоев сети, числа входов у нейронов. На данный момент известно, что и число слоев нейронов и число входов экспоненциально влияют на рост вычислительной сложности обратных преобразований;
– *угроза саботажа и нелояльности пользователя при обучении искусственной нейронной сети.* Практика показывает, что пользователи могут относиться отрицательно к усилению персональной ответственности за их действия. Пользователь пытается специально писать неустойчиво при обучении системы, а затем небрежно воспроизводить рукописный пароль при входе в нее. Это новая угроза. Она ослабляется, если система имеет средства автоматизированного тестирования и предсказания ожидаемой стойкости;

– *сговор* – это традиционная угроза (недобросовестный пользователь может специально передать свой пароль другому лицу). Данная угроза с введением биометрии ослабевает. Трудно научить другого человека достаточно эффективно воспроизводить почерк легального пользователя. Угроза может быть ослаблена при аутентификации по длинному составному ключу (паролю), каждая часть которого связана своей искусственной нейронной сетью со своим пользователем. Пользователи и администратор безопасности могут создать общий ключ только совместными усилиями, контролируя друг друга;
– *некорректное поведение администратора безопасности системы биометрико-нейросетевой аутентификации.* В системах биометрической аутентификации данная угроза снижается, если система настроена только на биометрические образы пользователя. Тогда нет необходимости посвящать администратора в тайну биометрического образа и длинного пароля (хранение длинного пароля пользователя осуществляется в запечатанном конверте в специальном сейфе);
– *неадекватная оценка уровня стойкости биометрико-нейросетевой системы аутентификации.* Биометрический образ пользователя, преобразованный биометрико-нейросетевой системой аутентификации, может оказаться много эффективнее классической парольной (ключевой) защиты, но и намного слабее ее при неудачном стечении обстоятельств;

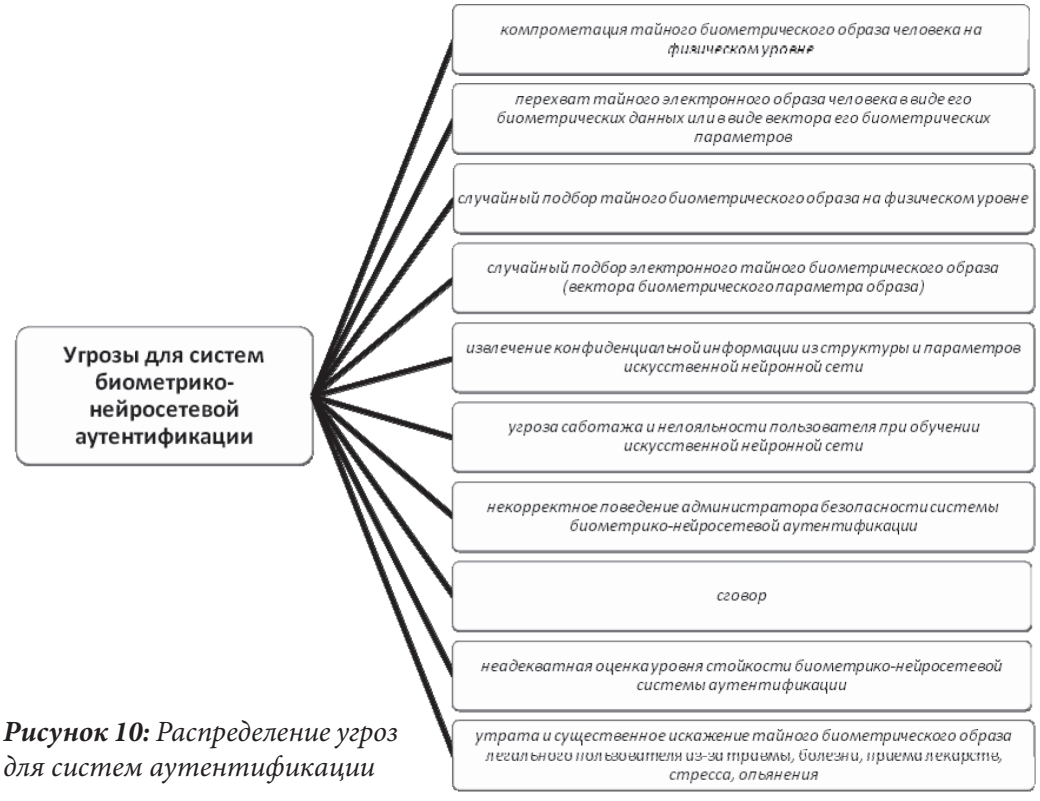

Рисунок 10: *Распределение угроз для систем аутентификации*

– *утрата и существенное искажение тайного биометрического образа легального пользователя из-за травмы, болезни, приема лекарств, стресса, опьянения.*

Это новая угроза, которая связана с тем, что в стрессовом состоянии у человека могут резко меняться параметры рукописного почерка. Кроме того, возможны заболевания и травмы рук. Опьянение, прием некоторых лекарств наркотического действия также могут приводить к утрате возможности доступа к информации через биометрические технологии защиты.

Данная угроза 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 хранится в сейфе, а доступ через него является нештатным. Рекомендуется введение в штатные системы аутентификации выходных проверок на соответствие полученного ключа действительному ключу, исключающих компрометацию.

Заключение

В связи с тем, что на данный момент не существует систем биометрической аутентификации, полностью удовлетворяющих требованиям обеспечения безопасности, разработчики пытаются совместить разные биометрические системы в одну мультибиометрическую систему [6]. К примеру, могут быть объединены в системе анализ голоса и рукописного почерка пользователя. Естественно, что при комбинировании нескольких биометрических систем должны быть проработаны механизмы их объединения.

Наиболее сильный вариант защиты системы аутентификации может быть получен, если воспользоваться последовательным механизмом объединения разнородных биометрических систем. Для этого используется составной ключ, каждый фрагмент которого формируется своей биометрической системой. При таком подходе получить общий ключ доступа можно только последовательно пройдя все биометрические системы аутентификации. Длина каждого фрагмента общего ключа должна быть пропорциональна стойкости формирующей его системы. Системы с низкой стойкостью к атаке случайного подбора имеют укороченные фрагменты общего ключа. Наоборот, более стойкие системы должны иметь более длинные его фрагменты [45].

Основное достоинство мультибиометрической системы аутентификации заключается в возможности компенсирования недостатков одних биометрических систем за счет преимущества других.

Вопросами разработки систем аутентификации занимаются многие научные и производственные организации. Предполагаем разработку системы, которая будет не объедением нескольких систем соединенных между собой параллельным или серийным способом. Вероятность ошибки /отказа/ в таких системах является соединение вероятности отказа каждой из систем. Создание системы, которая объединит напр. анализ параметров лица и параметры характеристик глаза в одно целое, позволит создать информационную структуру, которую будет тяжелее преодолеть.

Список использованных источников

[1] Ахметов Б.С., Алисов В.А., Вятчанинов С.Е. Нейросетевая мультибиометрическая аутентификация личности гражданина в системе электронного правительства // В сборнике трудов Международного симпозиума «Надежность и качество – 2012». – Пенза: Изд-во ПГУ, 2012. – Т.1. – С. 227-229.

[2] Akhmetov B., Kartbayev T., Volchihin V., Ivanov A., Malygin A. Highly Reliable Human-Being Personality's Multi-Biometric Authentication to Support Citizens Interaction // Global Journal on Technology. – North America, 2013. // http://www.world-education-center.org/index.php/P-ITCS/article/view/1728.

[3] Akhmetov B., Doszhanova A., Ivanov A., Kartbayev T. and Malygin A. Biometric Technology in Securing the Internet Using Large Neural Network Technology // WorldAcademy of Science, Engineering and Technology. – Singapore, 2013, july. – Issue 79. – P. 129-138 // http://www.waset.org.

[4] Akhmetov B.S., Ivanov A.I., Kartbayev T.S., Malygin A.Yu., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space. // International Journal of Computer technology and Applications. – India, 2013 – Vol. 4, Issue 5. – P. 846-855.

[5] Материалы сайта Группы компаний InfoWatch // http://www.infowatch.ru/analytics.

[6] Руд Б. Руководство по биометрии. – М.: Техносфера, 2007. – 368 с.

[7] ГОСТ Р ИСО/МЭК 19794-2-2005. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Данные изображения отпечатка пальца - контрольные точки. – М.: Стандартинформ, 2006. – Ч.2. – 42 с.

[8] Иванов А.И., Фунтиков Д.А., Агафонов С.Л. Прогнозирование уровня защищенности, обеспечиваемого папиллярным рисунком отпечатка пальца // Современные технологии безопасности. – 2005. – №3(14). – С. 36-37.

[9] Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.

[10] ГОСТ Р ИСО/МЭК 19794-6-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Данные изображения радужной оболочки глаза. – М.: Стандартинформ, 2007. Ч.6. – 28 с.

[11] ГОСТ Р ИСО/МЭК 19794-5-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Ч.5. Данные изображения лица. – М.: Стандартинформ, 2006. – 42 с.

[12] ФунтиковД.А. Крупкин А.Ю. Особенности использования термочувствительных сканеров отпечатков пальцев // Современные технологии безопасности. – 2005. – №1(12). – С. 34-36.

[13] ISO/IEC 1.37.19794.2 Biometric Data Interchange Format-Part 2: Finger Minutiae // http://www.incits.org/tc_home/m1htm/docs.

[14] ISO/IEC 1.37.19794.3 Biometric Data Interchange Format-Part 3: Finger Pattern // http://www.incits.org/tc_home/m1htm/docs.

[15] Иванов А.И.,СорокинИ.А., Кологоров В.А. Масштабирование сигналов в системах биометрической аутентификации по динамике подписи // Новые промышленные технологии. – 1998. – №6. – С. 37-41.

[16] Иванов А.И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем: дис.док. техн. наук: 05.13.01. – Пенза, 2002. – 383 с.
[17] Пат. 2148274РФ. Способ идентификации личности по особенностям подписи / А.И. Иванов, И.А. Сорокин, В.Л. Бочкарев, В.А. Оськин, В.В. Андрианов; опубл. 2000, Бюл. №12.
[18] ИвановА.И. Идентификация человека по особенностям его голоса // Современные технологии безопасности. - 2003. - №3. - С. 25-28.
[19] European ACTS projects. M2VTS Project: multi-modal biometric person authentication // http://www.tele.ucl.ac.be/ PROJECTS/M2VTS.
[20] Чморра А.Л. Маскировка ключа с помощью биометрии // Проблемы передачи информации. – 2011. – № 2(47). – С. 128-143.
[21] Пат. 2316120 РФ. Биометрическая система аутентификации / А.Л.Чморра, А.В. Уривский; опубл. 27.01.2008, Бюл. №3.
[22] Ушмаев О.В., Кузнецов В.В. Алгоритмы защищенной верификации на основе бинарного представления топологии отпечатка пальцев // Информатика и ее применения. – 2012. – №6(1). – С. 132-140.
[23] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во ПГУ, 2000. – 156 с.
[24] Волчихин В.И. Нейросетевая защита персональных биометрических данных. – М.: Радиотехника, 2012. – 210 с.
[25] Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. – Пенза: Изд-во ПГУ, 2005. – 273 с.
[26] Ахметов Б.С., Волчихин В.И., Иванов А.И., Малыгин А.Ю. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации. – Алматы: Изд-во КазНТУ им. Сатпаева, 2013. – 152 с.
[27] Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Научная серия «Нейрокомпьютеры и их применение». – М.: Радиотехника, 2004. – Книга 15. – 143 с.
[28] Ахметов Б.С., Надеев Д.Н., Фунтиков В.А., Иванов А.И., Малыгин А.Ю. Оценка рисков высоконадежной биометрии. – Алматы: КазНТУ, 2014. – 123 с.
[29] Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа. – Алматы: КазНТУ, 2014. – 144с.
[30] Juels A., Wattenberg M. A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security. – 1999. – P. 28-36.
[31] Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice // In Proc. IEEE Symp. on Security and Privacy. – 2001.
[32] Juels A., Sudan M. A Fuzzy Vault Scheme // IEEE International Symposium on Information Theory. – 2002. – P. 28-36
[33] Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy / In Eurocrypt. – 2004, april 13. – P. 523-540.
[34] Yang S., VerbauwhedeI. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme // Proc. IEEE ICASSP. – 2005. – P. 609-612

[35] Cauchie S., Brouard T., Cardot H. From features extraction to strong security in mobile environment: A new hybrid system // On the Move to Meaningful Internet Systems 2006: OTM 2006. – Springer: Workshops, 2006. – P. 489-498.
[36] Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes // Advances in Artificial Intelligence – IBERAMIA-SBIA (LNCS). – 2006. – №4140. – P. 178-187.
[37] Arakala A., Jeffers J., Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics (LNCS). – Springer, 2007. – №4642. – P. 760-769.
[38] Lee Y.J., Bae K., Lee S.J., Park K.R., Kim J. Biometric Key Binding: Fuzzy Vault Based on Iris Images // Proceedings of 2nd International Conference on Biometrics, Seoul, South Korea. – 2007, august. – P. 800-808.
[39] Nandakumar K., Jain A.K., Pankanti S. Fingerprint-Based Fuzzy Vault: Implementation and Performance // IEEE Transactions on Information Forensics and Security. – 2007. – №2(4). – P. 744-757.
[40] Balakirsky V.B., Ghazaryan A.R., Han Vinck A.J. Constructing Passwords from Biometrical Data // Advances in Biometrics (LNCS). – Springer, 2009. – №5558.– P. 889-898.
[41] Kanade S., Petrovska-Delacretaz D., Dorizzi B. Multi-Biometrics Based Cryptographic Key Regeneration Scheme//Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems. – 2009. – P. 333-339.
[42] Ахметов Б.С., Иванов А.И., Малыгин А.Ю., Картбаев Т.С. Оценка вероятностей появления ошибок нейросетевых преобразователей биометрия-код на основе малых выборок // В сб. мат. II Международной научной конференции «Высокие технологии – залог устойчивого развития». – Алматы: Изд-во Казахского национального технического ун-та, 2013. – С.234-237.
[43] Ахметов Б.С., Алимсеитова Ж.К., Серикова Н.И., Иванов А.И., Фунтикова Ю.В. Синтез критерия хи-квадрат для зависимых данных // Материалы **Международного Форума «Инженерное образование и наука в XXI веке: проблемы и перспективы»**, посвященного 80-летию КазНТУ имени К.И. Сатпаева. – Алматы, 2014. – С. 368-372.
[44] ГОСТ Р 15.011-96 Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения.
[45] МалыгинА.Ю., ВолчихинВ.И., ИвановА.И., ФунтиковВ.А. Быстрые алгоритмы тестирования высоконадежных нейросетевых механизмов биометрической защиты информации. – Пенза: Изд-во ПГУ, 2006. – 161 с.
[46] ВолчихинВ.И., ИвановА.И., Безяев А.В. и др. Нейросетевые преобразователи биометрических образов человека в код его личного криптографического ключа /под ред. А.Ю. Малыгина.Сер. «Нейрокомпьютеры и их применение». – М.: Радиотехника, 2008. - Книга 29. - 88 с.

Mukapil K., Beketova G., Zhumagalieva N., Tulemisova V
Kazakh National Technical University (KazNTU)
050013, Republic of Kazakhstan, Almaty 22a, Satpaev Street,
nazym_k.81@mail.ru

Jaroslav Kultan, Dr. Ing. PhD.
Ekonomická univerzita v Bratislave,
Dolnozemská cesta 1, 85335 Bratislava, Slovakia,
jkultan@gmail.com

Биометрические методы защиты информации

Мукапил К., Бекетова Г., Жуманғалиева Н., Тулемисова В., Култан Я.

Аннотация

Рассматриваются биометрические методы защиты информации. Дается сравнительный анализ технологий защиты информации с использованием «нечетких экстракторов» и высокоразмерных нейросетевых преобразователей биометрия-код. Описывются угрозы для систем биометрико-нейросетевой аутентификации

Целью статьи является анализ различных методов аутентификации личности исходя из трех основных методов: по собственности, по знаниям и по биометрическим параметрам. Также рассматривается разделение биометрических параметров на физиологические и поведенческие прибегая к их основным свойствам – всеобщность, уникальность, постоянство и измеримость. Учитывая данные факторы делается анализ методов аутентификации личности и систем использующих данные параметры.

В следующей части дается обзор технологии защиты информации и идентификации личности. Последняя часть статьи направленная на анализ некоторых угроз для систем биометрической аутентификации.

Статья является анализом существующего состояния и новых возможностей развития систем защиты информации

Ключевые слова:

биометрия, биометрическая идентификация, биометрические системы аутентификации, биометрические технологии, защита информации, нейронная сеть.