На правах рукописи

САМОТУГА Александр Евгеньевич

РАСПОЗНАВАНИЕ СУБЪЕКТОВ И ИХ ПСИХОФИЗИОЛОГИЧЕСКИХ СОСТОЯНИЙ НА ОСНОВЕ ПАРАМЕТРОВ ПОДПИСИ ДЛЯ ЗАЩИТЫ ДОКУМЕНТООБОРОТА

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Омск – 2017

Работа выполнена на кафедре «Комплексная защита информации» в ФГБОУ ВО «Омский государственный технический университет»

Научный руководитель: кандидат технических наук, доцент **Ложников Павел Сергеевич**

Официальные оппоненты: доктор технических наук, профессор **Мещеряков Роман Валерьевич** ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», проректор по научной работе и инновациям, заведующий кафедрой «Безопасности информационных систем»

Кандидат физико-математических наук **Ручай Алексей Николаевич** ФГБОУ ВО «Челябинский государственный университет», доцент по кафедре «Компьютерная безопасность и прикладная алгебра»

Ведущая организация: ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир

Защита диссертации состоится 21 декабря 2017г. в 10 часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВО «Уфимский государственный авиационный технический университет» по адресу: 450008, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» октября 2017 года.

Ученый секретарь
диссертационного совета,
д.т.н, доцент И. Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время идет интенсивный процесс внедрения информационных технологий, но при этом от использования бумажных документов окончательно не отказываются и бумажный документооборот остается востребованным. Наиболее распространенным стал смешанный документооборот (используются обе формы представления документов). Следующий этап развития документооборота – гибридный – подразумевает применение биометрических данных при формировании секретного ключа ЭЦП и обеспечение равного уровня защиты бумажных и электронных документов.

Несмотря на развитое законодательство, которое регулирует использование документов (Федеральный закон «Об информации, информационных технологиях и о защите информации», ГОСТ «Делопроизводство и архивное дело» и прочие), ущерб, вызванный подделкой документов, значителен и возрастает. Проведенное аналитическое исследование показало, что с 2008 по 2015 год в России финансовые потери возросли с 13 до 15,8 млрд. руб., мировых потерь из-за утечек информации (отчеты Zecurion Analytics): 2013 г. – 25 млрд. долл, 2014 г. – 18,5 млрд. долл, 2015 г. – 29 млрд. долл. Причиной от 35 до 58% случаев являются сотрудники (включая бывших). Фальсификациия документа становится возможной при передаче ключа классической электронно-цифровой подписи третьим лицам. Улучшение традиционных средств аутентификации не исправит ситуацию, т.к. нужно изменить постановку задачи: создать защиту от того, кому разрешено все в соответствии со служебными обязанностями.

В соответствии с обновленной «Доктриной информационной безопасности РФ», к новым угрозам относят оказание информационно-психофизиологического воздействия на сознание, что побуждает принимать во внимание возможное намерение сотрудников нанести ущерб.

Судить о намерении сотрудника нанести ущерб в момент выполнения должностных обязанностей или аутентификации можно, анализируя его психофизиологическое состояние (ПФС)[1]. Данную задачу, как и задачи идентификации и аутентификации субъекта, можно решить, используя особенности воспроизведения подписи, так как установлено, что ПФС субъекта отражается на почерке и подписи.

Методы идентификации субъекта по подписи широко распространены благодаря тому, что они не вызывают отторжения пользователей, являются для них привычным делом, для считывания параметров не требуется дорогостоящее обо-

[1] Е.П.Ильин определяет психофизиологическое состояние человека как «целостную системную реакцию (на уровне организма и часто – личности) на внешние и внутренние воздействия/ Ильин Е. П. Психофизиология состояний человека. — СПб.: Питер, 2005. — 412 с.

рудование. Накопленный опыт можно использовать в целях решения задачи защиты документов.

Настоящая работа посвящена решению задач разработки модели изменения признаков рукописных образов, метода оценки психофизиологического состояния субъекта, способа верификации субъекта, алгоритма создания гибридных документов, которые бы позволили создать систему, реализующую формирование подписываемых защищенных документов с одновременной оценкой психофизиологического состояния субъекта. Результаты исследования использовались при выполнении проектов, получивших поддержку Российского фонда фундаментальных исследований (№16-07-01204, № 15-07-09053).

Степень разработанности темы исследования. Вопросам, связанным с защитой смешанного документооборота, посвящены работы российских и зарубежных ученых, заложившие основы данной теории. Среди них Финько О.А., Елисеев Н.И., Конявский В.А., Гадасин В.А., Абасов Н.Д., , Храмцовская Н.А., L. Goyal, P. Diwan, M. Raman, M. K. Vijay, S. Low, A. M. Lapone. Вопросам, связанным с распознаванием субъекта или его ПФС по подписи, посвящены работы Hao F., Jun Chen, Annouar B.K., Колядина Д.В., Высоцкой Е.А., Дорошенко Т.Ю., Ажмухамедова И.М., Варвариной С.В., Иванова А.И., Епифанцева Б.Н., Безяева А.В., Ложникова П.С., Сулавко А.Е., Еременко А.В. Несмотря на наличие работ в данной области, полученные результаты недостаточны для внедрения на практике. Анализ этих и других работ позволил определиться с направлениями исследований, ориентированных на разработку следующего подхода к защите документов:

1) Реализовать защиту документа от нарушения целостности и аутентичности с использованием биометрических параметров его создателя;

2) Определять психофизиологическое состояние владельца документа по особенностям воспроизведения подписи.

Объектом исследования диссертационной работы являются защищенные системы смешанного документооборота.

Предметом исследования диссертационной работы являются алгоритмы формирования защищенных документов на основе особенностей воспроизведения подписи.

Цель диссертационной работы – повысить точность верификации субъекта и его психофизиологического состояния по подписи для защиты документов на электронных и бумажных носителях.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Разработать математическую модель рукописных образов субъектов с учетом их психофизиологического состояния.

2. Разработать метод оценки психофизиологического состояния, позволяющий выявить нахождение подписанта в состоянии, отличном от нормального.

3. Разработать способ верификации подписи субъекта, включающий в себя оценку состояния подписанта.

4. Разработать алгоритм создания документов с возможностью подтверждения целостности и аутентичности документа на электронных и бумажных носителях.

Методы исследования. В диссертации представлены результаты исследований, полученные с помощью теории вероятностей, математической статистики и имитационного моделирования.

Научная новизна результатов исследования:

1. Новизна математической модели рукописных образов субъектов, которая основана на анализе закономерностей изменения параметров воспроизведения подписи в зависимости от психофизиологического состояния подписанта отличается тем, что предлагается использовать статистическую зависимость, применяя коэффициенты для вычисления параметров подписи в измененном состоянии, основываясь на значениях параметров подписи в нормальном состоянии, что позволяет заменить проведение длительных экспериментов на простые вычислительные процедуры, чтобы получить эталон подписи в измененном состоянии.

2. Новизна разработанного метода распознавания психофизиологического состояния подписанта, основанного на анализе особенностей воспроизведения рукописных образов, отличающегося тем, что для классификации ПФС предлагается использовать искусственные нейронные сети многомерных функционалов наибольшего правдоподобия Байеса, что позволяет оценить ПФС подписанта на этапе верификации подписи.

3. Новизна предложенного способа верификации подписи с учетом его психофизиологического состояния, основанного на анализе особенностей воспроизведения рукописных образов отличающегося тем, что для распознавания личности подписанта предлагается использовать многомерные функционалы наибольшего правдоподобия Байеса, что позволяет повысить точность при верификации личности по особенностям почерка.

4. Новизна алгоритма создания гибридных документов в информационных системах, основанного на анализе особенностей воспроизведения рукописных образов с возможностью верификации личности обладателя информации в момент подписания документа, отличающегося введением блока оценки его психофизиологического состояния, что в последующем позволяет подтвердить его целостность и аутентичность, а также удостовериться в том, что создатель находился в адекватном состоянии.

Теоретическая и практическая значимость работы. Применение полученных результатов позволяет повысить защищенность корпоративных

информационных систем электронного и смешанного документооборота, реализовать защищенный гибридный документооборот. Теоретическую ценность представляют:

1. Математическая модель рукописных образов субъектов, которая дает возможность скорректировать эталон подписи, сформированный субъектом в нормальном (адекватном) состоянии таким образом, чтобы получить эталон подписи в измененном состоянии.

2. Метод распознавания психофизиологического состояния, который позволяет оценить состояние на этапе верификации подписи.

3. Способ верификации подписи с учетом его психофизиологического состояния, который позволяет повысить точность при идентификации личности по особенностям почерка.

4. Алгоритм создания гибридных документов с возможностью верификации личности подписанта и оценки его психофизиологического состояния по особенностям воспроизводимого рукописного образа.

Практическую значимость составляют:

1. Программный комплекс, реализующий способ верификации подписи, учитывающий состояние субъекта с помощью метода оценки его психофизиологического состояния, позволяющий распознать факт нахождения субъекта в измененном состоянии в момент написания автографа с вероятностью ошибочных решений 1-ого и 2-ого рода 0,008 и 0,005, соответственно.

Внедрение результатов работы. Результаты диссертационной работы внедрены в ООО «НТЦ «КАСИБ» и учебный процесс ФГБОУ ВО «ОмГТУ», что подтверждается актами внедрения.

Соответствие диссертации паспорту научной специальности. Представленная диссертация удовлетворяет п.4, п.11, п.13 паспорта специальности 05.13.19 – “Методы, модели и средства защиты информации, информационная безопасность”:

п. 4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации;

п. 11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа;

п. 13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Достоверность результатов подтверждена соответствием результатов имитационного моделирования а также использованием признанных методик статистической обработки данных.

Апробация работы. Основные результаты работы докладывались на Международной научно-практической конференции «Электронные средства и системы управления» (г. Томск, 12-14 ноября 2014 г.); Международной научно-практической конференции «Научно-технический прогресс: актуальные и перспективные направления будущего» (г. Кемерово, 10-11 августа 2016 г.); Международной научно-технической конференции «Динамика систем, механизмов и машин.» (г. Омск, 15-17 ноября 2016 г.); региональный этап Всероссийского конкурса проектов и разработок в области ИТ-технологий «IT ПРОРЫВ» (г. Омск, апрель 2014 г.).

Публикации. Материалы диссертации опубликованы в 11 научных работах. В число указанных публикаций входят 2 статьи в изданиях, индексируемых в Scopus, 5 статей из перечня ВАК рецензируемых научных изданий, 3 статьи в сборниках материалов международных, всероссийских и вузовских конференций. Получен патент на изобретение Российской Федерации.

Личный вклад автора. Основные результаты и положения, выносимые на защиту, получены лично автором. Все алгоритмы, обсуждаемые в работе, разработаны и экспериментально исследованы автором самостоятельно. Научный руководитель принимал участие в постановке цели и задач исследования, планировании экспериментов, предварительном анализе результатов экспериментов. Заимствованный материал обозначен в работе ссылками.

Положения, выносимые на защиту:

1. Предложена математическая модель рукописных образов субъектов, основанная на вычисленных коэффициентах параметров распределения, позволяющая скорректировать эталон подписи, сформированный субъектом в нормальном (адекватном) состоянии таким образом, чтобы получить эталон подписи в измененном состоянии.
2. Разработан метод оценки психофизиологического состояния субъекта по подписи на основе искусственных нейронных сетей функционалов наибольшего правдоподобия Байеса, позволяющий распознать факт нахождения субъекта в измененном состоянии в момент написания автографа с вероятностью ошибок 0,08.
3. Разработан способ верификации подписанта по особенностям рукописного образа с вероятностью ошибочных решений 1-ого и 2-ого рода 0,003 и 0,0065, устойчивый к попыткам его фальсификации, отличающийся от существующих учетом вероятного психофизиологического состояния субъекта, основанный на вейвлет-анализе параметров образа, многомерных функционалах наибольшего правдоподобия Байеса.

4. Предложен алгоритм создания гибридных документов с возможностью подтверждения личности создателя и оценки его психофизиологического состояния по особенностям воспроизводимого рукописного образа.

Структура и объём диссертации. Диссертация изложена на 124 страницах. Она состоит из введения, четырёх глав, заключения. Работа содержит 29 иллюстраций, 8 таблиц, список использованных источников, состоящий из 119 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность диссертационной работы, сформулирована цель и научная новизна исследований, показана практическая значимость полученных результатов, сформулированы выносимые на защиту научные положения. Дано определение гибридного документооборота.

В **первой главе** представлено аналитическое исследование проблемы защиты гибридного документооборота и подходы к ее решению. Выполнен аналитический обзор способов скрытой и явной оценки ПФС. Сформулированы задачи исследований, согласно которым требуется решить проблемы отчуждаемости ЭЦП от владельца, сложности применения ЭЦП к документам на бумажном носителе, возможность копирования изображения автографа и отсутствия быстрого способа автоматизированной проверки его аутентичности.

Во **второй главе** сформирована база рукописных образов. В течение нескольких дней проводился эксперимент по формированию базы подписей с привлечением 110 испытуемых, вводимых поочередно в следующие состояния (подтверждение «перехода» в соответствующее ПФС осуществлялось на холтеровском мониторе «Кардиотехника-04»):

1. Нормальное (или адекватное) состояние, при котором субъект не подвергался каким-либо воздействиям. Эксперимент проводился в начале дня после полноценного отдыха в предшествующие сутки. В данном состоянии наблюдаются наилучшие результаты деятельности индивидуума.

2. Возбуждение – характерно для человека, сконцентрированного на решении ответственной задачи. Данное состояние представляет собой общую физиологическую и психологическую активизацию организма. Перед началом эксперимента участник принимал кофе, что повышало ЧСС в среднем на 10%. Для сильно возбужденных людей характерно также учащенное дыхание и обильное потоотделение.

3. Усталость после физической нагрузки, характеризуется учащением ЧСС на 10-30%. Для получения нужного эффекта испытуемые подвергались интенсивной физической нагрузке, минимальный объем которой определялся методом Мартине (20 приседаний за 30 секунд) и далее варьировался в зависимости от пола и возраста.

4. Расслабленное (сонное) состояние, характеризующееся легкой сонливостью, низкой продуктивностью. Для имитации данного состояния участники принимали успокаивающие естественные растительные средства седативного действия, к которым относится пустырник, мята, валериана, и прослушивали успокаивающую музыку. ЧСС возвращались к значениям в состоянии покоя, либо происходило снижение ЧСС на 3-5%.

5. Опьянение. Испытуемый принимал алкоголь, дозировка рассчитывалась по формуле Видмарка. Масса выпитого соответствовала такому количеству алкоголя, для которого значение концентрации в крови было от 0,5 до 1‰. Данный уровень опьянения выбран, исходя из критериев, предлагаемых для определения степени выраженности алкогольной интоксикации В.И. Прозоровским и другими. Согласно принятой схеме, при меньшей концентрации отсутствует влияние алкоголя на организм. Данный уровень приводит к статистически значимым изменениям вариабельности сердечного ритма (ВСР).

Для ввода подписей субъектов использовался планшет фирмы Wacom. Для получения признаков использовались функции координат подписи $x(t)$ и $y(t)$, функция давления пера на планшет при письме $p(t)$. Предварительно из подписи удаляются точки с нулевым давлением, а функции $x(t)$, $y(t)$ и $p(t)$ нормировались по длительности (приводились к единому количеству отчетов). Функции $x(t)$ и $y(t)$ преобразуются в функцию скорости перемещения пера на планшете $V_{xy}(t)$.

Обработка функций $p(t)$ и $V_{xy}(t)$ происходит раздельно в 2 этапа: 1) разложение целевой функции в ряд Фурье; 2) нормирование амплитуд гармоник целевой функции по энергии (диапазон анализируемых частот составлял 0,1-10 Гц). В качестве признаков динамики подписи использовались 16 нормированных амплитуд низкочастотных гармоник функций $p(t)$ и $V_{xy}(t)$, 15 коэффициентов корреляции между функциями $x(t)$, $y(t)$, $p(t)$ и их производными. В качестве признаков внешнего вида подписи использовались 120 расстояний между некоторыми точками (точки выбираются равномерно с некоторым шагом, далее находятся расстояния между всеми парами этих точек, третье измерение – давление пера на планшет), 5 характеристик изображения подписи (отношение длины подписи к ее ширине, центр подписи, угол наклона подписи, угол наклона между центрами половин подписи.). Все обозначенные признаки имеют распределение, близкое к нормальному. Следующие признаки – коэффициенты вейвлет-преобразований Добеши по базису D6 функций $V_{xy}(t)$ и $p(t)$ имеют распределение, близкое к распределению Лапласа. Некоторые из перечисленных признаков использовались рядом исследователей в их работах, в том числе по идентификации личности.

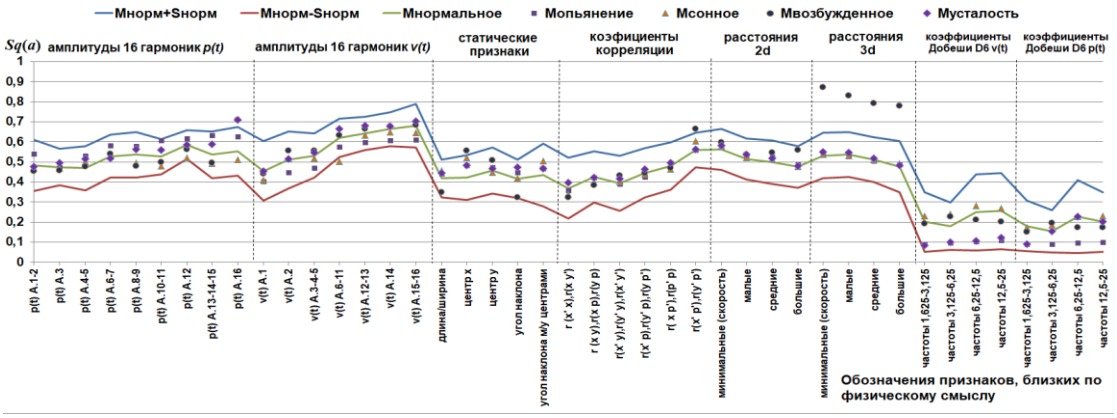

Рисунок 1– Информативность признаков для распознавания подписантов

Проведена оценка информативности признаков по площадям пересечения функций плотностей вероятности значений этого признака для задачи распознавания субъектов и их ПФС. Построены графики математических ожиданий $M_{ПФС}$ и среднеквадратичных отклонений $S_{ПФС}$ соответствующих площадей $S_q(a_j)$, характеризующих информативность различных групп признаков для задачи распознавания подписантов, находящихся в определенном ПФС (рисунок 1). Чем меньше $M_{ПФС}$ – тем информативнее признак в целом (в среднем для всех испытуемых), чем выше $S_{ПФС}$, тем больше различие в информативности признака для испытуемых. С точки зрения распознавания подписантов наиболее информативными являются вейвлет коэффициенты Добеши (рисунок 1), различия в информативности между остальными признаками не настолько существенны. Наименее информативными являются амплитуды высокочастотных гармоник функции скорости пера на планшете $V_{xy}(t)$. С точки зрения распознавания ПФС следующее ранжирование информативности признаков: вейвлет коэффициенты Добеши, статические признаки, коэффициенты корреляции между функциями рукописного образа, расстояния между его точками, амплитуды гармоник $V_{xy}(t)$ и $p(t)$.

При помощи специально разработанного программного модуля собраны биометрические параметры 110-ти пользователей, каждый из них ввел не менее 50 реализаций подписи в каждом состоянии. За каждым пользователем был закреплен другой, наблюдающий за вводом его биометрических данных. Далее каждый пользователь совершил 60 попыток подделки биометрических параметров пользователя, за вводом биометрических данных которого он наблюдал. Таким образом, получено 5500 реализаций “своих” и 6600 реализаций “чужих” пользователей для каждого состояния. Далее под реализацией подписи – вектор значений признаков подписи.

В **третьей главе** описаны метод оценки ПФС субъекта и способ распознавания подписанта по подписи, приводится модель изменения признаков рукописных образов в зависимости от ПФС подписанта.

Для формирования эталонов рассчитываются математическое ожидание и среднеквадратичное отклонение значений всех признаков. Для вычисления каждого параметра распределения использовалось не менее 21 реализаций значений признака согласно ГОСТ 52633.5-2011. Для поиска статистических закономерностей образов субъектов, описывающих изменения параметров воспроизведения подписи в зависимости от ПФС, построены графики математических ожиданий и среднеквадратичных отклонений признаков. Из них ясно, что некоторые признаки в различных состояниях имеют близкие значения, что говорит об схожих изменениях ряда признаков при нахождении человека в каком-либо из измененных состояний. В связи с чем предложен следующий подход: переход к модели двух состояний, где из всех состояний, отличных от нормального, создается эталон ПФС, которое будем называть «измененное». Это состояние будет включать все реализации, полученные в состояниях «опьянение», «усталость», «сонное» и «возбужденное». Были определены поправочные коэффициенты для эталона в нормальном состоянии, которые образуют векторы перехода эталона к измененному состоянию, а также построены соответствующие графики (рисунок 2). Коэффициенты позволяют получить эталон подписанта, находящегося в состоянии, условно названном «измененное», без необходимости ввода подписей в этом состоянии по формуле (1):

$$\begin{aligned} \mathrm{E}'_u &= \begin{bmatrix} m'_{u1} & \dots & m'_{un} \end{bmatrix} = \mathrm{E}_н \times \mathrm{K}_m = \begin{bmatrix} m_{н1} & \dots & m_{нn} \end{bmatrix} \times \begin{bmatrix} \kappa_{m1} \\ \dots \\ \kappa_{mn} \end{bmatrix} \approx \mathrm{E}_u = \begin{bmatrix} m_{u1} & \dots & m_{un} \end{bmatrix}, \\ \Theta'_u &= \begin{bmatrix} \sigma'_{u1} & \dots & \sigma'_{un} \end{bmatrix} = \Theta_н \times K_S = \begin{bmatrix} \sigma_{н1} & \dots & \sigma_{нn} \end{bmatrix} \times \begin{bmatrix} \kappa_{\sigma 1} \\ \dots \\ \kappa_{\sigma n} \end{bmatrix} \approx \Theta_u = \begin{bmatrix} \sigma_{u1} & \dots & \sigma_{un} \end{bmatrix}, \end{aligned} \quad (1)$$

где E_u и $E_н$ – матрицы математических ожиданий признаков субъекта в измененном и нормальном состоянии, соответственно, Θ_u и $\Theta_н$ – матрицы среднеквадратичных отклонений признаков субъекта в измененном и нормальном состоянии, соответственно, K_m и K_s – матрицы поправочных коэффициентов для математических ожиданий и среднеквадратичных отклонений, соответственно, n – количество признаков. Назовем преобразованный эталон, состоящий из матриц E'_u и Θ'_u, синтетическим.

За счет описанного преобразования можно отказаться от обязательного создания эталонов подписей субъектов для каждого из измененных состояний, но при этом на стадии идентификации субъекта иметь возможность обнаружить, отличается ли состояние субъекта от нормального.

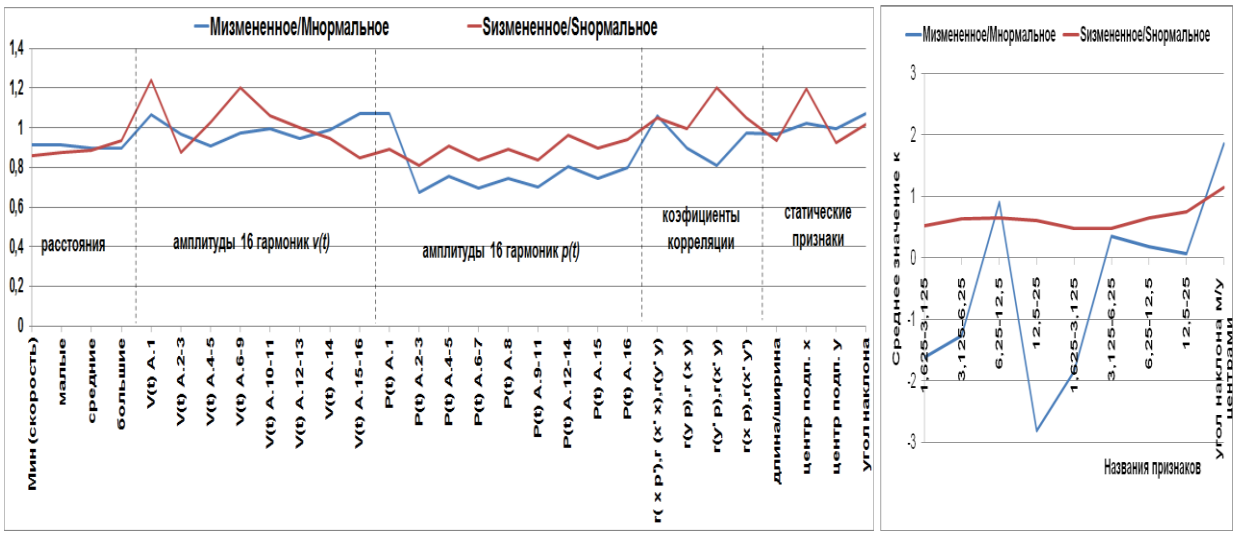

Рисунок 2 – Коэффициент изменения признаков к в зависимости от ПФС подписанта

Проведен эксперимент по распознаванию ПФС субъектов по подписи, состоящий из 2-х этапов: использованием исходных естественных эталонов подписей, полученных в нормальном и измененном состояниях и с использованием естественных эталонов подписей для нормального ПФС и искусственных эталонов (преобразованных по формуле (1)) для измененного ПФС.

На первом этапе применялись следующие подходы: последовательное применение модифицированной или классической формулы Байеса, мера Хемминга, принцип накопления, метрика Пирсона.

Метод последовательного применения формулы Байеса заключается в следующем. На каждом шаге по формуле гипотез Байеса или ее модифицированного варианта (2) рассчитываются апостериорные вероятности гипотез с учетом значения одного из признаков, при этом за априорную вероятность гипотезы принимается ее апостериорная вероятность, вычисленная на предыдущем шаге. На первом шаге все гипотезы равновероятны $P(H_i|A_0)=n\text{-}1$, где n – количество гипотез. На последнем шаге предпочтение отдается гипотезе с максимальной апостериорной вероятностью.

$$P(H_i|A_j) = P(H_i|A_{j-1}) + \left(\frac{P(H_i|A_{j-1})P(A_j|H_i)}{\sum_{i=1}^{n} P(H_i|A_{j-1})P(A_j|H_i)} - P(H_i|A_{j-1}) \right) \times (W_j), \quad (2)$$

где $P(H_i|A_j)$ – апостериорная вероятность i-й гипотезы, вычисляемая на j-м шаге при поступлении j-го признака, $P(A_j|H_i)$ – условная вероятность i-й гипотезы на j-м шаге (равна плотности вероятности значения j-го признака на основе параметров i-ого эталона), W_j – вес j-го признака, характеризующий его информативность. Условные вероятности вычисляются исходя из закона распределения значений признаков, как плотности вероятности соответствующего закона распределения.

Вес признака на каждом шаге предлагается определять как взвешенное среднее площадей пересечения плотностей вероятности признаков, характеризующих различные эталоны.

Лучшие результаты по идентификации ПФС субъектов при использовании естественных эталонов получены с помощью метода последовательного применения классической формулы Байеса (т.е. при W_j=1). Средняя вероятность ошибки распознавания 2-х состояний 110 субъектов составила 0,073. Достоверность полученных результатов 0,99 при доверительном интервале 0,01.

В работе Иванова и др.[2] предложено повышать размерность формулы Байеса, учитывая за один шаг информацию о нескольких признаках (плотности вероятности $f_h(a_j)$ нескольких признаков a_j на каждом шаге необходимо перемножать, воспринимая их как вероятности одновременного возникновения независимых событий A_j). При повышении размерности n многомерного функционала наибольшего правдоподобия Байеса (3) (МФНПБ) появляется множество вариантов его записи.

$$P(H_h|A_s) = \frac{P(H_h|A_{s-1})\prod_{x=1}^{n} f_h(a_{j(s,x)})}{\sum_{h=1}^{n}(P(H_h|A_{s-1})\prod_{x=1}^{n} f_h(a_{j(s,x)}))}, \qquad (3)$$

где $j(s, x)$ – номер признака, который больше не совпадает с номером шага s, но зависит от него. На каждом шаге целесообразно использовать уникальные сочетания из n неповторяющихся признаков. В общем случае, количество возможных неповторяющихся шагов последовательного применения n-мерного функционала (3) равно числу сочетаний без повторений C_η^n из η по n, где η – общее количество признаков ($n \leq \eta$).

Предлагается конструировать N нейронов на основе различных сочетаний неповторяющихся шагов, в основе которых лежит функционал (3). Если выявить оптимальные значения числа шагов и размерности, то такой подход гораздо эффективнее чем повторение η раз двумерного правила Байеса (2) или однократное применение η-мерного функционала (3).

На втором этапе проведен вычислительный эксперимент по распознаванию ПФС с использованием сети из многомерных функционалов Байеса (3). Наилучший результат с вероятностью ошибки 0,08 достигается при следующей конфигурации сети (таблица 1).

Таблица 1– Конфигурация сети многомерных функционалов Байеса

[2] Иванов А.И., Ложников П.С., Качайкин Е.И., Сулавко А.Е. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса // Вопросы защиты информации / ФГУП «ВИМИ». – Москва: 2015. – №3. – С. 48-54.

число нейронов	размерность	шагов	число нейронов	размерность	шагов	число нейронов	размерность	шагов
100	5	10	100	20	10	100	50	5
100	5	20	100	20	20	100	100	1
100	10	10	100	50	1			
100	10	20						

Таким образом, полученная погрешность вероятностей существенна, но можно заключить, что результат удовлетворительный и построенная статистическая модель упрощенно описывает изменения параметров рукописных образов, при изменении состояния субъекта.

При разработке способа верификации субъектов с учетом ПФС выполнено сравнение разных методов принятия решений: сетей квадратичных форм, настраиваемых при помощи адаптированного алгоритма обучения персептронов из ГОСТ Р 52633.5-2011, сетей из нейронов на базе метрик Пирсона и Хи-модуль, МФНПБ. Установлено, что все функционалы теряют мощность, если состояния подписантов на этапах обучения и распознавания не совпадают (это эквивалентно снижению репрезентативности обучающей выборки), потери мощности тем выше, чем выше их размерность. Вероятность ошибки в среднем возрастает: для функционала Пирсона на 103%, для Хи-модуль на 49%, для квадратичной формы с обучением по ГОСТ Р 52633.5 на 73%, для МППФБ на 326%, для МФНПБ на 1077%. Таким образом, самым устойчивым функционалом является мера Хи-модуль. Если объединить функционалы в сеть, устойчивость сети зависит от их размерностей.

Наилучший результат по верификации подписантов получен с использованием всех рассмотренных признаков и применением многомерных функционалов Байеса (3) и превосходит достигнутый ранее уровень: FRR=0,0014, FAR=0,0045. Но данные показатели достигаются при условии строгого совпадения ПФС подписантов на этапе создания эталона и распознавания.

Таким образом, предлагается сначала распознать состояние подписанта, а потом верифицировать его личность. С учетом ошибки распознавания ПФС вероятность ошибок 1-ого и 2-ого рода предлагаемого способа верификации подписанта составила: FRR=0,003, FAR=0,0065.

В **четвертой главе** приводится разработанный алгоритм создания гибридных документов. Основные этапы работы с гибридным документом выглядят следующим образом (рисунок 3):

1. Создание эталонов ПФС и субъектов. Включает сбор рукописных образов при помощи планшета, получение признаков, формирование эталонов, используемых для биометрической идентификации субъектов и их ПФС, сохранение полученных эталонов на облачном сервере.

2. Идентификация субъекта и его ПФС, формирование защищенного гибридного документа (рисунок 4). На облачный сервер отправляется автограф субъекта (и секретный рукописный образ – опционально) и текст документа, после формирования сервер отдает готовый к использованию гибридный документ с информацией для проверки целостности и аутентичности.

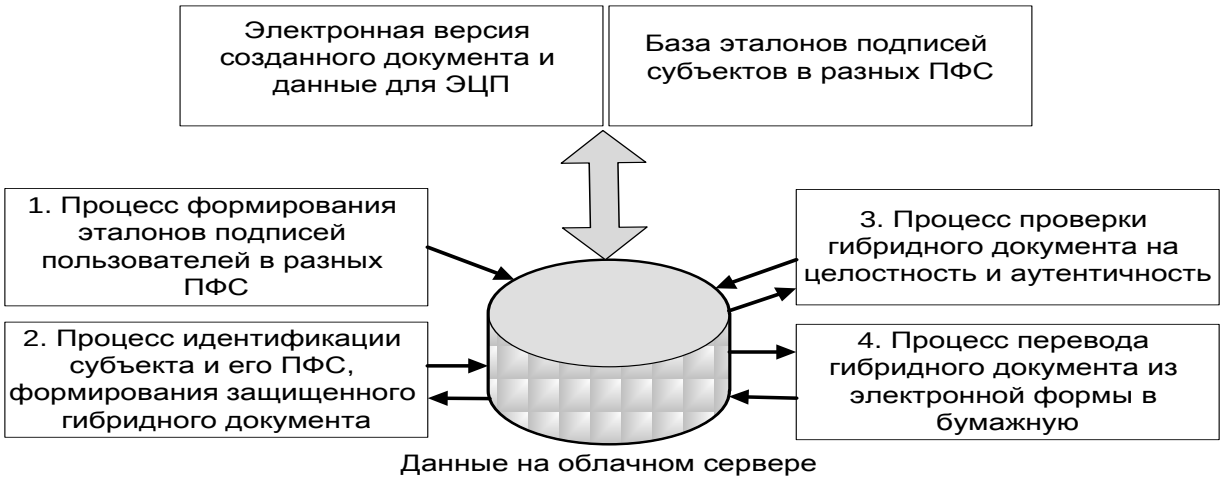

Рисунок 3– Структурная схема системы защищенного гибридного документооборота

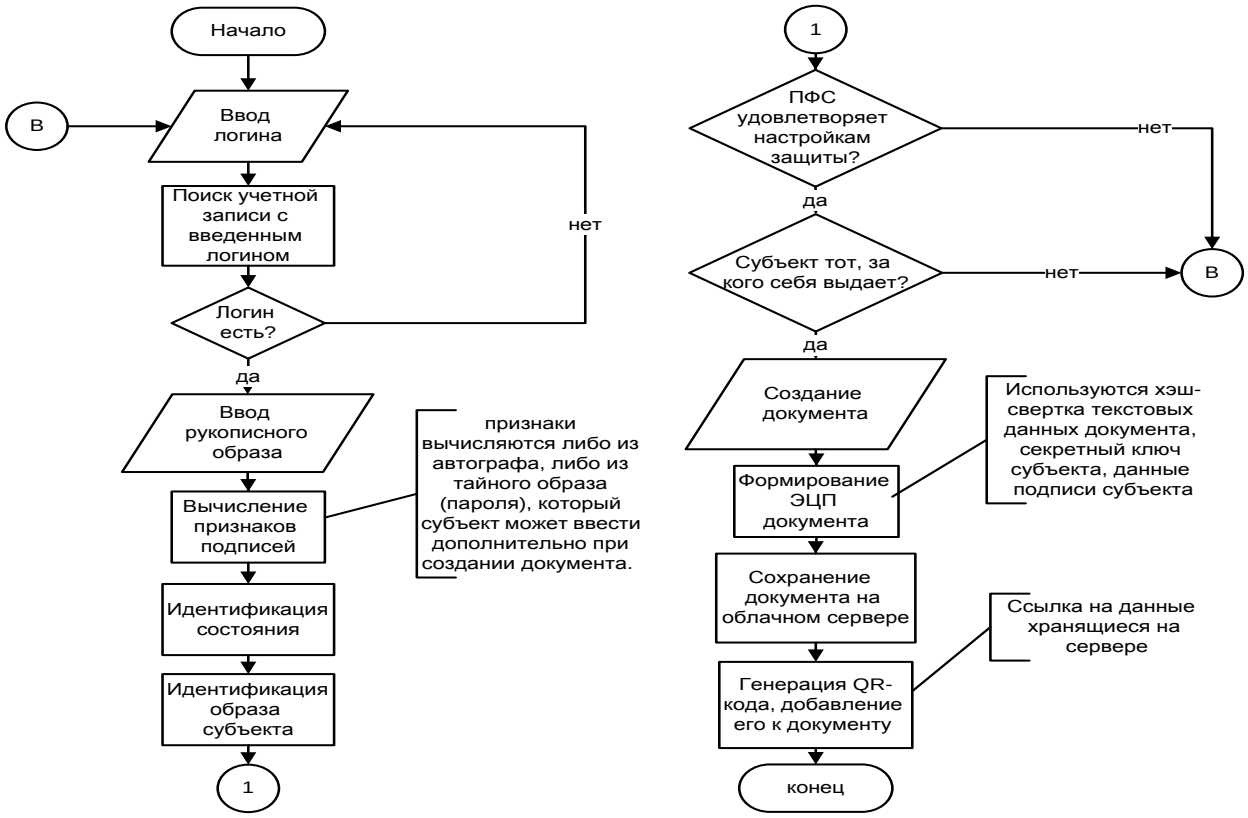

Рисунок 4 – Блок схема алгоритма формирования защищенного гибридного документа

3. Проверка гибридного документа на целостность и аутентичность. Включает сканирование прикрепленной информации, текста документа, сравнение с данными на сервере. При обнаружении нарушения целостности, субъект имеет возможность восстановить содержание документа.

4. Перевод гибридного документа из электронной среды в аналоговую и обратно. Предполагает печать документа со всем необходимыми для его проверки дополнительными данными, занесенными в штрих-код или сканирование документа и текстового содержания и дополнительных данных. Включает в себя проверку на целостность и аутентичность. При переводе из аналоговой среды, выполняется сканирование текстового содержания документа, затем чтение информации из QR-кода. Для распознавания текста используется OCR-библиотека (например, Tesseract от компании Google). Уменьшить число ошибок при распознавании предлагается путем использования наиболее хорошо распознаваемого шрифта – Arial, а также применением одним из существующих алгоритмов помехоустойчивого кодирования.

Разработан прототип программного комплекса для оценки эффективности предложенных алгоритмов, модели, их отладки. Прототип реализован на основе технологии облачных вычислений («cloud computing»). Архитектура состоит из следующих подсистем: ввода биометрических данных – ввод биометрических данных, принятия решений – выделение признаков и создание эталонов, управления – взаимодействие с базой данных, контроль информации о пользователях, обработка документов – все, что связано с обработкой документов, взаимодействия – обмен данными между остальными компонентами. Комплекс можно использовать в системах смешанного документооборота для защиты от подделки документов, подписей, отчуждения ЭЦП, подписания документа субъектом в ПФС отличающимся от нормального.

В **заключении** сформулированы основные результаты работы и подведены итоги.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработана математическая модель рукописных образов субъектов, которая описывает обнаруженные закономерности изменения параметров воспроизведения подписи при изменении ПФС субъекта и дает возможность скорректировать эталон подписи, сформированный субъектом в нормальном (адекватном) состоянии таким образом, чтобы получить эталоны подписи в измененном состоянии.
2. Разработан метод распознавания измененного ПФС с использованием разработанной модели на основе искусственной нейронной сети многомерных функционалов наибольшего правдоподобия Байеса. Метод позволяет распознать факт нахождения субъекта в измененном состоянии в момент написания автографа с вероятностью ошибки 0,08. Достоверность полученных результатов 0,99 при доверительном интервале 0,01.

3. Разработан способ верификации подписанта по особенностям автографа, устойчивый к попыткам ее фальсификации, учитывающий психофизиологическое состояние субъекта с вероятностью ошибочных решений 1-ого и 2-ого рода 0,003 и 0,0065 соответственно. Полученный результат превосходит достигнутые ранее.

4. Разработан алгоритм создания защищенных документов с возможностью резервного восстановления оригинала, подтверждения целостности, а также личности и ПФС создателя по подписи.

Перспективы дальнейшей разработки темы. Дальнейшие исследования могут быть направлены на построение модели изменения параметров подсознательных движений субъекта во времени в зависимости от его ПФС и типа темперамента. В перспективе это позволит достигнуть лучших результатов по распознаванию человека и его ПФС по подписи и другим модальностям (клавиатурный почерк, голос и другие виды подсознательных движений), а также решить проблему потери актуальности («устаревания») биометрического эталона.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации, индексируемые в Scopus:

1. Ложников, П.С. Идентификация личности и оценка ее психофизиологического состояния в процессе написания подписи / П.С. Ложников, А.Е. Сулавко, А.Е. Самотуга // Информация. – 2015. – том 6. – Вып. 3. – С. 454–466.
2. Иванов, А.И. Технология формирования гибридных документов / А.И. Иванов, П.С. Ложников, А.Е. Самотуга // Кибернетика и системный анализ. – 2014. – том 50. – № 6. – С. 152–156.

Публикации в рецензируемых журналах из списка ВАК:

3. Сулавко, А.Е. Идентификация психофизиологических состояний подписантов по особенностям воспроизведения автографа / А.Е. Сулавко, А.В. Еременко, Е.А. Левитская, А.Е. Самотуга // Информационно-измерительные и управляющие системы. – 2017. – №1. – С. 40–48.
4. Ложников, П.С. Модель защиты гибридных документов на основе рукописных подписей их владельцев с учетом психофизиологического состояния подписантов / П.С. Ложников, А.Е. Сулавко, А.Е. Самотуга // Вопросы защиты информации. – 2016. – № 4(115). – С. 47–59.
5. Еременко, А.В. Разграничение доступа к информации на основе скрытого мониторинга пользователей компьютерных систем: непрерывная идентификация / А.В. Еременко, Е.А.Левитская, А.Е. Сулавко, А.Е. Самотуга // Сибирской государственной автомобильно-дорожной академии / СибАДИ. – 2014. – Вып. 6 (40) . – С. 92–102.
6. Сулавко, А.Е. Исключение искаженных биометрических данных из эталона субъекта в системах идентификации / А.Е. Сулавко, А.В. Еременко, Е.А. Левитская, А.Е. Самотуга // Информационные технологии и вычислительные системы. – 2013. – № 3. – С. 96–101.

7. Ложников, П.С. Технология проверки целостности и аутентичности документов в гибридном документообороте / П.С. Ложников, А.Е. Самотуга // Известия ТулГУ. Технические науки. Вып. 3 / Изд-во ТулГУ. – 2013. – С. 402–408.

Публикации в других изданиях

8. Самотуга, А.Е. Обнаружение подделок рукописных паролей в процессе их воспроизведения / А.Е. Самотуга, А.Е. Сулавко // Научно-технический прогресс: актуальные и перспективные направления будущего: Сборник материалов III Международной научно-практической конференции: в 2-х т. – т. 1/ Кемерово: УИП КузГТУ. – 2016. – С. 53–56.
9. Самотуга, А.Е. Об устойчивости параметров автографа в процессе его воспроизведения при изменении функционального состояния подписанта / А.Е. Самотуга // Динамика систем, механизмов и машин. Омск. – 2016. – № 1.– С. 293–302.
10. Ложников, П.С. Способ формирования гибридных документов с использованием биометрической подписи / П.С. Ложников, А.Е. Самотуга // Электронные средства и системы управления: Материалы докладов X Международной научно-практической конференции. В 2 ч. – Ч.2 / Томск: В-Спектр. – 2014. – С. 79–83.

Патент РФ на изобретение

11. Пат. 2543927 Российская Федерация, МПК G06K9/00. Способ идентификации личности по особенностям динамики написания пароля [Текст] / Епифанцев Б.Н., Ложников П.С., Самотуга А.Е., Сулавко А.Е.; заявитель Омский государственный технический университет; заяв. 22.04.14, опубл. 10.03.2015, приоритет 22.04.2014, дата регистрации 03.02.2015. – 7 с.

Диссертант  Самотуга А.Е.