На правах рукописи

Сабанов Алексей Геннадьевич

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ИЕРАРХИИ ДОВЕРИЯ К РЕЗУЛЬТАТАМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ СУБЪЕКТОВ ДОСТУПА

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени доктора технических наук

Томск – 2020

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Научный консультант: доктор технических наук, профессор Шелупанов Александр Александрович, ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», президент

Официальные оппоненты: Бабенко Людмила Климентьевна, доктор технических наук, профессор, Южный федеральный университет, профессор кафедры «Безопасность информационных технологий»

Ложников Павел Сергеевич, доктор технических наук, доцент, ФГБОУ ВО «Омский государственный технический университет», заведующий кафедрой «Комплексная защита информации»

Язов Юрий Константинович, доктор технических наук, профессор Федеральное автономное учреждение «ГНИИИ ФСТЭК России», главный научный сотрудник

Ведущая организация: Академия ФСО России

Защита диссертации состоится 26 ноября 2020 года в 15:00 часов на заседании диссертационного совета Д 212.268.03 при ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники» по адресу: пр. Ленина, д. 40, г. Томск, Томская обл., 634050. С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники».

Автореферат разослан « » _____ 2020 г.

Ученый секретарь
диссертационного совета  Костюченко Евгений Юрьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Управление доступом пользователей в существующих и перспективных информационных системах (ИС) включает в себя применение процессов идентификации и аутентификации (ИА) субъектов и объектов доступа. Процессы аутентификации особенно востребованы в случае дефицита доверия к подлинности и подтверждению владения предъявленными идентификаторами взаимодействующими сторонами, обусловленного, например, предоставлением удалённого доступа и/или использованием небезопасной среды обмена сообщениями. Для снижения рисков проникновения злоумышленника в ИС под видом легального пользователя и формирования определённого уровня доверия (УД) к подлинности взаимодействующих сторон (субъектов и объектов доступа) должны применяться научно обоснованные, закреплённые в нормативно-правовой базе (НПБ) методы, механизмы и средства ИА в составе системы управления доступом, являющейся частью каждой ИС. Проблема корректного управления идентификацией, аутентификацией и авторизацией особенно важна для ИС, обрабатывающих информацию ограниченного доступа. В условиях недостатка научного обоснования, нормативных требований и методических рекомендаций уполномоченных государственных органов операторы ИС самостоятельно выбирают механизмы и средства ИА от разных производителей, что повышает риски реализации атак, направленных на предоставление доступа злоумышленнику.

Создание и развитие ИС с числом субъектов доступа в сотни тысяч и даже десятки миллионов пользователей формирует новую проблему научного поиска необходимого и достаточного количества и качества используемых идентификаторов для достижения заданного уровня достоверности идентификации (ДИ) и разработки шкалы доверия к результатам ИА для таких систем. Особенно остро эта проблема проявляется в открытых ИС общего пользования (ИСОП) с самостоятельной регистрацией субъектов и объектов доступа. Идентификация субъектов при электронном взаимодействии (ЭВ) имеет вероятностную природу, обусловленную процессом верификации предъявленных идентификационных атрибутов (ИдА) с занесёнными ранее значениями при регистрации субъектов в различных государственных реестрах и базах данных. Всеми указанными выше обстоятельствами определяется **актуальность** темы диссертационного исследования.

Значительный вклад в развитие теории и практики защиты информации в ИС, в том числе при рассмотрении проблем идентификации и аутентификации, внесли Н.А. Гайдамакин, В.А. Герасименко, А.А. Грушо, П.Н. Девянин, П.Д. Зегжда, А.М. Ивашко, С.М. Климов, И.Д. Королев, А.И. Костогрызов, А.С. Кузьмин, А.И. Куприянов, О.Б. Макаревич, В.Ф. Макаров, В.В. Меньших, В.А. Минаев, С.И. Смирнов, М.П. Сычев, А.А. Стрельцов, А.А. Тарасов, Л.М. Ухлинов, А.В. Черемушкин, В.Ф. Шаньгин, А.А. Шелупанов, В.П. Шерстюк, И.Б. Шубинский, А.Ю. Щербаков, Ю.К. Язов, W. Burr, M.A. Burrows, J. Clark, W. Diffie, D.F. Dodson, C. Kaufman, J. Kjaersgaard, A. Lensrta, G. Lowe, J. Myers, R.M. Needham, N. Pole, W.T. Polk, K. Rannenberg, B. Schneier, G. Stoneburmner, S.B. Wilson, T.Y.C. Woo и др. В их исследованиях разработана концепция защиты информации (ЗИ), обоснованы принципы обеспечения информационной безопасности (ИБ) и построения систем защиты информации (СЗИ) объектов информатизации, электронных документов (ЭД) с использованием программно-аппаратных СЗИ, рассмотрены теоретические аспекты и методология организации криптографической ЗИ, развита теория функциональной надежности (ФН), а также сформулированы основы построения моделей угроз и нарушителей безопасности информации.

Диссертационная работа посвящена комплексному исследованию процессов идентификации и аутентификации с целью обоснования и создания методологии формирования иерархии доверия к результатам ИА субъектов доступа.

Научная проблема состоит в обосновании теоретических положений и создании методологии формирования иерархии доверия к результатам ИА субъектов доступа (СД), в том числе при удаленном ЭВ. Несмотря на интенсивный рост количества ИС и зарегистрированных в них объектов и субъектов, а также возрастающие требования относительно повышения доверия к электронным формам взаимодействия государства, личности и бизнеса, применяемые сегодня подходы системно не учитывают достаточно развитый арсенал теоретических подходов, математических моделей и методик для комплексного анализа доверия к результатам ИА. Таким образом, при высокой потребности в настоящее время отсутствуют концепция и развитая методология иерархии доверия к результатам ИА СД.

Объектом исследования являются процессы ИА, а также их реализация в системах идентификации и аутентификации (СИА) субъектов доступа.

Предметом исследования выступает система моделей, методов и алгоритмов оценки доверия к результатам идентификации и аутентификации СД.

Цель исследования – создание методологии формирования иерархии доверия к результатам ИА субъектов доступа, в том числе при удаленном ЭВ.

Разработка новых и развитие существующих методов, моделей и алгоритмов оценки доверия к ИА позволяют теоретически обосновать стандарты, рекомендации и требования к процессам и СИА в действующих и проектируемых ИС.

Для достижения поставленной цели решены следующие **задачи**.

1. Проведен анализ НПБ, рекомендаций, стандартов и результатов научных работ, связанных с концептуальными подходами к исследованию ФН, достоверности результатов ИА СД и безопасности обрабатываемой при этом информации.

2. Разработана концепция формирования иерархии уровней доверия к результатам ИА субъектов ЭВ.

3. Обоснована и создана методология оценок достоверности, надежности и безопасности идентификации на основе анализа рисков, позволяющая формировать УД к результатам первичной идентификации (ПИ) СД ИС на базе использования предложенных и существующих методов и моделей идентификации.

4. Предложены показатели доверия к результатам ПИ для формирования на их основе подходов к оценке доверия к результатам идентификации СД.

5. Сформирован комплекс моделей, методов и алгоритмов оценки рисков при анализе безопасности аутентификационной информации (АИ) и ФН процесса аутентификации; разработана методика оценки рисков, учитывающая участников, порядок и состав основных процедур аутентификации.

6. Созданы новые и усовершенствованы существующие модели и методы оценки ФН аутентификации субъектов доступа к информационным ресурсам, а также разработаны показатели доверия к результатам работы систем ИА на основе анализа безопасности идентификационной и аутентификационной информации, достоверности результатов и надежности работы СИА.

7. Апробирована теоретическая и методологическая база формирования иерархии УД к результатам ИА при решении практических задач.

Методы исследования. Для решения задач обоснования, создания и развития методологии построения иерархии УД и в конечном итоге повышения доверия к результатам ИА субъектов доступа применялись методы системного анализа, теории множеств, функциональной надежности, методы теории вероятностей и случайных процессов, оценки рисков, а также методы структурно-функционального анализа, теории управления, защиты информации и систем массового обслуживания.

Научная новизна проведенного диссертационного исследования и полученных результатов заключается в следующем:

– впервые разработана методология построения иерархии доверия к результатам ИА субъектов доступа при ЭВ на основе моделирования основных процессов и СИА. Она отличается от известных учетом рисков и специфики процессов ИА, в том числе для больших ИС с числом пользователей порядка 10^6;

– разработан новый метод оценки рисков первичной идентификации субъектов доступа, отличающийся от известных применением динамического метода построения матриц рисков к ПИ, который позволяет определять величины допустимых рисков и средних значений рисков вероятных опасных событий (ВОС);

– предложен способ многоуровневой оценки рисков на основе разбиения процесса аутентификации на ряд последовательных связанных процедур, что дает возможность определять вероятностные характеристики разнородных по длительности и повторяемости процедур ИА в корпоративных и открытых ИС;

– выполнена оригинальная классификация методов и систем ИА, а также средств и механизмов аутентификации для выявления границ применимости различных технологий ИА по критериям целей и задач обеспечения доступности, конфиденциальности и целостности идентификационных и аутентификационных данных пользователей ИС, отличающаяся от известных полнотой выбора критериев, что обеспечивает возможность многоуровневого анализа рисков процессов и транзакций в СИА для оценивания рисков с заданным уровнем детализации;

– разработаны вероятностные модели и методики оценки надежности процессов ИА, отличающиеся от известных оцениванием не отказа оборудования, а отказа в услугах, что в соответствии с многоуровневым

принципом исследования позволяет проводить оценку ФН как СИА целиком, так и выполняемых процессов, а также отдельных процедур, таких как ПИ участников удалённого ЭВ.

Достоверность и обоснованность научных положений, результатов и выводов работы обеспечивается многосторонним анализом современного состояния исследований в предметной области, системным обоснованием предложенных методов, моделей и алгоритмов, не противоречащих известным положениям других авторов, достаточной апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также подтверждается положительным эффектом от внедрения в практику построения и модернизации СИА в организациях различного подчинения.

Научная значимость работы состоит в развитии теории и методологии обеспечения информационной безопасности в части создания новых и совершенствовании существующих моделей, методов и алгоритмов оценки доверия с целью построения иерархии доверия к результатам ИА участников удалённого ЭВ с учётом применяемых и перспективных технологий, учитывающих риски нарушения безопасности информации.

Практическая значимость результатов исследования заключается в их использовании для построения и модернизации СИА современных ИС, что подтверждается актами о внедрении. Применение положений диссертационной работы позволяет сократить, как минимум, на 25% сроки проведения оценок безопасности, функциональной надежности и достоверности результатов ИА СД на этапах проектирования и эксплуатации ИС, а также администрирования СИА.

Прикладная направленность диссертационной работы состоит в использовании ее положений при разработке национальных стандартов по ИА, выполнении научно-исследовательских работ и поиске технических решений, используемых в ряде ведомств.

Реализация результатов работы. Разработанные в диссертации модели, методы и алгоритмы использовались при выполнении НИР и НИОКР в Министерстве коммуникаций и связи РФ, гос. контракт № 012/155 от 12.12.2011; таможенных органах РФ (9 гос. контрактов 2007–2011 гг.); Пенсионном фонде РФ (гос. контракты № 14-141-D от 18.05.2009, № 23-158-Д от 04.05.2010 и др. – всего 9 гос. контрактов); Федеральном агентстве по рыболовству, гос. контракт № 97-01/2011 от 31.05.2011; Центре

системы мониторинга рыболовства и связи, гос. контракты № 41-Ю от 24.11.2009 и № 44-10 от 08.12.2009; проекте АТЭС «Разработка руководства АТЭС по электронной коммерции» ECSG 06/2008T и CTI 53/2009T/ECSG; Министерстве образования и науки РФ, шифр работы (темы) 14.577.21.0172 от 01.11.2015; ФСТЭК России, шифр работ «Момент-16», 2016 г., «Идентификация», 2018 г.; при проектировании и производстве средств защиты информации JaCarta, JaCarta SF/ГОСТ, Secret Disk Enterprise, JaCarta Management System, СКЗИ «КриптоБД».

Положения, выносимые на защиту

1. Методология построения иерархии доверия к результатам ИА субъектов доступа на основе учета рисков и моделирования основных процессов и систем ИА с целью оценки надежности и безопасности обрабатываемой информации, отличающаяся от известных учетом анализа рисков и специфики процессов аутентификации, в том числе при переходе к облачным вычислениям и большим ИС, позволяющая оценивать планируемые или используемые методы и средства ИА для выработки рекомендаций с целью повышения доверия к результатам ИА пользователей ИС различного назначения. Соответствует п. 1 паспорта специальности 05.13.19.
2. Метод оценки рисков первичной идентификации субъектов доступа с помощью матриц рисков, позволяющий определять значения допустимых рисков и средние значения рисков вероятных опасных событий. Соответствует п. 7 паспорта специальности 05.13.19.
3. Методика многоуровневой оценки рисков на основе разбиения процессов аутентификации на ряд последовательных процедур, что позволяет определять вероятностные характеристики разнородных по длительности и повторяемости процедур ИА в корпоративных и открытых ИС. Соответствует п. 7 паспорта специальности 05.13.19.
4. Классификация идентификаторов, систем ИА, а также методов, средств и механизмов аутентификации для установления границ применимости различных технологий ИА по критериям целей и задач, а также обеспечения доступности, конфиденциальности и целостности идентификационных и аутентификационных данных пользователей ИС, предназначенная для разработки показателей доверия при первичной идентификации (достоверность, надежность и безопасность) и аутентификации (качество первичной идентификации, используемый метод аутентификации и способ генерации, хранения, применения

аутентификационной информации), а также многоуровневого анализа рисков работы систем ИА, позволяющего проводить оценки рисков с заданным уровнем детализации. Соответствует пункту 11 паспорта специальности 05.13.19.

5. Вероятностные модели и методики оценки ФН процессов ИА, позволяющие проводить оценку надёжности ПИ и аутентификации участников удалённого ЭВ. Соответствует пункту 2 паспорта специальности 05.13.19.

Апробация результатов работы. Результаты диссертационного исследования докладывались на научно-технических конференциях «Методы и технические средства обеспечения информационной безопасности» (2003–2019), научно-практических конференциях «Комплексная защита информации» (2005–2013), международных конференциях «Рускрипто» (2004–2019), «Инфофорум» (24 доклада, 2005–2016), «PKI-форум» (2003–2019), Уральском форуме «Информационная безопасность банков» (2009–2020), расширенных заседаниях Совета по обеспечению информационной безопасности таможенных органов РФ (2006–2015), региональном семинаре ITU (2013), совещании-семинаре работников ФНС России по вопросу информационной безопасности (2007–2017), конференциях Международной академии связи (2013–2019) и на других форумах.

Внедрение. Результаты работы внедрены в Пенсионном фонде РФ, Федеральной таможенной службе РФ, ГНИВЦ ФНС России, администрации Ленинградской области, ЗАО «РУСАЛ Глобал Менеджмент Б.В.», ООО «Удостоверяющий Центр Сибири», ОАО «Ростелеком-ДВ», ФБГУ ЦСМС Росрыболовства, ЦКБ Управления делами Президента РФ, МИАЦ РАМН, Московском городском суде, ИАЦ г. Санкт-Петербурга, ООО НТЦ «Фобос-НТ», ОАО «Газпромбанк», КБ «Возрождение», учебном процессе Томского государственного университета систем управления и радиоэлектроники, Нижегородского государственного университета им. Н.И. Лобачевского, Национального исследовательского университета «Московский институт электронной техники» и МГТУ им. Н.Э. Баумана.

Личный вклад автора и публикации по теме диссертационной работы. Формулирование темы исследования и постановка научных задач по изучению отдельных аспектов ИА выполнялись автором самостоятельно. Более 85% объема всех работ, связанных с темой диссертационного исследования, выполнено лично автором.

По теме диссертации имеется 67 публикаций (из которых 50 без соавторов) в изданиях, рекомендованных ВАК России, две статьи в изданиях, цитируемых в Web of Science, получены два патента на изобретение: № 2523174 от 22.05.2014 (соавтор) и № 2635927 от 05.09.2016 (соавтор), в соавторстве опубликованы 3 монографии, 3 учебных пособия, из них два с грифом УМО.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений. Общий объем работы составляет 357 с. машинописного текста, содержит 47 рисунков и 39 таблиц. Список литературы включает 258 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение. Обоснована актуальность темы диссертации, дана ее краткая характеристика, сформулированы проблема, цель и задачи исследования, определены объект и предмет работы, приведены положения, выносимые на защиту, аргументированы научная ценность и практическая значимость, представлены данные об апробации и результатах внедрения, изложено краткое содержание глав диссертации.

В **первой главе** выполнен анализ научных работ по теме диссертации, международных и российских стандартов, зарубежной и отечественной НПБ по вопросам регулирования процессов ИА. Выявлена необходимость развития новых подходов к решению задач оценивания рисков ИА, включающих разработку **математических моделей, методик** и **алгоритмов** проведения соответствующих оценок. С увеличением количества зарегистрированных в ИС субъектов доступа системы ИА, кроме решения традиционных задач обеспечения конфиденциальности и целостности циркулирующей в системах информации, должны удовлетворять требованию доступности, т.е. подчиняться правилам систем массового обслуживания, а также обеспечивать конфиденциальность идентификационных данных (ИД) пользователей.

Установлена потребность в разработке новых подходов, методов и моделей, адаптированных к проведению анализа **функциональной надежности** работы СИА как существенной части системы управления доступом ИС предприятия.

Выявлена взаимосвязь **безопасности, надёжности** и **достоверности** результатов ИА, оценка которых базируется на **анализе рисков**.

Обоснована необходимость введения **уровней доверия** к результатам ИА, применение которых позволяет существенно повысить эффективность управления доступом пользователей, в том числе в удаленном режиме.

Анализ НПБ РФ показал необходимость разработки **системы национальных стандартов** по ИА, а также совершенствования отечественной НПБ по вопросам регулирования процессов ИА. В отличие от рассмотренных международных стандартов, в целях совершенствования отечественной НПБ по ИА требуется разработка показателей доверия и научно обоснованных рекомендаций, особенно для объектов критической информационной инфраструктуры (КИИ).

Во **второй главе** представлены основные положения **методологии** формирования иерархии доверия к результатам идентификации субъектов доступа, базирующиеся на материалах научных исследований, а также на международных и национальных стандартах (рисунок 1). Под методологией предлагается понимать совокупность способов (методов, моделей, алгоритмов) достижения поставленной цели. Для исследования доверия к результатам идентификации необходимо определить характеристики процесса идентификации, позволяющие с помощью оценки рисков установить определенный уровень доверия. Установлено, что в качестве базовых характеристик должны использоваться ФН работы системы идентификации, достоверность ПИ и безопасность персональных данных, которые обрабатываются и хранятся в ИС.

Впервые идентификация разделена на первичную, выполняемую однократно при регистрации нового пользователя, и вторичную идентификацию (ВИ), выполняемую при каждом запросе субъекта на доступ. Сформулированы цели, задачи и требования к ПИ и ВИ. Целью ПИ является установление (подтверждение) соответствия между СД и заявленными им ИД. ПИ должна определить, тот ли это субъект, за кого себя выдает, и возможность его регистрации в конкретной ИС. В результате ПИ субъекту (объекту) доступа присваивается уникальный идентификатор доступа, который однозначно определяет соотнесенную с ним зарегистрированную ИИ и аутентификационную информацию (АИ). При идентификации взаимодействуют субъект доступа, регистрирующая и доверяющая стороны. При этом регистрирующая сторона осуществляет ПИ, регистрацию и хранение ИИ, а доверяющая сторона – ВИ СД. Дополнительно в ПИ может участвовать полномочная сторона, выполняющая верификацию ИД субъекта и их подтверждение официальными свидетельствами.

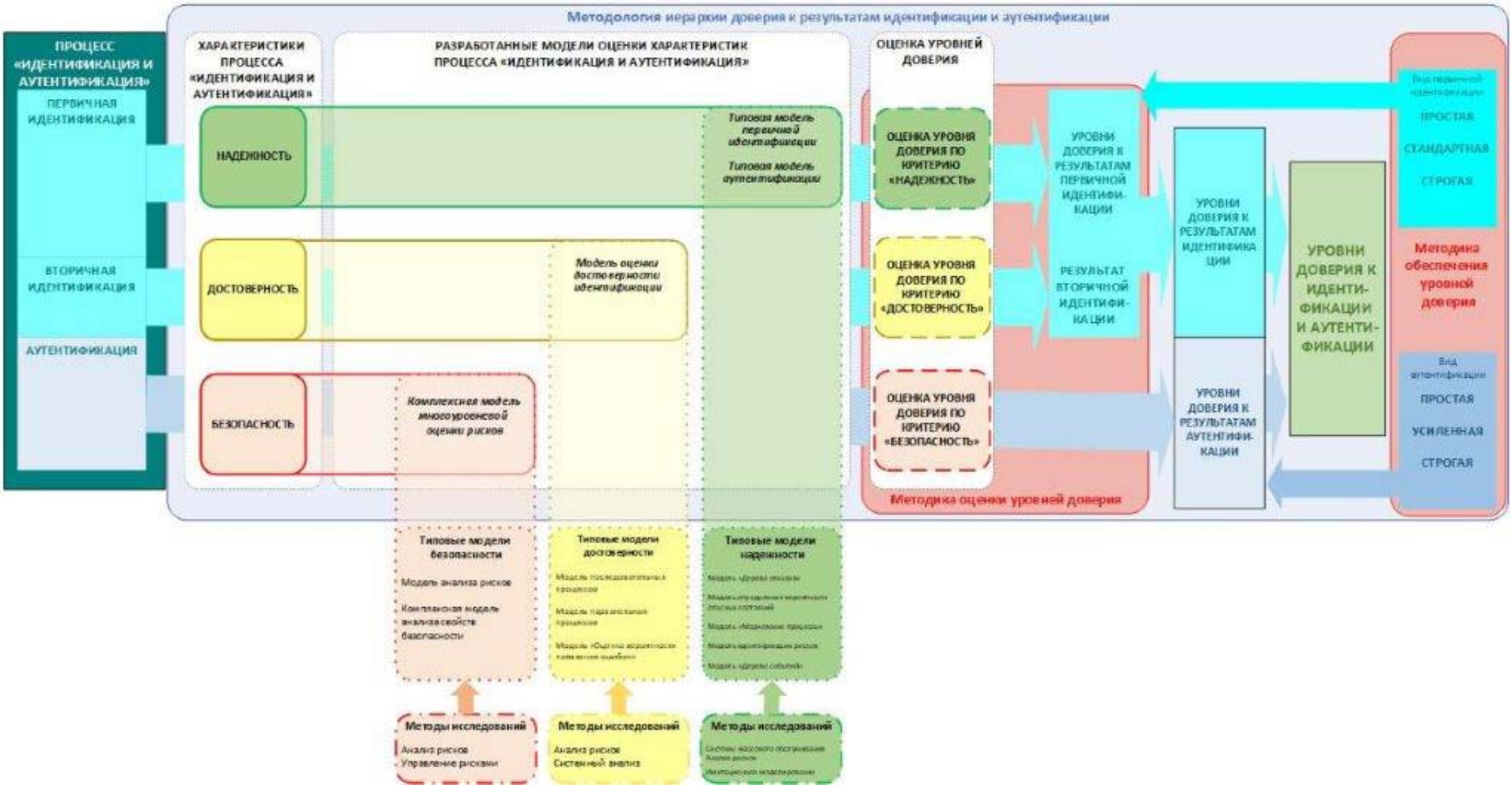

Рисунок 1 – Методология формирования иерархии доверия к ИА

Установлено, что доверие к результатам идентификации определяется главным образом результатами ПИ и зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем ИдА, верификации идентификационных атрибутов и привязки ИИ к личности заявителя (таблица 1).

Установлены три уровня доверия к результатам идентификации: низкий, средний и высокий. На низком уровне доверия к результатам идентификации имеется некоторая уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответствует зарегистрированной ИИ. На среднем уровне доверия к результатам идентификации появляется умеренная уверенность. На высоком уровне доверия к результатам идентификации существует значительная уверенность в том, что субъект доступа действительно соответствует зарегистрированной ИИ, которая однозначно определяется соотнесенным с ней предъявленным идентификатором доступа. Высокий уровень доверия к результатам идентификации соответствует высокому уровню доверия к результатам ПИ при условии успешной ВИ.

Указанные положения вошли в первый национальный стандарт ГОСТ Р 58833-2020 «Идентификация и аутентификация. Общие положения» и в проект ГОСТ Р ХХХ-2020 «Идентификация и аутентификация. Уровни доверия к результатам идентификации», куда также введены основные понятия и требования к организации процессов идентификации с целью достижения определенных уровней доверия к полученным результатам.

Впервые проведена оценка рисков ПИ. Рассмотрены типовые угрозы и возможные атаки, идентифицированы основные риски ПИ, которые согласно ГОСТ Р 31010 рассмотрены в виде набора ВОС (таблица 2).

Для указанного набора ВОС на основе принципа ALARP (As low as reasonably practicable – низкий, насколько реально возможно) построены матрицы рисков (МР), анализ которых позволил определить уровни допустимых рисков для трех типов информационных систем (ИС): закрытых (корпоративных), открытых ИС с личной явкой нового пользователя к регистратору и открытых ИС без личной явки субъекта к регистратору.

Для повышения точности расчетов использовался динамический способ построения МР и оценивания рисков, разработанный в АО «НИИАС».

Таблица 1 – Общая характеристика уровней доверия к результатам ПИ

Первичная регистрация субъекта (объекта) доступа			Необходимость подтверждения идентифика-ционных данных	Уверенность в том, что субъект действительно соответствует заявленным идентификацион-ным данным	Уровень доверия к результатам первичной идентификации	Возможность регистрации субъекта (объекта) доступа
Уникальность идентифика-ционной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных в электронных реестрах	Привязка идентифика-ционных данных				
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Не рассматривается	Не рассматривается	Не рассматривается	Отказ в регистрации субъекта доступа
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Отсутствует необходимость подтверждения	Нет уверенности	Не достигнут низкий уровень доверия	Регистрация субъекта (объекта) доступа как анонима
Уникальность обеспечивается	Существование не проверяется	Привязка не выполняется	Необходимо подтверждение	Некоторая уверенность	Низкий уровень доверия	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование подтверждается свидетельствами	Привязка с использование м одного фактора	Необходимо подтверждение	Умеренная уверенность	Средний уровень доверия	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование подтверждается официальными свидетельствами	Привязка с использование м двух и более факторов	Необходимо подтверждение	Значительная уверенность	Высокий уровень доверия	Регистрация субъекта (объекта) доступа

Таблица 2 – Пример идентификации типовых рисков первичной идентификации

Номер ВОС	Элементы риска	Причины опасных событий	Источники опасных событий	Характер воздействий	Обстоятельства воздействий
1	Подбор схожего лица, грим, маска	Желание злоумышленников совершить действия от имени заявителя	Информация о потенциальной возможности совершения действий	Маскарад. Подлог официальных документов	Невнимательность регистратора, помехи, социальная инженерия
2	Подделка официальных документов	Желание злоумышленников совершить действия от имени заявителя	Информация о потенциальной возможности совершения действий	Подделка официальных документов, ч.3 ст.327 УК РФ	Отсутствие обученных сотрудников, регистратора и оборудования
3	Отказ от регистрации	Уход от ответственности	Зарегистрированный пользователь	Непризнание участия в регистрации и личной подписи	Неточное исполнение регламента регистрации
4	Наличие ошибок в официальных реестрах	Невнимательность оператора, сбои и ошибки при передаче	Человеческий фактор	Наличие совпадающих идентификационных атрибутов	Невыполнение условий регистрации нового пользователя
5	Не достигнута уверенность в однозначной связи личности с идентификационными данными	Отсутствие подтверждающей информации надлежащего качества	Заявитель не предоставил, а регистратор не выполнил требований установления связи	Отказ заявителя от видеосъемки, непредоставление факторов владения и/или знаний, пассивность регистратора	Неточное исполнение регламента регистрации или его несовершенство
6	Отсутствие однозначной уникальности идентификационных атрибутов	Ошибки первого и второго рода	Ошибки оператора реестров, применение биометрии в сравнении «один ко многим»	Получение совпадающих значений идентификационных атрибутов из официальных источников	Неизбежность ошибок для баз данных, содержащих более 10^7 учетных записей
7	Внутренний инсайд, плохо организованная и/или задокументированная передача баз данных с ПДн	Слабый менеджмент ИБ, предпосылки к инсайду, только «бумажная» защита	Минимальная ответственность пользователей ИСПДн, отсутствие технических мер	Несанкционированный доступ, кража ПДн из ИС или при передаче внешним контрагентам	Наличие предварительного сговора или тщательного планирования события

При этом риск ***R*** оценивался как произведение частоты ВОС на величину последствий: ***R=F×C***, где ***C*** – вектор значений ущерба; ***F*** – вектор частоты возникновения нежелательного события. Пример расчета приведен на рисунке 2.

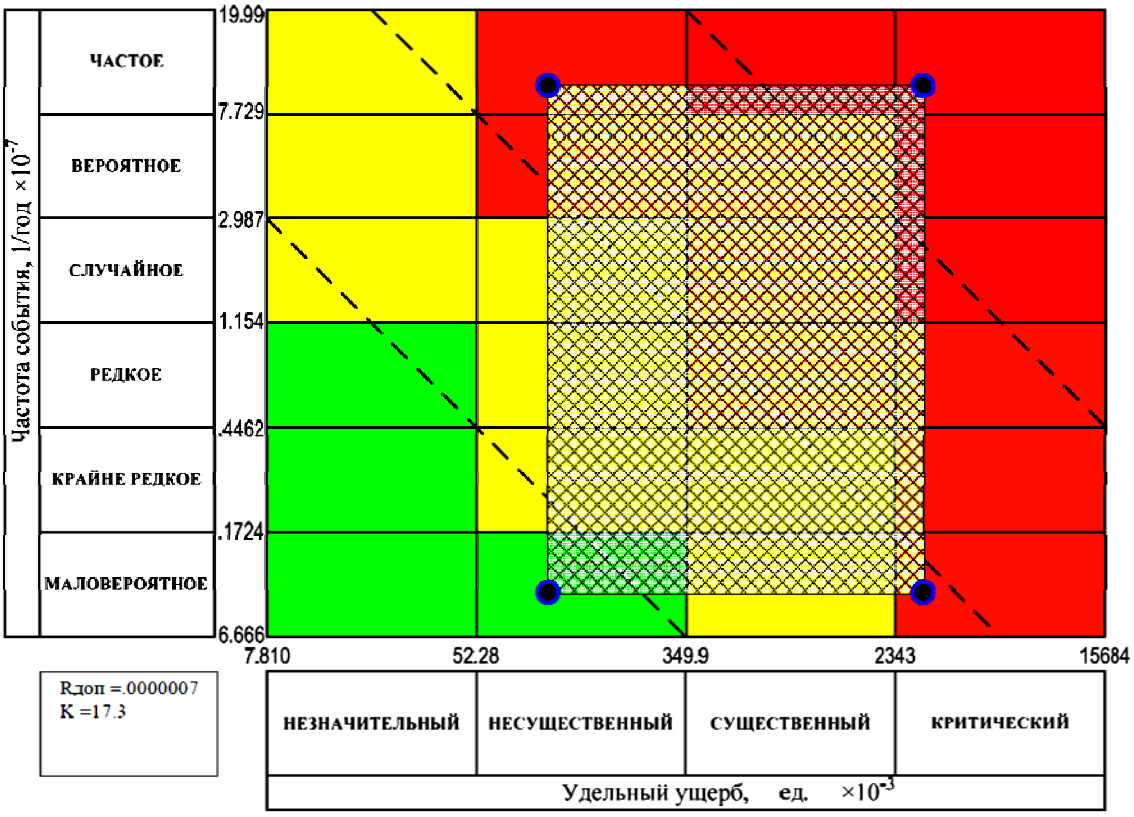

Рисунок 2 – Пример построения матрицы рисков ВОС2 для корпоративных ИС

Результаты расчетов средних значений рисков $R_{ср}$, допустимых значений рисков $R_{доп}$ и их отношения $R_{ср}/R_{доп}$ для корпоративных (корп.) ИС, открытых ИС с личной явкой нового пользователя к регистратору (с_л) и открытых ИС без личной явки (б_л) представлены на рисунке 3.

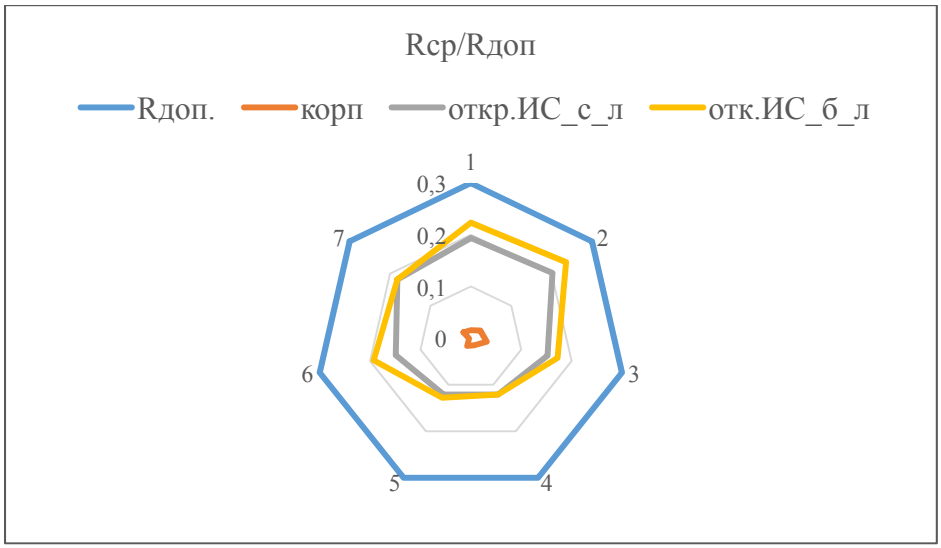

Рисунок 3 – Результаты расчета отношения $R_{ср}$ / $R_{доп}$ в виде лепесткового графика

Установлено, что уровень рисков ПИ для открытых систем на порядок выше, чем для корпоративных, при этом наибольший риск представляет регистрация нового пользователя в удаленном режиме без личного присутствия. Расчеты для различных ВОС выявили примерно одинаковые тенденции: величина относительного среднего риска в корпоративных ИС находится в пределах 3%, для открытых ИС с личной явкой – в пределах 12–20%, а для открытых ИС с регистрацией новых пользователей без личной явки – от 15 до 25%. При этом значения как допустимого, так и среднего риска при регистрации новых пользователей без их присутствия на два порядка выше, чем при личной явке.

Сформулирована задача идентификации СД в перспективных ИС, насчитывающих от сотен тысяч до десятков миллионов пользователей. Установлена зависимость необходимого количества идентификаторов с известными оценками безошибочности идентификации от числа зарегистрированных в ИС субъектов и объектов доступа.

В простейшем случае одного присвоенного при регистрации идентификатора в закрытой корпоративной ИС задача вторичной идентификации сводится к вычислению некоторой функции

$$y = f(a, x_1), \tag{1}$$

где x_1 – предоставленная претендентом на доступ буквенно-цифровая последовательность; a – индивидуальный параметр пользователя.

При этом происходит сравнение значения y с заранее занесённой (эталонной) величиной $Y_0 = F(a, X_0)$ в базу данных учётных записей (БДУЗ). В случае $y = Y_0$ идентификация считается успешно пройденной.

Для территориально разнесённых ИС с большим количеством пользователей (БИС), и особенно для ИС общего пользования (ИСОП) с самостоятельной регистрацией новых пользователей, одного идентификатора для выполнения ПИ может быть недостаточно. Для таких ИС уравнение (1) усложняется:

$$Y = f(a, x_1, x_2, ..., x_k) = f(a, X), \tag{2}$$

где k – число идентификаторов.

Функция проверки соответствия введённых значений идентификаторов $X = \{x_i\}$, $i = 1, 2, ..., k$, эталонным значениям $X_0 = \{x_{0i}\}$, $i = 1, 2, ..., k$, в базе данных учетных записей распадается на k пар. По сути, находится пересечение конечных множеств $\mathrm{Y} \bigcap \mathrm{Y}_0$. Если число N зарегистрированных субъектов и объектов в закрытых корпоративных ИС $N_{\text{ЗКИС}} \geq 10^4$ или в ИСОП $N_{\text{ИСОП}} \geq 10^3$, необходимо применять дополнительные меры для повышения

надёжности и безопасности автоматической ПИ. В частности, поскольку точность автоматической идентификации объекта с помощью одного идентификатора в сертификате ключа проверки электронной подписи (СКПЭП), как правило, не превышает 10^{-3}, требуется введение в процедуру идентификации некоторого числа дополнительных идентификаторов, зависящего от количества зарегистрированных пользователей в БДУЗ и класса ИС. В этом случае задача сводится к поиску минимального значения числа идентификаторов *K*, необходимого для однозначной идентификации конкретного субъекта или объекта из общего числа зарегистрированных объектов *N*.

Для общего решения задачи о достоверности идентификации субъекта (объекта) примем необходимость достижения заданного значения достоверности D в интервале $0 < D \le 1$ при использовании набора идентификаторов ID_i, $i = 1,2,...,M$. В качестве основной цели ПИ определим поиск минимального, но достаточного количества идентификаторов K для достижения заданного значения достоверности в зависимости от масштаба информационной системы.

В начальном приближении воспользуемся подходом структурной надежности на основе метода конечных автоматов, заключающимся в том, что проверку каждого предъявленного идентификатора будем считать независимо работающим (по надежности) прибором. Тогда достоверность идентификации D для схемы последовательно предъявляемых идентификаторов с номером i будет определяться соотношением

$$D = \prod_{i=1}^{K} (1 - q_i), \tag{3}$$

где q_i – вероятность ошибки работы i-го конечного автомата; K – число идентификаторов.

Из выражения (3) следует, что вероятность безошибочной работы системы, состоящей из последовательного соединения элементов, будет ниже, чем вероятность безотказной работы ее самого надёжного элемента.

В случае схемы параллельного (независимого) предъявления идентификаторов достоверность идентификации определяется по формуле

$$D = 1 - \prod_{i=1}^{K} q_i, \tag{4}$$

где q_i – вероятность ошибки работы i -го конечного автомата[1].

[1] Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем: учеб. пособие. СПб.: Университет ИТМО, 2015. 93 с.

Для выполнения основной функции идентификации – уникальности и различимости каждого субъекта из общего количества N – необходимо стремиться к достижению величины достоверности идентификации:

$$D \geq 1 - \frac{1}{N+1}. \quad (5)$$

Таким образом, для БИС предпочтительнее схема одновременного предъявления идентификаторов, что согласуется с постулатом надежности.

Для оценки **надежности** процедуры ПИ принят ряд допущений: верификацию каждого идентификатора можно представить в виде конечного автомата; результат проверки одного идентификатора не влияет на результаты проверки другого. При этом к системе идентификации применяется марковское представление случайных процессов, при котором на элемент системы действует простейший поток заявок. Сумма вероятностей выходов из каждого состояния есть полная группа несовместных событий $\sum_{i=1}^{n} P = 1,$ где n – число состояний системы.

Процедуру регистрации нового пользователя в ИС открытого типа (пользователь регистрируется самостоятельно) упрощенно можно представить в виде следующих состояний:

1 – претендент послал запрос на сервер центра регистрации (ЦР) с целью зарегистрироваться в ИС;

2 – идентификаторы претендента пришли на сервер вместе с запросом на регистрацию. С сервера ЦР высылается запрос на верификацию;

3 – получены ответы на запрос сервера. Если данные совпали, ЦР создает учетную запись (УЗ) нового легального пользователя ИС;

4 – ЦР создал или зарегистрировал АИ нового легального пользователя;

5 – ЦР выдал пользователю ЭУ (например, в виде сертификата ключа проверки подписи) и АИ в случае, когда АИ была создана ЦР.

В приведенных обозначениях состояний системы (СС) процесс регистрации можно представить в виде направленного графа, где СС обозначены цифрами 1–5 (рисунок 4).

Определим вероятность работы системы до возникновения первого функционального отказа $P_{ФО}$:

$$P_{ФО} = 1 - P_1 + P_1(1 - P_2) + P_1P_2(1 - P_3) + P_1P_2(1 - P_3) + \\ + P_1P_2P_3(1 - P_4) + P_1P_2P_3P_4(1 - P_5), \quad (6)$$

где P_i – вероятность нахождения системы в состояния i, i=1, 2, 3, 4, 5.

Вероятность наступления функционально опасного отказа

$$P_{\text{ФОО}} = 1 - P_1 P_2 P_3 P_4 (1 - P_5). \qquad (7)$$

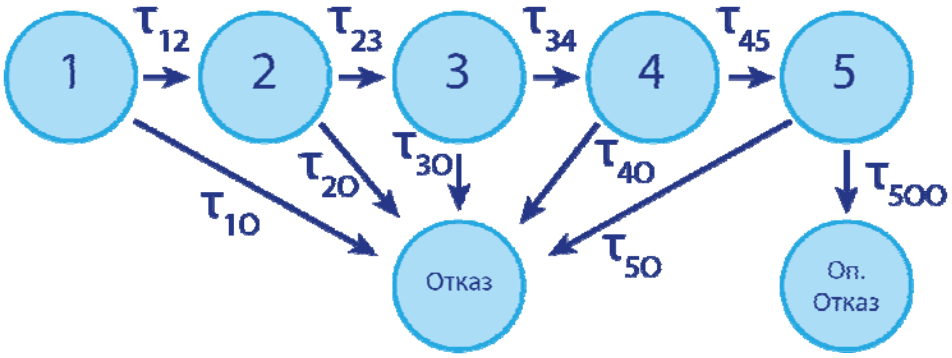

Рисунок 4 – Направленный граф состояний системы регистрации

Пример расчета вероятностей отказа и опасного отказа для равновероятного нахождения системы в состояниях $P_1 = P_2 = \cdots = P_5$ приведен на рисунке 5.

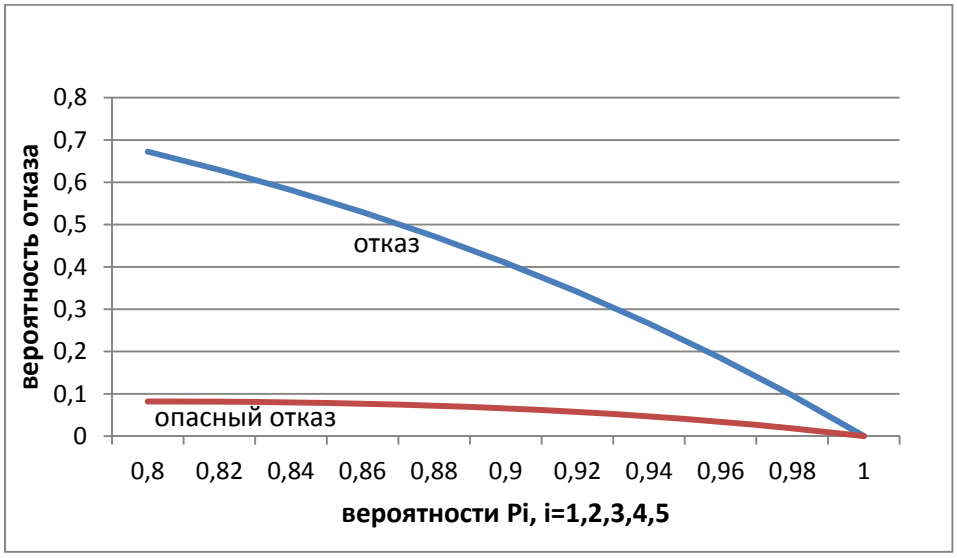

Рисунок 5 – Пример параметрического расчета вероятностей отказов

Для повышения надёжности результатов идентификации схема в виде последовательного предъявления и верификации должна быть заменена схемой параллельного сравнения предъявленных претендентом идентификаторов с имеющимися в официальных реестрах. В этом случае удастся достичь необходимого уровня надёжности ПИ пользователя при доступе к информационным ресурсам, оценить которую сверху можно по формуле

$$q_1 \cdot q_2 \cdot \ldots \cdot q_K \le \frac{1}{N+1}, \qquad (8)$$

где q_i – вероятность безошибочной идентификации с применением i-го идентификатора; K – минимально необходимое, но достаточное число идентификаторов; N – количество зарегистрированных в ИС объектов и субъектов доступа.

Таким образом, установлено, что требования к достоверности ПИ, определенной по формуле (5), и ФН ПИ (8) совпадают.

Предложена универсальная классификация основных используемых на практике идентификаторов. Показана роль корпоративного идентификатора для организации доступа пользователей.

На основе проведенных исследований сформулированы *показатели доверия* (функциональная надежность работы системы идентификации, достоверность получаемых результатов и безопасность личных данных пользователей) и представлен *способ оценки доверия* к результатам идентификации в соответствии с предложенными критериями для ИС различного назначения, которые являются существенной частью предлагаемой в диссертационной работе методологии формирования иерархии доверия к результатам ИА.

Третья глава посвящена анализу процесса аутентификации и функционирования СИА с целью создания методологии формирования УД к результатам аутентификации. Рассмотрены основные информационные потоки и участники процессов ИА пользователей при УЭВ, в том числе при переходе к облачным вычислениям. Выполнен многоуровневый анализ угроз и векторов типовых атак для идентификации основных рисков аутентификации на основе многостороннего анализа (построение дерева событий, дерева неисправностей и вида отказов и др.). Для оценки рисков аутентификации проведен анализ применимости методов анализа рисков, рекомендованных ГОСТ Р 31010, установлена применимость 17 из 31 метода. Также установлена применимость пяти методов управления рисками, из них два метода (анализ вероятных опасных событий и экономический анализ) наиболее приемлемы для исследования процесса ИА. Выполнен анализ архитектуры и типовых схем СИА для закрытых корпоративных ИС и ИСОП с целью выявления типовых особенностей их функционирования для последующего исследования и моделирования. Разработана оригинальная классификация СИА по критериям выполнения целей обеспечения доступности, целостности и конфиденциальности, показывающая многообразие задач и вытекающих из них требований к безопасности и надёжности СИА, разделенных по уровням доверия (рисунок 6).

Показано, что проектирование, построение, поддержка и развитие СИА, а также выбор и внедрение средств ИА должны базироваться на циклическом анализе рисков. Установлено, что в целях обеспечения доступности, достоверности результатов и отказоустойчивости на этапах проектирования и совершенствования СИА необходимо исследовать с помощью методов теории массового обслуживания и теории ФН с учетом требований безопасности хранимой и обрабатываемой информации.

Разработана классификация средств идентификации и аутентификации по признаку применяемых технологий (рисунок 7).

Классификация для определения границ областей применения наиболее развитых технологий аутентификации по критериям целей и выполняемых задач представлена на рисунке 8.

Усовершенствована общая схема анализа рисков применительно к анализу аутентификации, включающая исследование угроз, уязвимостей, определение ВОС и степени последствий их наступления до и после использования контрмер. Усовершенствование состоит в рассмотрении многоуровневых пространств (угроз, уязвимостей, последствий) и применении многоуровневой модели СИА, что позволяет уточнять величину рисков и обосновывать новые подходы к оценке защищённости системы. В частности, с помощью многоуровневой модели угроз детализировано влияние компонентов СИА по принципу от «общего к частному» на величину остаточных рисков, что способствовало обоснованию необходимости введения уровней доверия к результатам ПИ субъекта при регистрации нового пользователя в ИСОП.

Установлено, что наиболее критичными являются процессы ПИ субъекта доступа и хранения АИ. Углублённый анализ на втором и третьем уровне детализации показал, что к наиболее опасным событиям необходимо также отнести процедуру предъявления АИ. Возможности разработанной методики оценки рисков продемонстрированы на примере идентификации рисков экспертным методом применительно к работе СИА.

Размер риска может быть оценен по формуле $R = \sum_{i=1}^{M} \left[P(U_i) \cdot L(U_i) \right]$, где U_i – опасное событие i; $P(U_i)$ – вероятность наступления i-го опасного события; $L(U_i)$ – ущерб от наступления i-го опасного события; M – количество ВОС. При этом ВОС ранжированы на основе вероятности появления опасного события в год P и относительного значения риска $\overline{R}$ (таблица 3). Условие нормировки $\overline{R} = \dfrac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} L(U_i)} = 1$.

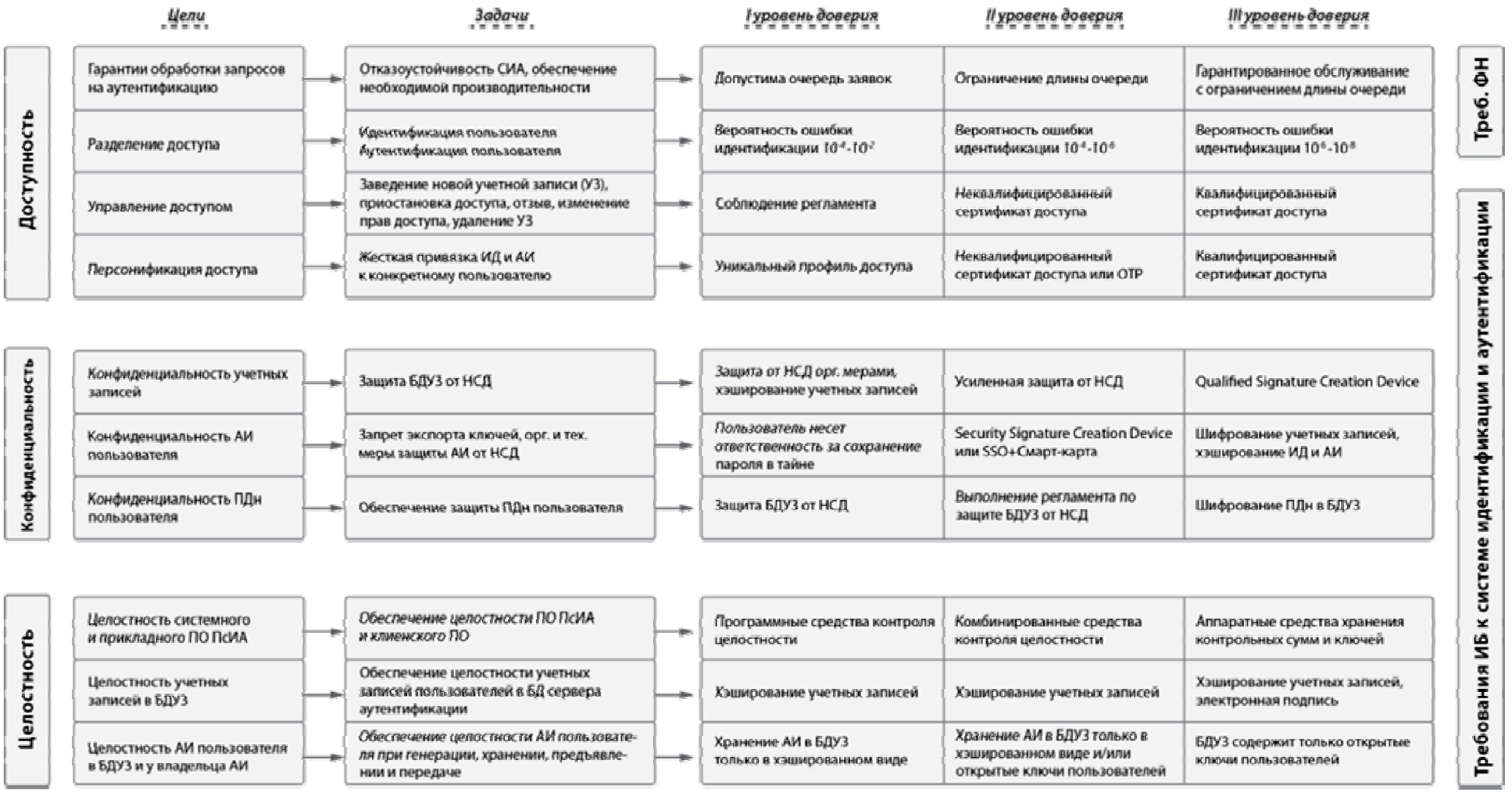

Рисунок 6 – Классификация СИА по целям и задачам информационной безопасности

Рисунок 7 – Классификация средств идентификации и аутентификации

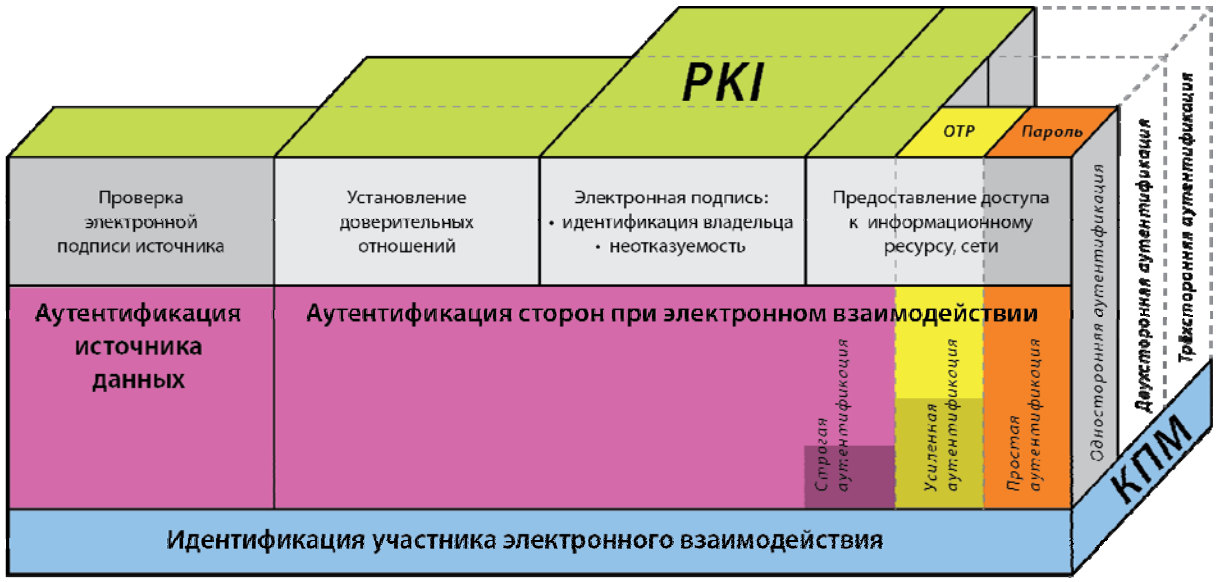

Рисунок 8 – Классификация по целям и задачам применения методов ИА

Результаты ранжирования представлены на рисунке 9 в виде пронумерованных точек, обозначающих номер вероятного опасного события в таблице 3, в плоскости параметров $\{\bar{R}, (-\lg P)\}$.

Для снижения риска ВОС 2 (фишинг – подмена сайта, на который пользователю необходимо предоставить доступ) достаточно перейти с парольной аутентификации на технологию защищенного доступа с использованием двусторонней взаимной аутентификации на основе

цифровых сертификатов на стороне сервера и клиента, что ведет к снижению вероятности подмены сайта приблизительно на два порядка (с 10^{-4} до 10^{-6}). Снижение рисков в рассмотренных примерах может проводиться не только в отношении частоты реализации ВОС, но и посредством уменьшения величины риска за счет организационных и технических мер защиты, таких как внедрение СЗИ.

Таблица 3 – Пример ранжирования рисков аутентификации при электронном удаленном взаимодействии

ВОС	Описание опасного события	P	$\overline{R}$
1	Воздействие вредоносного ПО	10^{-3}	0,122
2	Фишинг	10^{-4}	0,141
3	Риск добровольной передачи носителя (ключа и АИ)	10^{-4}	0,110
4	Ошибки или целенаправленные действия при смене АИ	10^{-4}	0,096
5	Использование уязвимостей СИА	10^{-4}	0,088
6	Ошибки валидации	10^{-5}	0,120
7	Spoofing (подмена) доверенной стороны	10^{-5}	0,089
8	Помощь инсайдера	10^{-5}	0,084
9	Регистрация злоумышленника под видом легального пользователя	10^{-6}	0,137

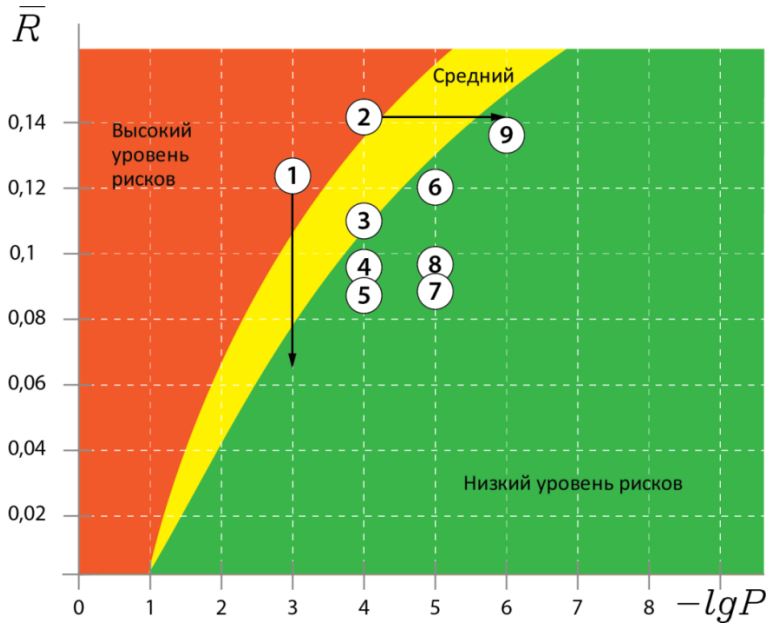

Рисунок 9 – Пример управления рисками для СИА

К достоинствам данного метода анализа рисков аутентификации можно отнести наглядность проводимого анализа. Этот метод наряду с известным методом экономического анализа можно рекомендовать для управления рисками СИА.

Для исследования ФН СИА применены известные и разработаны новые вероятностные модели, позволяющие оценить производительность СИА. Система многоуровневых моделей для исследования надежности СИА на этапах проектирования должна включать модели исследования поведения СИА, описываемых с помощью инструментов системы массового обслуживания (СМО). Модели второго уровня детализации СИА, на котором учитываются процедуры, составляющие процессы ИА, позволяют исследовать влияние надежности выполнения отдельных процедур и определить их вероятностные характеристики. Модели третьего уровня детализации СИА дают возможность разработать методику оценки влияния отказов и опасных отказов на выполнение критичных процедур. Модели четвертого уровня позволяют детализировать риски на микроуровне, например на уровне чипа смарт-карты.

На основе анализа рисков сформулированы показатели доверия к результатам отдельно взятого процесса аутентификации (достоверность, функциональная надежность и безопасность). Показано, что доверие к результатам аутентификации зависит от достигнутого уровня доверия к результатам ПИ, применяемых методов аутентификации, способа генерации, хранения и предъявления АИ и уровней выполнения требований ИБ к работе самой СИА, а также к защите ИдА, являющихся ПДн. Выявлено, что учет количества факторов аутентификации имеет смысл только при их одновременном использовании. Планируемый протокол аутентификации должен соответствовать заданному уровню доверия к методу аутентификации.

Разработан метод оценки доверия к результатам ИА зарегистрированного субъекта доступа в соответствии с предложенными критериями доверия. В отличие от отдельно взятых процессов идентификации и аутентификации, доверие к итоговым результатам ИА складывается из полученных результатов доверия к надежности идентификации нового пользователя при регистрации, обеспечению конфиденциальности секрета (АИ) на протяжении его жизненного цикла и корректности реализации методов аутентификации. Уровни доверия к применяемым методам аутентификации представлены в таблице 4.

На основе выполненного анализа разработана методология формирования уровней доверия к результатам ИА, отличающаяся от зарубежных аналогов учетом рисков и специфики применения сертифицированных СЗИ и СКЗИ.

Таблица 4 – Уровни доверия к широко используемым методам аутентификации

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от известных атак	односторонний	знание	низкий
2	сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	одноразовый пароль	доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	односторонний	владение	
3	"второй канал" (пример: телефон+SMS)	одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение	средний
4	устройство одноразовых паролей, динамически генерирующее OTP	одноразовый пароль	защита устройства	односторонний	владение	
5	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия	высокий
6	криптографическй ключ в СВТ или на незащенном паролем носителе	криптографические ключи	защита ключей	односторонний или взаимный	владение	
7	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание	
8	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	очень высокий
9	СВТ с криптографическим ПО и отдельное устройство с помещённым в него и хранящемся в нём криптографическим ключом + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия	
10	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия	самый высокий

Иерархия доверия к результатам идентификации и аутентификации субъектов доступа представлена на рисунке 10.

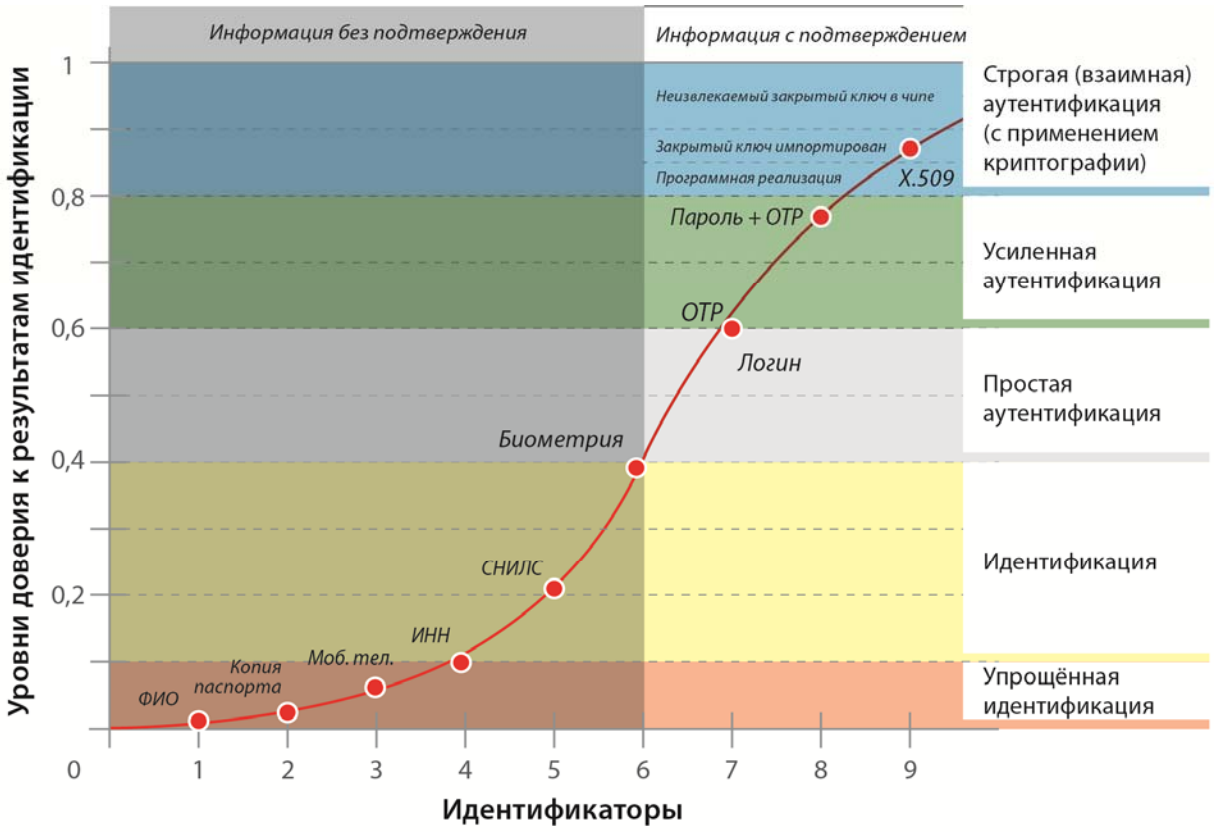

Рисунок 10 – Уровни доверия к идентификации и аутентификации субъекта доступа

Приведенные в **четвертой главе** примеры показывают возможности применения предложенной методологии к решению практических задач.

Непосредственное участие автора в разработке системы национальных стандартов по ИА (ГОСТ Р 58833 «Идентификация и аутентификация. Общие положения» и последующие стандарты по ИА в рамках ТК 362 и ТК 22) является примером синтеза науки и нормотворчества.

Примеры внедрения разработанных и модернизированных в диссертационном исследовании методов анализа процессов ИА показывают его не только научный, но и прикладной характер. Так, разработанная многоуровневая система оценки рисков ИА предоставляет возможность проведения анализа на необходимом уровне детализации, что позволило, в частности, создать защищенное средство отчуждения и переноса информации JaCarta SF ГОСТ, выполненное с учетом требований ФСТЭК России к средствам отчуждения информации на съёмных носителях. Это изделие можно применять в ИС, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну. Участие

автора в разработке и создании данного изделия подтверждено патентом 2635927 от 05.09.2016. «Компактный аппаратный электронный носитель информации с многоуровневым регулированием доступа к отдельным разделам памяти», который внесен в список «100 лучших изобретений России» за 2017 год.

На основе созданной в диссертации методологии разработаны примеры требований к аутентификации некоторых групп пользователей при их взаимодействии для достижения определенных уровней доверия. Установлено, что самым безопасным с наиболее достоверными результатами методом аутентификации является строгая аутентификация, основанная на применении цифрового сертификата доступа.

При этом самым надежным и безопасным устройством аутентификации является смарт-карта класса SSCD с неизвлекаемыми закрытыми ключами. Такие устройства сертифицированы по требованиям ФСБ России, при этом срок использования закрытого ключа, в отличие от 15 месяцев для программной реализации, разрешен до 3 лет.

Рассмотрена задача обеспечения юридической силы (ЮС) и юридической значимости электронных документов (ЭД). Показано, что аналогом реквизитов бумажных документов являются сервисы безопасности, применяемые для создания, оформления и подписи ЭД. Установлено, что минимально необходимым и достаточным для большинства операций с ЭД, обладающих ЮС, является следующий набор сервисов безопасности:

- аутентификация (ГОСТ Р 588-33-2020, ISO 29115: 2013, 9798-3:1998);
- электронная подпись (ГОСТ Р 34.10-2012, ISO 7498, ISO/IEC 13888-1);
- метка доверенного времени (RFC 3161 «Time-Stamp Protocol (TSP)»);
- валидация сертификата ключа проверки подписи (RFC 2459);
- проверка полномочий подписанта (ITU-T X.509, v.7);
- доверенная гарантированная доставка документов и сообщений.

Использование совокупности указанных сервисов позволит поднять уровень доверия к ЭД до уровня официальных бумажных документов, что необходимо для развития цифровой экономики России.

Разработанный способ защиты данных под управлением различных СУБД и созданное на его основе СКЗИ «Крипто БД» (сертифицировано по требованиям ФСБ России до класса КС3) сочетают в себе синтез лучших практик аутентификации, шифрования данных и позволяют надежно защищать конфиденциальную информацию, в частности ПДн, в ряде критичных к разглашению информации ГИС России.

ЗАКЛЮЧЕНИЕ

В диссертации решена важная народно-хозяйственная проблема – разработана методология построения иерархии уровней доверия к результатам ИА субъектов доступа, в том числе при удаленном электронном взаимодействии, позволяющая значительно развить методы исследования ИА и формировать уровни доверия к результатам ИА в ИС различного назначения.

1. Сформулированы критерии доверия к результатам ИА. Установлено, что доверие к результатам идентификации в задачах управления доступом пользователей определяется главным образом уровнем доверия, достигнутым при ПИ заявителя во время его регистрации в конкретной ИС. Доверие к результатам ПИ зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем идентификационных атрибутов, доверия к результатам верификации этих идентификационных атрибутов и доверия к привязке ИИ к личности заявителя. Доверие к результатам аутентификации зависит от качества ПИ при регистрации, способа генерации, хранения и использования АИ (секрета), а также от методов аутентификации (протоколов, применяемых для аутентификации, количества используемых факторов и способов обмена АИ). Таким образом, в работе содержатся основные положения, методы и модели, необходимые для совершенствования способов ЗИ применительно к задаче ИА участников ЭВ, оценки рисков, достоверности, надежности, безопасности и формирования на их основе уровней доверия к результатам ИА.

2. Формализованы процедуры ПИ и ВИ, разработаны методики и модели анализа достоверности, безопасности и надежности идентификации при удаленном ЭВ на основе анализа рисков, позволяющие определить требования к ПИ в ИС с большим числом субъектов доступа.

3. Разработан метод оценки рисков ПИ для корпоративных ИС и систем открытого типа с личной явкой субъекта к регистратору и в удаленном режиме, без личной явки. Приведены оценки рисков для указанных типов ИС. Построены матрицы рисков ПИ, применение которых существенно повышает обоснование результатов анализа рисков на основе определенных из матриц рисков допустимых уровней рисков для типовых ВОС. Установлено, что значения относительного среднего риска для корпоративных ИС находятся в пределах 3%, для открытых ИС с личной явкой субъекта на регистрацию – в пределах 12–20%, а без личной явки – от 15 до 25%.

4. Проведен параметрический анализ влияния ошибок ПИ на достоверность результатов для разных моделей процесса верификации предъявленных субъектом идентификационных атрибутов при регистрации. Обоснована необходимость применения схемы одновременной (параллельной) верификации предъявленных субъектом идентификационных атрибутов, что значительно снижает результирующие ошибки.

5. Для оценки рисков аутентификации разработаны и модернизированы модели и методики, позволяющие проводить анализ рисков с необходимой глубиной детализации для ИС различного назначения. Разработаны многоуровневые модели и методы анализа рисков нарушения ИБ, включающие рассмотрение угроз, уязвимостей, ВОС и возможных последствий. Рекомендованы два метода управления рисками аутентификации.

6. Разработаны вероятностные модели и методики оценки ФН процессов ИА, а также методика оценки достоверности результатов при удаленном ЭВ для формирования уровней надежности ИА в ИС различного назначения.

7. На основе предложенной методологии и разработанных методов, моделей и методик решён ряд практических задач, что существенно повысило уровень защищённости информационных ресурсов Российской Федерации. На базе проведенного анализа международных стандартов и нормативных документов, а также стандарта ГОСТ Р 58833 «Идентификация и аутентификация. Общие положения», созданного с использованием положений диссертационной работы, под руководством и с непосредственным участием автора разрабатывается серия национальных стандартов по ИА.

8. Применение полученных научных результатов на стадиях проектирования и эксплуатации СИА позволяет на 35–45% сократить сроки проектирования и/или модернизации существующих ИС, снизить затраты на администрирование системы управления доступом на 25–40% и сократить количество инцидентов нарушений безопасности, связанных с идентификацией и аутентификацией, на 15–30%.

Таким образом, в диссертационной работе решена крупная научная проблема, имеющая существенное теоретическое и прикладное значение.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Учебные пособия и монографии

1. Аутентификация. Теория и практика / А.Г. Сабанов [и др.] ; под ред. проф. А.А. Шелупанова. – М.: Горячая линия – Телеком, 2009. – 552 с.

2. Защита персональных данных в медицинских организациях / А.Г. Сабанов [и др.]. – М.: Горячая линия – Телеком, 2012. – 206 с.

3. Национальная платежная система. Бизнес-энциклопедия / А.Г. Сабанов [и др.] ; ред.-сост. А.С. Воронин. – М.: КНОРУС : ЦИПСиР, 2013. – 424 с.

4. Платежные карты: бизнес-энциклопедия / А.Г. Сабанов [и др.]. – М.: Маркет ДС, 2013. – 523 с.

5. Сабанов А.Г. Идентификация и аутентификация пользователей. Информационно-методическое пособие / А.Г. Сабанов. – Изд. дом «Афина», 2018. – Режим доступа: www.inside-zi.ru

6. Удостоверяющие автоматизированные системы и средства: Введение в теорию и практику удостоверяющих автоматизированных систем: моногр. / А.Г. Сабанов [и др.] ; под ред. С.В. Баушева и А.С. Кузьмина. – СПб.: БХВ-Петербург, 2015. – 304 с.

Основные статьи в журналах перечня ВАК

7. Сабанов А.Г. Об аутентификации при организации доступа к «облачным» сервисам в информационных системах общего пользования / А.Г. Сабанов // Вопросы защиты информации. – 2012. – № 4. – С. 50–58.

8. Сабанов А.Г. Методы исследования надежности удаленной аутентификации / А.Г. Сабанов // Электросвязь. – 2012. – № 10. – С. 20–24.

9. Сабанов А.Г. Аутентификация как часть единого пространства доверия / А.Г. Сабанов // Электросвязь. – 2012. – № 8. – С. 40–44.

10. Сабанов А.Г. Об уровнях строгости аутентификации / А.Г. Сабанов // Доклады ТУСУР. – 2012. – № 2(26). – С. 134–139.

11. Сабанов А.Г. Об оценке рисков удаленной аутентификации / А.Г. Сабанов // Электросвязь. – 2013. – № 4. – С. 27–32.

12. Сабанов А.Г. Об уровнях аутентификации в информационном обществе / А.Г. Сабанов // Инсайд. Защита информации. – 2012. – № 2(44). – С. 68–74.

13. Сабанов А.Г. Основные процессы аутентификации / А.Г. Сабанов // Вопросы защиты информации. – 2012. – № 3. – С. 54–57.

14. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам / А.Г. Сабанов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2013. – № 2-1. – С. 45–51.

15. Сабанов А.Г. Комплексная защита электронного документооборота / А.Г. Сабанов // Оборонный комплекс научно-техническому прогрессу России. – 2012. – № 4. – С. 72–77.

16. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2-1. – С. 61–67.

17. Сабанов А.Г. Комплексная защита электронного документооборота / А.Г. Сабанов // Оборонный комплекс научно-техническому прогрессу России. – 2012. – № 4. – С. 72–77.

18. Додохов А.Л. Способ защиты баз данных, содержащих персональные данные / А.Л. Додохов, А.Г. Сабанов // Вопросы защиты информации. – 2013. – № 3. – С. 4–9.

19. Сабанов А.Г. Модели для исследования безопасности и надежности процессов аутентификации / А.Г. Сабанов // Электросвязь. – 2013. – № 10. – С. 38–42.

20. Сабанов А.Г. Классификация процессов аутентификации / А.Г. Сабанов // Вопросы защиты информации. – 2013. – № 3. – С. 46–52.

21. Додохов А.Л. Один из подходов к защите персональных данных в публичных облачных приложения / А.Л. Додохов, А.Г. Сабанов // Вопросы защиты информации. – 2013. – № 2. – С. 3–9.

22. Сабанов А.Г. Концепция электронного пропуска сотрудника предприятия оборонно-промышленного комплекса / А.Г. Сабанов // Оборонный комплекс научно-техническому прогрессу России. – 2013. – № 3. – С. 10–16.

23. Сабанов А.Г. Вопросы идентификации и аутентификации в информационных системах общего использования / А.Г. Сабанов // Информационно-измерительные и управляющие системы. – 2013. – Т. 11, № 7. – С. 081–084.

24. Сабанов А.Г. Аутентификация при электронном обмене конфиденциальными документами / А.Г. Сабанов // Доклады ТУСУР. – 2011. – № 2(24). – С. 263–266.

25. Додохов А.Л. Исследование применения СУБД Oracle для защиты персональных данных / А.Л. Додохов, А.Г. Сабанов // Доклады ТУСУР. – 2011. – № 2(24). – С. 267–270.

26. Сабанов А.Г. Концепция моделирования процессов аутентификации / А.Г. Сабанов // Доклады ТУСУР. – 2013. – № 3(29). – С. 71–75.

27. Сабанов А.Г. Методика идентификации рисков процессов аутентификации / А.Г. Сабанов // Доклады ТУСУР. – 2013. – № 4 (30). – С. 93–97.

28. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации / А.Г. Сабанов // Инсайд. Защита информации. – 2013. – № 4(52). – С. 82–88.

29. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности / А.Г. Сабанов // Электросвязь. – 2014. – № 2 (113). – С. 6–9.

30. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации / А.Г. Сабанов // Вопросы защиты информации. – 2014. – № 1(104). – С. 13–22.

31. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии / А.Г. Сабанов // Электросвязь. – 2014. – № 5. – С. 44–47.

32. Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии / А.Г. Сабанов // Доклады ТУСУР. – 2014. – № 2(32). – С. 180–184.

33. Сабанов А.Г. Юридическая сила электронного документа: технологическая составляющая / А.Г. Сабанов // Инсайд. Защита информации. – 2014. – № 3 (57). – С. 20–25.

34. Сабанов А.Г. О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии / А.Г. Сабанов // Электросвязь. – 2014. – № 6. – С. 39–42.

35. Сабанов А.Г. Некоторые проблемы информационной безопасности предприятий среднего и малого бизнеса / А.Г. Сабанов // Инсайд. Защита информации. – 2015. – № 5(65). – С. 16–18.

36. Сабанов А.Г. Сравнительный анализ биометрических методов идентификации личности / А.Г. Сабанов, С.Г. Смолина // Труды ИСА РАН. – 2016. – Т. 66, № 3. – С. 12–21.

37. Сабанов А.Г. Формирование уровней доверия к идентификации и аутентификации субъектов при удаленном электронном взаимодействии / А.Г. Сабанов // Электросвязь. – 2015. – № 10. – С. 46–51.

38. Сабанов А.Г. О неизвлекаемости закрытых ключей / А.Г. Сабанов // Инсайд. Защита информации. – 2015. – № 2. – С. 30–33.

39. Сабанов А.Г. Доверенные системы как средство противодействия кибер-угрозам / А.Г. Сабанов // Инсайд. Защита информации. – 2015. – № 3. – С. 17–21.

40. Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Ч. 1 / А.Г. Сабанов // Инсайд. Защита информации. – 2016. – № 2(68). – С. 84–87.

41. Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Ч. 2 / А.Г. Сабанов // Инсайд. Защита информации. – 2016. – № 3. – С. 70–74.

42. Сабанов А.Г. О доверии к сервисам безопасности, обеспечивающим юридическую силу электронным документам. Ч. 1 / А.Г. Сабанов // Первая миля. – 2016. – № 1 (#54). – С. 42–43.

43. Сабанов А.Г. О доверии к сервисам безопасности, обеспечивающим юридическую силу электронным документам. Ч. 2 / А.Г. Сабанов // Первая миля. – 2016. – № 2 (#55). – С. 34–37.

44. Сабанов А.Г. Об уровнях аутентификации в информационном обществе / А.Г. Сабанов // Инсайд. Защита информации. – 2012. – № 2(44). – С. 68–74.

45. Sabanov A. Information Security Aspects in e-Commerce / A. Sabanov // APEC Conference, 15–16 November, 2008. – Pekin, Chine. – P. 78–83.

46. Сабанов А.Г. Некоторые проблемы идентификации при удалённом электронном взаимодействии / А.Г. Сабанов // Первая миля. – 2014. – № 2 (#41). – С. 94–97.

47. Сабанов А.Г. Биометрическая идентификация: оправдаются ли ожидания? / А.Г. Сабанов // Первая миля. – 2014. – № 1(#40). – С. 59–60.

48. Сабанов А.Г. Некоторые проблемы обеспечения безопасности интернета вещей / А.Г. Сабанов // Инсайд. Защита информации. – 2016. – № 4 (70). – С. 54–58.

49. Сабанов А.Г. Способ определения строгости аутентификации / А.Г. Сабанов // Электросвязь. – 2016. – № 8. – С. 56–61.

50. Сабанов А.Г. Некоторые проблемы доверия к электронному документу / А.Г. Сабанов // Инсайд. Защита информации. – 2018. – № 3(79). – С. 10–15.

51. Минаев В.А. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия / В.А. Минаев, И.Д. Королев, А.Г. Сабанов // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(30). – С. 43–49.

52. Сабанов А.Г. Критерии доверия к результатам идентификации субъектов доступа / А.Г. Сабанов // Электросвязь. – 2019. – № 3. – С. 38–44.

53. Сабанов А.Г. Уровни доверия к аутентификаторам / А.Г. Сабанов // Вопросы защиты информации. – 2019. – № 2. – С. 10–17.

54. Sabanov A.G. Assurance criteria to access entities identification results / A.G. Sabanov // Телекоммуникации. – 2019. – N 3. – С. 38.

55. Сабанов А.Г. Вопросы доверия при построении электронного правительства / А.Г. Сабанов // Инсайд. Защита информации. – 2010. – № 3 (32). – С. 66–70.

56. Сабанов А.Г. Уровни доверия к результатам идентификации и аутентификации субъекта доступа в период цифровой трансформации / А.Г. Сабанов // Вопросы кибербезопасности. – 2019. – № 5 (33). – С. 19–25.

57. Mamchenko Mark. Exploring the Taxonomy of USB-Based Attacks / Mark Mamchenko, Alexey Sabanov // Twelfth International Conference "Management of large-scale system development" (MLSD), 25 November 2019 / IEEE *Xplore*. – 2019. – P. 926–929. – DOI: 10.1109/MLSD.2019.8910969. – URL: https://ieeexplore.ieee.org/document/8910969.

58. Сабанов А.Г. Концепция предварительного анализа рисков первичной идентификации субъектов доступа / А.Г. Сабанов // Инсайд. Защита информации. – 2020. – № 2. – С. 74–79.

59. Сабанов А.Г. Метод анализа технологических рисков первичной идентификации субъектов доступа / А.Г. Сабанов, И.Б. Шубинский // Инсайд. Защита информации. – 2020. – № 3. – С. 57–61.

60. Сабанов А.Г. Моделирование процесса первичной идентификации субъектов доступа для оценки достоверности автоматической регистрации / А.Г. Сабанов // Инсайд. Защита информации. – 2020. – № 4. – С. 31–35.

Статьи в прочих рецензируемых научно-технических журналах и трудах

61. Сабанов А.Г. Вопросы доверия к результатам аутентификации субъекта доступа / А.Г. Сабанов // Методы и технические средства обеспечения безопасности информации». – 2019. – № 28. – С. 57–59.

62. Сабанов А.Г. Об уровнях доверия к первичной идентификации / А.Г. Сабанов // Методы и технические средства обеспечения безопасности информации. – 2018. – № 27. – С. 57–58.

63. Сабанов А.Г. Проблемы надежности идентификации и аутентификации при удаленном электронном взаимодействии / А.Г. Сабанов // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 80–82.

64. Сабанов А.Г. Анализ рисков аутентификации при удаленном электронном взаимодействии / А.Г. Сабанов // Методы и технические средства обеспечения безопасности информации. – 2014. – № 24. – С. 53.

65. Сабанов А.Г. Роль аутентификации и электронной подписи в обеспечении юридической силы электронным документам для систем M2M / А.Г. Сабанов // Материалы 4-й всероссийской научно-практической конференции «ГЛОНАСС-регионам», 20–21 мая 2014 г. / под общ. ред. А.Н. Новикова. – 2014. – С. 73–79.

Патенты и изобретения

Пат. 2523174 Российская Федерация. Способ защиты информации на материальном (бумажном) носителе. – Заявл. 22.05.14 ; опубл. 20.07.14. (соавтор)

Пат. 2635027 Российская Федерация. Компактный аппаратный электронный носитель информации с многоуровневым регулированием доступа к отдельным разделам памяти. – Заявл. 05.09.16 ; опубл. 08.11.17. (соавтор)

Список сокращений

АИ – аутентификационная информация
БИС – большая информационная система
ВИ – вторичная идентификация
ВОС – вероятное опасное событие
ГИС – государственная информационная система
ЗИ – защита информации
ИА – идентификация и аутентификация
ИД – идентификационные данные
ИИ – идентификационная информация
ИС – информационная система
ИСОП – информационная система общего пользования
НПБ – нормативно-правовая база
ПИ – первичная идентификация
СД – субъект доступа
СЗИ – средство защиты информации
СИА – система идентификации и аутентификации
УЭВ – удаленное электронное взаимодействие
ФН – функциональная надежность
ЭВ – электронное взаимодействие
ЭД – электронный документ
ЭУ – электронное удостоверение
ЮС – юридическая сила
SSCD – Secure signature creation device, устройство безопасной генерации ключей электронной подписи

Тираж 100 экз. Заказ 168.
Томский государственный университет
систем управления и радиоэлектроники.
634050, г. Томск, пр. Ленина, 40.
Тел. (83822) 533018.