На правах рукописи

Экз. №____

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

Диссертация на соискание учёной степени доктора технических наук

Томск 2020 г.

Официальные оппоненты:	Петров Петр Петрович, Доктор физ.-мат. наук, профессор, Высшая школа экономики
	Макаревич Олег Борисович, Доктор технических наук, профессор, ФГАОУВО "Южный федеральный университет"
	Язов Юрий Константинович, Доктор технических наук, профессор ГНИИИ ПТЗИ ФСТЭК
Ведущая организация:	Академия ФСО России, г.Орел

Защита диссертации состоится «15» _____ 2020 года в 10:00 часов на заседании диссертационного совета ДС 212.008.10 при Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Томский государственный университет систем управления и электроники» по адресу: пр. Ленина, 40, Томск, Томская обл., 634050.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Томский государственный университет систем управления и электроники».

Автореферат разослан « » _____ 2020 г.

Ученый секретарь диссертационного совета — Костюченко Евгений Юрьевич

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В связи с ускоряющейся информатизацией общества и ростом масштабов и количества информационных систем (ИС) различного назначения актуализировалась задача управления доступом пользователей к информационным ресурсам, решение которой, прежде всего, связано с процессами идентификации и аутентификации пользователей средствами информационной системы. Процессы аутентификации, как правило, необходимы тогда, когда взаимодействующие стороны испытывают дефицит доверия к подлинности предъявленных идентификаторов, особенно в условиях удалённого доступа и/или использования небезопасной среды обмена сообщениями.

В условиях резкого обострения информационного противостояния в современном мире и непрерывного роста количества кибератак на ИС различного назначения с целью получения несанкционированного доступа (НСД) к информационным ресурсам во всех сферах электронного взаимодействия (ЭВ), практически любая среда информационного обмена потенциально подвержена возможным атакам, а вопросы доверия к результатам автоматической идентификации и аутентификации (ИА) субъектов и объектов доступа становятся весьма актуальными практически для любой ИС.

Ряд вычислительных процессов в ИС проводится от имени пользователей, что формирует риски однозначной ассоциации определённого вычислительного процесса как действия, проводимого конкретным физическим лицом. С другой стороны, существуют риски того, что в операционной среде современных многозадачных информационных систем вычислительный процесс, действующий в интересах злоумышленника, может имитировать параллельное функционирование множества легальных субъектов и объектов доступа.

Для снижения указанных рисков и формирования определённого уровня доверия к подлинности взаимодействующих сторон (субъектов и объектов доступа) должны применяться научно обоснованные, закреплённые в нормативно-правовой базе и методических рекомендациях методы, механизмы и средства ИА в составе систем управления доступом, являющихся частью ИС.

Задача управления идентификацией и аутентификацией особенно важна для ИС, обрабатывающих информацию ограниченного доступа. Одной из главных задач системы управления доступом информационной системы является принятие обоснованного решения типа «свой/чужой» при обработке запроса на авторизацию.

В настоящее время в Российской Федерации наблюдается существенное отставание в части регулирования процессов идентификации и аутентификации [1, 2]. Результаты анализа [3] показали, что в последние 20 лет международные стандарты по идентификации и аутентификации непрерывно развиваются как количественно, так и качественно. При этом в Российской Федерации в части регулирования процессов идентификации и аутентификации действует единственный стандарт [4], разработанный Международной организацией по стандартизации в 1994 году и введённый в действие в нашей стране с 1999 года. Такое положение объясняется тем, что в связи с последствиями технологического провала 90-х годов по ряду направлений в научной и технической сферах проблемам исследования и регулирования процессов идентификации и аутентификации не уделялось достаточного внимания.

Это привело как к значительному отставанию в части нормативно - правовой базы по идентификации и аутентификации, так и к весьма скромному по полноте и качеству содержанию отечественной базы технических спецификаций (стандартов, методик, руководств и т.п.) методов, протоколов и технологий ИА. В условиях нуждающейся в совершенствовании нормативно-правовой базы и недостатка утверждённых методических рекомендаций уполномоченных органов возникла ситуация произвольного выбора владельцами ИС методов, механизмов и средств ИА от разных производителей в рамках несовершенных политик безопасности в отношении управления доступом, что породило рост рисков реализации атак, связанных с предоставлением доступа злоумышленнику. В то же время, с момента принятия Стратегии развития информационного общества в Российской Федерации, утверждённой Указом

Президента РФ от 7 февраля 2008 г. N Пр-212, стали более интенсивно развиваться ИС как гражданского, так и военного назначения.

Согласно постановлению Правительства РФ от 28 ноября 2011 г. N 977 в эксплуатацию поэтапно вводится единая система идентификации и аутентификации (ЕСИА). При этом актуальным становится развитие базовых принципов национальной универсальной платформы защищённого доступа к различным информационным ресурсам ИС, используемым для предоставления государственных услуг, в том числе – с учетом перехода к облачным вычислениям. Создание систем управления удалённым доступом к конфиденциальной информации (КИ), содержащей, в частности, персональные данные граждан (ПДн), является непростой проблемой. Не менее сложной, и во многом пока нерешённой проблемой, включающей в себя ИА сторон ЭВ, является обеспечение юридической силы электронным документам (ЮСЭД).

Без определения набора минимально-необходимых сервисов безопасности, обеспечивающих ЮСЭД, и выработки требований по поддержке сервисов, в том числе надежной ИА сторон ЭВ, полный переход к безбумажному документообороту в ряде правоотношений между государством, бизнесом и личностью может стать нерешаемой задачей.

Еще одна актуальная задача связана с развитием ИС с большим числом зарегистрированных субъектов доступа. Создание и развитие значительного числа ИС с числом субъектов доступа, насчитывающих сотни тысяч, а подчас и десятки миллионов пользователей, формирует необходимость научного поиска необходимого и достаточного числа традиционно используемых идентификационных атрибутов для достижения заданного уровня достоверности идентификации при регистрации нового пользователя и разработки иерархии доверия к результатам ИА для таких систем. Известно, что идентификация субъектов в таких ИС при ЭВ имеет вероятностную природу, обусловленную процессом верификации предъявленных идентификационных данных с занесёнными ранее значениями при регистрации субъектов в различные реестры и

базы данных. Многообразие технических реализаций применяемых схем информационного обмена, методов ИА в отсутствии достаточно чётких требований нормативной базы также нуждается во введении определённых уровней доверия к результатам ИА сторон ЭВ. Всеми указанными выше обстоятельствами определяется **актуальность** теоретических исследований процессов и систем ИА с целью выработки подходов к формированию иерархии доверия к результатам идентификации и аутентификации субъектов ЭВ.

Значительный вклад в развитие теории и практики ИБ АИС, в том числе, в рассмотрении проблем аутентификации и организации управления доступом, внесли А.П. Баранов [5], Н.А. Гайдамакин [6], В.А. Герасименко [7, 8], А.А. Грушо [9, 10], П.Д. Зегжда [11], А.М. Ивашко [12], В.А. Конявский [13, 14], А.И. Костогрызов [15, 16, 17], А.С. Кузьмин [18], А.А. Малюк [8], В.А.Минаев [19, 20, 21], С.Н. Смирнов [22, 23], А.А. Стрельцов [24], А.А. Тарасов [25, 26], Л.М. Ухлинов [27], А.В. Черемушкин [28, 29], В.Ф. Шаньгин [30], А.А. Шелупанов [31, 32, 33], В.П. Шерстюк [34], И.Б. Шубинский [35, 36], А.Ю. Щеглов [37], А.Ю. Щербаков [38]. В их исследованиях разработана концепция защиты информации, обоснованы принципы обеспечения ИБ и построения систем защиты информации объектов информатизации, электронных документов с использованием программно-аппаратных средств ЗИ, рассмотрены теоретические аспекты и методология организации криптографической ЗИ, развита теория функциональной надежности, основы теории функциональной устойчивости, а также сформулированы основы построения моделей угроз и нарушителей безопасности информации.

Указанные работы создали научно-методическую базу исследования многих аспектов защиты информации, в том числе ИА. Наиболее существенный вклад в развитие теории и практики ИА внесли А.П.Алферов [39], Н.А.Гайдамакин [6], А.А.Грушо [9], А.Ю.Зубов [40], коллектив МИФИ под руководством А.А.Малюка (А.И.Толстой, Н.Г.Милославская, С.В.Запечников и др.) [41] А.В.Черемушкин [28]. В работе В.Ф.Шаньгина [30] проблемам

идентификации и аутентификации уделено много внимания, материал аккуратно изложен (в основном на основе методических материалов МИФИ [41]), однако не содержит новых теоретических положений, моделей и методик исследования ИА. Наиболее фундаментальным трудом по аутентификации является учебник под ред. проф. Шелупанова [42], однако материал требует современных доработок. В частности, в указанных работах не рассмотрены вопросы ИА при удаленном электронном взаимодействии (УЭВ), не содержится анализа перехода к облачным вычислениям, нет детального рассмотрения процессов идентификации, аутентификации и оценки связанных с этими процессами рисков.

Достаточно близкой к теме настоящего диссертационного исследования является работа Н.А.Гайдамакина [6]. Однако несмотря на весьма скрупулезное исследование моделей безопасности при организации доступа пользователей вопросы ИА в ней отражены только в виде общих постулатов.

Анализ перечисленных работ показал отсутствие научного подхода к выработке требований по производительности и надежности систем ИА (обеспечение доступности сервиса ИА), хотя для некоторых методов аутентификации (применение одноразовых паролей) большей частью загружается не клиентское рабочее место (как в случае применения механизма аутентификации с применением электронной подписи), а вычислительные ресурсы сервера. Многие вопросы ИА просто не исследованы или не имеют логического завершения. Например, в работе [31] проведен анализ угроз процессам аутентификации в ИС, развиты модели и методы анализа с помощью сетей Петри, но не даны рекомендации, как ими пользоваться на практике. Анализ систем с помощью Сетей Петри, как известно, дает в качестве результата ответ на достижимость пути фишек и время пути.

Попытки ряда авторов, например, [37], [43] исследования надежности ИА также не привели к заметным научным результатам. Так, прямой перенос методов теории надежности механизмов и машин (структурной надежности) на процессы ИА дал результаты, которые по мнению самих авторов далеки от

жизни [37].

В отличие от указанных источников в настоящей работе рассматриваются не только закрытые, но и открытые ИС, частным случаем которых являются ИС общего пользования (ИСОП), в том числе современные информационные системы, насчитывающие десятки миллионов пользователей, примером которых является АИС «Налог-2» ФНС. Разработан концептуальный многоуровневый подход к анализу рисков безопасности информации в процессах аутентификации и исследованию достоверности и надежности процессов ИА.

В существующем нормативно – правовом поле требуется создать механизмы надежного доступа к информационным ресурсам государственных ИС (ГИС) с заданным уровнем доверия к аутентификации пользователей. Уровни доверия к результатам ИА субъектов доступа необходимо определить на основе анализа рисков с учетом технологических решений и выполнения требований ИБ. В отсутствие таких решений в ГИС становится проблематичной организация безопасного межведомственного взаимодействия и поддержка юридически значимого электронного документооборота, а также предоставление защищенного доступа к удаленным сервисам, в том числе, «облачным». Для разработки рекомендаций и технических требований в существующем правовом поле необходимо проведение комплексных аналитических исследований с последующим анализом полученных результатов, их сравнением с экспериментальными данным и накопленным опытом построения и эксплуатации систем ИА. Проведение теоретических исследований процессов ИА без синтеза новых подходов (методик) и создания математических моделей представляется затруднительным. Следовательно, главной целью настоящей работы является разработка теоретических основ методологии, включающих в себя модели и методы анализа ИА участников УЭВ.

Всеми указанными выше обстоятельствами определяется **актуальность** темы диссертационного исследования, в котором решается проблема создания теоретической и методологической базы построения иерархии доверия к ре-

зультатам идентификации и аутентификации субъектов электронного взаимодействия.

Научная проблема состоит в необходимости создания теоретических положений и формировании иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

Практическая сторона данной проблемы заключается в том, что несмотря на интенсивный рост количества информационных систем и зарегистрированных в них объектов и субъектов, а также возрастающие требования по повышению доверия к электронным формам взаимодействия государства, личности и бизнеса, применяемые сегодня оценки доверия к результатам идентификации и аутентификации не позволяют использовать развитый арсенал теоретических подходов, математических моделей и методик для комплексного анализа доверия к результатам идентификации и аутентификации на научной основе. Это сдерживает внедрение научно обоснованных подходов к проектированию и государственному регулированию в части безопасности и обеспечения доверия к результатам работы систем идентификации и аутентификации, входящих составной частью во все информационных системы независимо от их состава и назначения. Таким образом, имеется сложная и важная практическая проблема, суть которой состоит в том, что при высокой практической потребности сегодня отсутствуют концепция и развитая методология иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

В теоретической части данная проблема охватывает несколько подлежащих разрешению противоречий.

Первое противоречие заключается в том, что имеющиеся исследования идентификации и аутентификации касались отдельных аспектов или процессов, в то время как для оценки доверия к результатам идентификации и аутентификации необходим комплексный анализ, включающий в себя анализ рисков нарушения требований безопасности информации, функциональной

надежности выполнения основных процессов и соответствия системы идентификации и аутентификации требованиям доступности, конфиденциальности и целостности обрабатываемой идентификационной и аутентификационной информации пользователей информационной системы.

Второе противоречие связано с тем, что для развития теоретических положений и разработки концепции повышения доверия к результатам ИА связано с формализацией описания предметной области, однако для многих факторов и условий, характерных и существенных в области защиты информации для систем идентификации и аутентификации, таких как множество угроз безопасности информации и процессы их реализации, процедуры принятия решений на применение мер и средств защиты, наличие характеристик нечисловой природы, сегодня не имеется формальных моделей и пути разработки таких моделей не сформированы. Так, если протоколы аутентификации формализованы и исследованы, то для процессов идентификации пока не существует общепринятых моделей и методов исследования. Разнородность, разномасштабность и большое количество учитываемых факторов затрудняет построение адекватных математических моделей и переход к количественным методам их учета. В результате методы формального описания некоторых из упомянутых выше факторов при исследовании идентификации и аутентификации сегодня ориентированы на расчеты только частных показателей, а системные аспекты их сопряжения не разработаны.

Третье противоречие заключается в том, что существующие подходы к оценке доверия только формируются и не находятся в стадии промышленного применения. Постановка задачи по определению допустимых и остаточных рисков и соответствующих им уровней доверия (assurance levels) и пути ее решения для многих актуальных систем и процессов пока не определены. Применительно к исследованию доверия к результатам работы системы идентификации и аутентификации и выполняемых в процессе ее работы процедур методологическая часть пока не разработана. Это обусловливает необходимость изыскания новых подходов к разработке такой методологии.

Четвертое противоречие заключается в том, что при исследовании доверия к результатам идентификации и аутентификации необходимо моделировать однократные и регулярно повторяющиеся, последовательные и параллельные процессы, влияющие на защищенность информации, учитывать случайный характер многих из них (например, процессов, влияющих на надежность работы системы и реализацию угроз безопасности информации), что не позволяет в большинстве случаев непосредственно применять традиционные методы математического моделирования. Именно по этой причине до сих пор такие модели практически не разрабатывались.

Таким образом, неразрешенность указанных противоречий, непроработанность путей их разрешения обусловливает наличие теоретической проблемы.

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

Предметом исследования являются модели, методы и алгоритмы оценки доверия к результатам идентификации и аутентификации субъектов доступа.

Целью исследования является создание методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

Разработка и модернизация существующих методов, моделей и алгоритмов оценки доверия к идентификации и аутентификации позволят сформировать теоретическое обоснование для разработки стандартов, выработки рекомендаций и требований к процессам и системам идентификации и аутентификации субъектов доступа в существующих и проектируемых ИС.

Для достижения поставленной цели необходимо решение следующих **задач**:

1. Анализ нормативно-правовых документов, рекомендаций, стандартов и ре-

зультатов научных работ для выработки концептуальных подходов к исследованию надёжности и достоверности результатов идентификации и аутентификации субъектов доступа и безопасности обрабатываемой при этом информации.

2. Разработка концепции формирования иерархии уровней доверия к результатам идентификации и аутентификации субъектов электронного взаимодействия.

3. Создание методологии оценок достоверности, надежности и безопасности идентификации на основе анализа рисков, позволяющей формировать уровни доверия к результатам первичной идентификации субъектов доступа информационных систем на основе использования разработанных и известных методов и моделей идентификации.

4. Разработка критериев доверия к результатам первичной идентификации для формирования на их основе подходов к оценке доверия к результатам идентификации субъектов доступа.

5. Формирование комплекса моделей и методов оценки рисков при анализе безопасности аутентификационной информации и функциональной надежности процесса аутентификации; разработка методики оценки рисков, учитывающей участников, порядок и состав основных процедур аутентификации.

6. Создание новых и модернизированных моделей и методов оценки надежности аутентификации субъектов доступа к информационным ресурсам, а также разработка с их использованием критериев доверия и алгоритма оценки доверия к результатам работы систем идентификации и аутентификации на основе анализа безопасности идентификационной и аутентификационной информации, достоверности результатов и надежности работы системы идентификации и аутентификации, позволяющих в совокупности с решением задач пунктов 3-5 создать методологию формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа в информационных системах.

7. Апробация теоретической и методологической базы формирования иерархии уровней доверия к результатам идентификации и аутентификации при решении практических задач:

1) создания первого национального стандарта по идентификации и аутентификации субъектов доступа, описывающего основы и единые правила создания систем идентификации и аутентификации и проекта второго национального стандарта, формирующего уровни доверия к результатам цифровой идентификации субъектов доступа;

2) применение методов, моделей и способов оценки доверия к результатам идентификации и аутентификации при решении практических задач построения систем идентификации и аутентификации, разработки новых систем защиты информации, экспертизы нормативной документации;

3) разработка способов достижения заданного уровня доверия к результатам идентификации и аутентификации для типовых информационных систем;

4) оценка роли идентификации и аутентификации, а также других сервисов безопасности на основе инфраструктуры открытых ключей, в построения единого пространства доверия с целью создания, передачи, обработки и хранения электронных документов, обладающих юридической силой;

5) разработка способа защиты персональных данных и управления доступом к ним, в том числе при переходе к облачным вычислениям.

Методы исследования. Для решения поставленных задач развития методологии построения иерархии к уровням доверия и, в конечном счете, повышения доверия к результатам идентификации и аутентификации субъектов доступа применялись методы системного анализа, теории множеств, случайных процессов, надежности, вероятностей, оценки рисков, а также методы структурно-функционального анализа, теории управления, защиты информации и методы исследования систем массового обслуживания.

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

- разработана методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа при электронном взаимодействии на основе моделирования основных процессов и систем идентификации и аутентификации, отличающиеся от известных учетом анализа рисков и специфики процессов идентификации и аутентификации, в том числе для больших информационных систем с числом пользователей порядка 10^6 с учетом перехода к облачным вычислениям;
- предложен подход многоуровневой оценки рисков и исследования надёжности на основе разбиения процесса аутентификации на ряд последовательных процедур, что позволило определять вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых ИС;
- проведена классификация процессов и систем идентификации и аутентификации, 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, что обеспечило возможность многоуровневого анализа рисков процессов и транзакций в системах идентификации и аутентификации, позволяющего проводить оценки рисков с заданным уровнем детализации;
- разработаны математические модели и методики оценки функциональной надёжности процессов идентификации и аутентификации, что позволяет проводить оценку надёжности первичной идентификации и аутентификации участников удалённого электронного взаимодействия;
- предложена методика хранения и обработки информации ограниченного доступа при переходе к облачным вычислениям с применением строгой аутентификации для доступа к защищенной конфиденциальной информации при переходе к облачным вычислениям, позволяющая минимизировать риски НСД к защищаемой информации за счет распределения ключей шифрования данных методом их зашифровывания на открытых ключах пользователей

внутри защищенного периметра организации.

Научная ценность диссертации состоит в развитии теории и методологии обеспечения информационной безопасности в части создания новых и модернизации существующих моделей, методов и алгоритмов оценки доверия с целью построения иерархии доверия к результатам идентификации и аутентификации участников уделённого электронного взаимодействия с учётом применяемых и перспективных технологий, учитывающих риски нарушения безопасности информации.

Практическая ценность полученных результатов заключается в том, что в диссертации решена важная проблема разработки методологии формирования иерархии уровней доверия и оценки доверия к результатам идентификации и аутентификации субъектов доступа, позволяющая использовать ее в практической деятельности по построению и модернизации систем управления доступом современных информационных систем, что подтверждается актами о внедрении в практическую работу. Применение положений данной диссертационной работы позволяет сократить сроки проведения оценок безопасности, функциональной надежности и достоверности результатов идентификации и аутентификации субъектов доступа на этапах проектирования и эксплуатации информационных систем различного назначения, как минимум, на 25%.

Прикладная направленность диссертационной работы проявилась в разработке национальных стандартов, научно-технических отчетов, конкретных технических решениях, используемых в Министерстве обороны и ряде ведомств. Так, результаты диссертационного исследования использовались при разработке ГОСТ Р 58833 «Идентификации и аутентификация. Общие положения», проекта ГОСТ Р XXXXX «Идентификации и аутентификация. Уровни доверия к результатам идентификации», создании промышленных систем идентификации и аутентификации, а также их технического сопровождения в Пенсионном Фонде Российской Федерации, Федеральном агентстве по

рыболовству, Федеральной таможенной службе Российской Федерации, Федеральном государственном учреждении «Центр системы мониторинга рыболовства и связи», ОАО «Ростелеком», ОАО «Русал», ЦКБ Управления делами Президента РФ, Комитетах по информатизации Санкт-Петербурга и Ленинградской области, МИАЦ РАМН, НТЦ «Фобос-НТ», в ПАО «Газпромбанк» и КБ «Возрождение», что подтверждено соответствующими актами об использовании результатов диссертационного исследования.

Реализация результатов работы. Разработанные в диссертации модели, методы и алгоритмы использовались при выполнении НИОКР и НИР в:

– Министерстве коммуникаций и связи РФ, государственный контракт № 012/155 от 12 декабря 2011 г.,

– Таможенных органах РФ (9 государственных контрактов 2007- 2011 гг.),

– Пенсионном фонде РФ (государственные контракты №14-141-D от 18 мая 2009 г., №23-158-Д от 04 мая 2010 г. и др.- всего 9 госконтрактов),

– Федеральном агентстве по рыболовству контракт №97-01/2011 от 31 мая 2011 г., Центре системы мониторинга рыболовства и связи, государственные контракты №41-Ю от 24 ноября 2009 г. и № 44-10 от 08 декабря 2009 г.,

– АТЭС - в проектах «Руководство АТЭС по реализации принципов "прозрачности" в электронной коммерции» 2003-2005 гг., проекте АТЭС «Разработка руководства АТЭС по электронной коммерции" ECSG 06/2008T и CTI 53/2009T/ECSG,

– Министерстве образования и науки Российской Федерации, шифр работы (темы) 14.577.21.0172 от 01.11.2015 г.;

– Министерстве обороны, договор № OS – 1216909 на поставку от 26 сентября 2016 г.;

– Федеральной службе по техническому и экспортному контролю при разработке первого национального стандарта по идентификации и аутентификации ГОСТ Р 58833 «Идентификация и аутентификация. Общие положения»

и нормативной базы обеспечения информационной безопасности, шифр работы "Момент-16"-2016 г., шифр работы "Идентификация"-2018 г.;

– при проектировании и производстве средств защиты информации JaCarta, JaCarta SF/ГОСТ, Secret Disk Enterprise, JaCarta Management System, средств криптографической защиты информации «КриптоБД» и «Криптотокен-2»;

– в учебном процессе МГТУ им. Н.Э. Баумана, Нижегородского государственного университета им. Н.И. Лобачевского и Томского государственного университета систем управления и радиоэлектроники.

Достоверность и обоснованность научных положений, результатов и основных выводов работы обеспечивается многосторонним анализом современного состояния исследований в предметной области, подтверждением корректности предложенных моделей и алгоритмов, согласованностью полученных результатов с известными теоретическими и экспериментальными данными, апробацией основных положений диссертации 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 систем идентификации и аутентификации в организациях различного подчинения.

Положения, выносимые на защиту:

1. методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа на основе моделирования основных процессов и систем идентификации и аутентификации, отличающаяся от известных учетом анализа рисков и специфики процессов аутентификации, в том числе при переходе к облачным вычислениям и большим информационным системам, насчитывающим миллионы пользователей (пункт 1 Паспорта специальности);
2. методика многоуровневой оценки рисков и исследования надёжности на основе разбиения процессов идентификации и аутентификации на ряд по-

следовательных процедур, что позволило определять вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых ИС (пункт 7 Паспорта специальности);

3. классификация процессов и систем идентификации и аутентификации, 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, что обеспечило возможность разработки критериев риска для 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 идентификации и аутентификации, позволяющего проводить оценки рисков с заданным уровнем детализации (пункт 11 Паспорта специальности);
4. математические модели и методики оценки функциональной надёжности процессов идентификации и аутентификации, позволяющие проводить оценку надёжности первичной идентификации и аутентификации участников удалённого электронного взаимодействия (пункт 2 Паспорта специальности);
5. методика хранения и обработки информации ограниченного доступа при переходе к облачным вычислениям с применением строгой аутентификации для доступа к защищенной конфиденциальной информации, позволяющая минимизировать риски НСД к защищаемой информации за счет распределения ключей шифрования данных методом их зашифровывания на открытых ключах пользователей внутри защищенного периметра организации (пункт 13 Паспорта специальности).

Апробация результатов работы. Результаты исследования докладывались на научно-технических конференциях «Методы и технические средства

обеспечения информационной безопасности» г. Санкт-Петербург в 2003-2019 гг., научно-практических конференциях «Комплексная защита информации», 2005-2013 гг., ежегодных научных конференциях по радиофизике. Н. Новгород, ННГУ им. Н. И. Лобачевского – 2012 и 2013 гг., международных конференциях «Рускрипто» в 2004-2019 гг., международных конференциях «Инфофорум» - 24 доклада в 2005-2016 гг., международных конференциях "PKI-форум" (СПб) в 2003-2019 гг., Уральском Форуме «Информационная безопасность банков» в 2009-2020 гг., Расширенных заседаниях Совета по обеспечению ИБ таможенных органов РФ в 2006-2015 гг., региональном семинаре Международного союза электросвязи (ITU) в 2013 г., конференциях Международной академии связи в 2013-2019 гг., Международных научно-практических конференциях «ГЛОНАСС-регионам», г.Орел в 2014-2015 гг., Европейском международном форуме по проблемам электронной подписи. EFPE Польша. Медзыздрое. 4-6 июня 2014 г., Совещании-семинаре работников центрального аппарата и территориальных органов ФНС России по вопросу информационной безопасности в 2007-2016 гг., VII Международном IT-форуме с участием стран БРИКС и ШОС. Ханты-Мансийск, 6-7 июля 2015 г.; всего было сделано более 300 докладов по теме диссертационной работы на международных, всероссийских и отраслевых мероприятиях по вопросам защиты информации.

Внедрение. Результаты работы внедрены в Пенсионном фонде РФ, Федеральной таможенной службе РФ, ГНИВЦ ФНС России, ЗАО «РУСАЛ Глобал Менеджмент Б.В.», ООО «Удостоверяющий Центр Сибири», ОАО «Ростелеком», ФБГУ ЦСМС Росрыболовства, ЦКБ Управления делами Президента РФ, МИАЦ РАМН, ООО НТЦ «Фобос-НТ», Газпромбанке, КБ «Возрождение», учебном процессе Томского государственного университета систем управления и радиоэлектроники, Нижегородского государственного университета им. Н.И. Лобачевского, МГТУ им. Н.Э. Баумана.

Соответствие паспорту специальности. Цель диссертационного ис-

следования соответствует формуле специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность", состоящей в исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения, а также в разработке новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности.

Работа соответствует перечисленным в паспорте специальности областям исследования 1, 2, 7, 11, 13. В частности, в диссертации развивается общая теория и методология обеспечения информационной безопасности и защиты информации в части исследования процессов аутентификации и построения индикаторов доверия к результатам идентификации и аутентификации пользователей информационных систем (пункт 1 Паспорта специальности). Разработана методология и определен минимально-достаточный набор сервисов безопасности для обеспечения юридической силы электронным документам в системах электронного документооборота (пункт 4). Для формирования уровней доверия и построения иерархии доверия к результатам идентификации и аутентификации впервые применены методы анализа рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах (пункт 7). В целом работа посвящена совершенствованию моделей противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (пункт 8) в части пункта 11 "Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа". Разработанная в диссертации методология формирования иерархии доверия к результатам идентификации и аутентификации при удаленном электронном взаимодействии, позволившая сформулировать требования безопасности и надежности к системам идентификации и аутентификации, соответствует пункту 12 "Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы

управления". Разработанные в диссертации модели для исследования безопасности и надежности идентификации и аутентификации соответствуют п.13 "Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности".

Личный вклад автора и публикации по теме диссертационной работы. Формулирование темы исследования и постановка задач на изучение отдельных аспектов идентификации и аутентификации проводилась автором самостоятельно. Автор данной диссертационной работы более 18 лет занимается исключительно проблемами исследования идентификации и аутентификации. За это время по теме диссертации самостоятельно и в соавторстве опубликовано 3 монографии, 3 учебных пособия, более 300 научных статей во всероссийских и профильных журналах, 60 статей (из них 15 – в соавторстве) опубликовано в изданиях, рекомендованных ВАК России, две работы опубликованы в изданиях Web of Science, имеются патенты на изобретение №2523174 от 22.05.2014 г. и №2635927 от 05.09.2016 г.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы. Общий объем работы составляет 334 стр. машинописного текста, 44 рисунков и 40 таблиц. Список литературы содержит 244 наименования.

1 Современное состояние методологического обеспечения процессов идентификации и аутентификации субъектов доступа

1.1 Анализ международных и национальных стандартов, нормативных правовых актов и методических документов по защите информации, регламентирующих основные аспекты идентификации и аутентификации субъектов доступа

Основы безопасности взаимодействия открытых систем, в частности, при управлении доступом пользователей, заложены в работах, достаточно полно изложенных в [44], а также в работах специалистов известных научно-исследовательских институтов National Institute of Standards and Technology (NIST, США) [45] и British Standards Institution (BSI, Великобритания) [46].

История разработки стандартов по идентификации и аутентификации тесно связана с историей развития информационных технологий и особенно – технологий удаленного электронного взаимодействия. Интенсивный рост открытых систем массового электронного обслуживания (e-Banking, e-Commerce, e-Government, e-Health и других составляющих информатизации общества) потребовал создания сервисов безопасности, обеспечивающих приемлемый уровень рисков использования информационных систем. Одним из самых сложных, но необходимых элементов информационной системы является сервис аутентификации – сервис подтверждения подлинности предъявленных заявителем идентификаторов и доказательства принадлежности конкретному субъекту. Данный факт нашел отражение в системе международных стандартов. Нормативных документов по аутентификации в количественном отношении гораздо больше, чем по идентификации, а история их намного богаче и тянется уже более 30 лет.

Анализ хронологии развития стандартов по идентификации и аутентификации с учетом их содержания показал следующие тенденции (Рисунок 1.1):

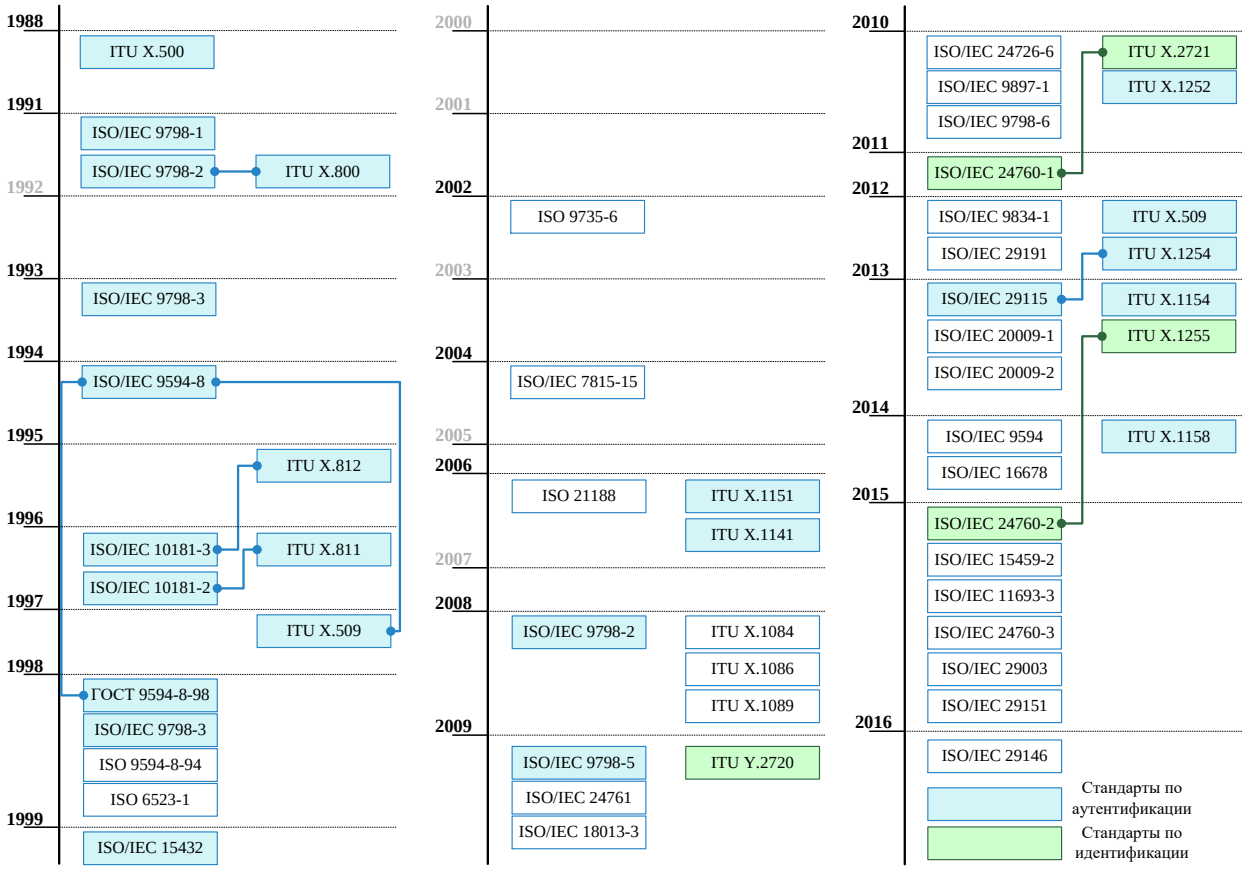

Рисунок 1.1 – Хронология развития международных стандартов по идентификации и аутентификации

– 1988 г. Появление первой версии рекомендаций X.509 Международного союза электросвязи. Необходимо отметить, что с первой версии этого документа ITU-T Rec.X.509 (08/1988) [47] по третью ITU-T Rec.X.509 (08/1997) [48], изданную в 1997 г., рекомендация называлась «Директория: основы аутентификации»; в последних версиях, например, 2012 и 2015 годов, в названии остается «Директория: основы PKI и атрибуты сертификатов». Приводятся два вида аутентификации: простая, с применением в качестве аутентификатора пароля, и строгая, с применением криптографических функций;

– 1991 г. Одним из первых стандартов по аутентификации пользователей открытых систем, разработанных ИСО, также является стандарт «Общая модель механизмов аутентификации объектов» [49]. Почти одновременно с ним был опубликован стандарт по архитектуре безопасности для взаимосвязи

открытых систем, технически согласованный с рекомендацией ITU Rec.X.800 [50], в котором подробно рассмотрены базовые услуги безопасности, в первую очередь «аутентификация», на уровнях эталонной модели взаимодействия открытых систем (OSI). Заметим, что стандарт ISO/IEC 9798-1:1991, первоначально состоящий из трех частей (первые части вышли в 1991 г., третья часть – в 1993 г.), переиздавался несколько раз. Например, часть 2 впервые была опубликована в 1991 г., второй раз – в 1996 г., последний раз - в 2018 г.;

– 1994 г. Существенное влияние на создание существующей системы международных стандартов по идентификации и аутентификации оказал стандарт ISO/IEC 9594-8 [51]. Восьмая часть данного стандарта явилась развитием [47], подробно описывающим два вида аутентификации: простую (парольную) и строгую, на основе применения открытого и закрытого ключей. Закрытый ключ, согласно третьей части стандарта [52], служит в качестве аутентификатора, и его генерация может осуществляться внутри смарт-карты пользователем, удостоверяющим центром или доверенной третьей стороной. Через четыре года данный стандарт был переведен на русский язык и вошел в нормативную базу Российской Федерации, до сих пор этот стандарт [4] является единственным по идентификации и аутентификации пользователей;

– 1996 г. К числу первых стандартов по обеспечению безопасности процессов аутентификации, тесно связанных с построением систем обеспечения доверия при удаленном электронном взаимодействии [47, 49, 50, 52], относится и ISO/IEC 10181-2 [53] - текст стандарта полностью идентичен выпущенным в том же году рекомендациям ITU-T Rec.X.811 [54]. Данные рекомендации опирались на стандарт Международного союза электросвязи по общей безопасности взаимодействия открытых систем [55];

– 1997 г. Вышла в свет полностью пересмотренная версия стандарта ITU-T Rec.X.509 [48], сопряженного (практически идентичного, отличие только в описании технических подробностей в стандарте МСЭ) рассмотренной выше восьмой части стандарта ISO/IEC 9594-8-94. Оба связанных стандарта называются «Основы аутентификации». Описаны и специфицированы

простая и строгая аутентификация с применением асимметричной криптографии. Представлены основные сервисы безопасности на базе инфраструктуры открытых ключей: аутентификация источника данных и взаимная аутентификация, управление доступом, конфиденциальность данных, целостность и неотказуемость. Также определены основные механизмы, применяющиеся в указанных сервисах: простая и строгая аутентификация, шифрование и целостность данных, электронная подпись.

– 1998 г. Опубликована переработанная[1] третья часть стандарта ISO/IEC 9798 [52], посвящённая применению криптографических алгоритмов цифровой подписи для аутентификации объектов и субъектов. Стандарт включил в себя 4 механизма аутентификации: два – для односторонней аутентификации объекта и два – для взаимной аутентификации. Рассмотрены возможности применения следующих криптографических алгоритмов: симметричных алгоритмов, цифровой подписи, криптографической функции проверки и механизма с нулевым знанием.

– 2009 г. Опубликован стандарт ITU-T Rec.Y.2720 [56], обобщающий наработки многих рекомендаций, в том числе ITU-T Rec.X.1151, ITU-T Rec.X.1141 для управления идентификацией объектов и субъектов в сетях нового поколения. В системе ISO/IEC первая часть аналогичного назначения стандарта появится лишь в 2011 г. (ISO/IEC 24760-1 [57]). Положения стандарта ИСО рассматривают те же категории, что и стандарт ITU-T Rec.Y.2721 (2010) [58].

– 2013 г. Применение методов управления рисками к задачам идентификации и аутентификации, а также появление ряда работ NIST способствовали появлению первого стандарта ИСО по уровням доверия к аутентификации - ISO/IEC 29115 [59], гармонизированного с ITU-T Rec.X.1254 [60].

– 2015 г. Опубликован стандарт ISO/IEC 24760-2 [61], соответствую-

[1] С момента появления первой версии стандарта ISO/IEC 9798 прошло 5 лет и за это время обновлены все три части.

щий рекомендациям ITU-T Rec.X.1255 (09/2013) [62] по управлению идентификацией. Основные положения этих стандартов опираются на стандарты ISO/IEC 24760-1:2011 и ISO/IEC 29115:2013 [63].

Работа по развитию и обновлению стандартов продолжается. За последние 5 лет число ежегодно публикуемых стандартов по идентификации и аутентификации существенно выросло, при этом акцент от общих принципов решения задач идентификации и аутентификации смещается в сторону прикладного применения этих процессов в различных отраслях (медицина, финансы, транспорт и т.д.).

Анализ количества стандартов ИСО, непосредственно связанных с развитием технологий идентификации и аутентификации, по годам издания показал (Рисунок 1.1), что, если в период с 1996 г. по 2008 г. в год выпускалось не более одного стандарта, то в период с 2009 г. по 2015 г. издавалось по 2-3 стандарта. При этом количество стандартов, связанных с цифровой идентификацией и аутентификацией в различных сферах жизнедеятельности (финансы, транспорт, здравоохранение и т.д.) росло в арифметической прогрессии. Например, при контекстном запросе на сайте ИСО (http://www.iso.org/iso/home.htm) по термину «authentication» за последние 10 лет в результатах приводится 66 стандартов. Стандарты менялись не только количественно, но и качественно. Так, если в ИСО/МЭК 10181 – 2:1996 [53] были заложены теоретические основы (участники обмена, виды передаваемой аутентификационной информации, модели угроз и т.д.) всех видов аутентификации, то уже в ИСО/МЭК 9798-3:1998 [52] были описаны два вида аутентификации: простая (с использованием в качестве аутентификатора пароля) и строгая (в качестве аутентификатора применяется закрытый ключ цифровой подписи, соответствующий сертификату доступа).

Установлено, что при разработке стандартов соблюдалась их преемственность и идентичность (Таблица 1.1). Например, единственный стандарт по аутентификации ГОСТ Р ИСО/МЭК 9594-8-98 [4], является переводом

стандарта ISO/IEC 9594-8:1994 [**Ошибка! Закладка не определена.**] и одновременно частью связанного с ним стандарта ITU Rec.X.509 [48].

К наиболее важными с точки зрения регламентации процедур идентификации и аутентификации следует отнести (Таблица 1.1, связанные между собой стандарты расположены в одной строке):

– стандарты, определяющие теоретические основы, базовую архитектуру и терминологию в области идентификации и аутентификации;

– стандарты, определяющие вопросы, связанные с доверием к идентификации и аутентификации;

– стандарты, регламентирующие процессы управления идентификацией и аутентификацией.

Таблица 1.1 – Соответствие стандартов МСЭ и ИСО по идентификации и аутентификации

ITU-T x.800 (1991) Методы защиты. Аутентификация объектов. Архитектура безопасности для взаимодействия открытых систем	ISO/IEC 7498-2:1989 Аутентификация объектов. Архитектура безопасности для взаимодействия открытых систем
ITU-T x.509 (1997) Взаимодействие открытых систем. Справочник сертификатов. Основы аутентификации	ISO/IEC 9594-8:1998 Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации
ITU-T x.811 (1995) Теоретические основы аутентификации	ISO/IEC 10181-2:1996 Основы безопасности для открытых систем. Часть 2. Основы аутентификации
ITU-T x.1252 (2010) Базовые термины и определения в области управления идентификацией	ISO/IEC 24760-1:2011 Руководство по управлению идентификацией. Часть 1. Терминология и понятия
ITU-T x.1254 (2012) Структура гарантии аутентификации объекта	ISO/IEC 29115:2013 Структура доверия к аутентификации сущности
ITU-T x.1255 (2013) Структура обнаружения информации по управлению идентификацией	ISO/IEC 24760-1:2015 Общие основы управления идентификацией. Часть 2. Эталонная архитектура и требования

Начиная с 2009 г. (появление стандарта ISO/IEC 9798-5:2009 [64]), поня-

тия «идентификация» и «аутентификация» стали весьма близкими. Действительно, доверие к результатам аутентификации [61] существенно зависит от корректности проведения первичной идентификации. Благодаря этому, опубликованные в последние годы стандарты все чаще оперируют более общим понятием «идентификация».

При этом в отличие от стандартов по аутентификации, имеющих почти сорокалетнюю историю, развитые стандарты по идентификации появились относительно недавно (так, стандарт ITU-T Y.2720 принят в 2009 г., остальные еще позже). Возможной причиной возникновения такой ситуации явилось отсутствие адекватных математических моделей идентификации, необходимых для решения задач в широком диапазоне информационных систем, которые нередко насчитывают десятки миллионов и более пользователей, а также вопросы оценки надёжности идентификации объектов в таких системах [1].

В стандартах ITU-T Rec.X.1254 (09/2012) и ISO/IEC 29115:2013 на основе анализа рисков предложено 4 уровня доверия к результатам идентификации (Таблица 1.2).

Таблица 1.2 – Уровни доверия к результатам идентификации

Уровень	Описание	Задача	Средства контроля
Уровень 1 - низкий	Слабая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста	Собственное утверждение или заявление
Уровень 2 - средний	Определенная степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, и объект, владеющий идентичностью, реально существует	Проверка подлинности идентичности путем использования информации из авторитетного источника
Уровень 3 - высокий	Высокая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность использу-	Проверка подлинности идентичности путем использования информации из авторитетного источника + верификация идентичности

		ется в других контекстах	
Уровень 4 - очень высокий	Очень высокая степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования информации из достоверного источника + верификация идентичности + личное присутствие объекта

Рассмотрены механизмы аутентификации, определенные в основополагающих стандартах ISO/IEC 9594-8:1994 и ISO/IEC 29115:2013 [65] в сравнении с часто упоминаемым стандартом FIDO [66] (Рисунок 1.2)

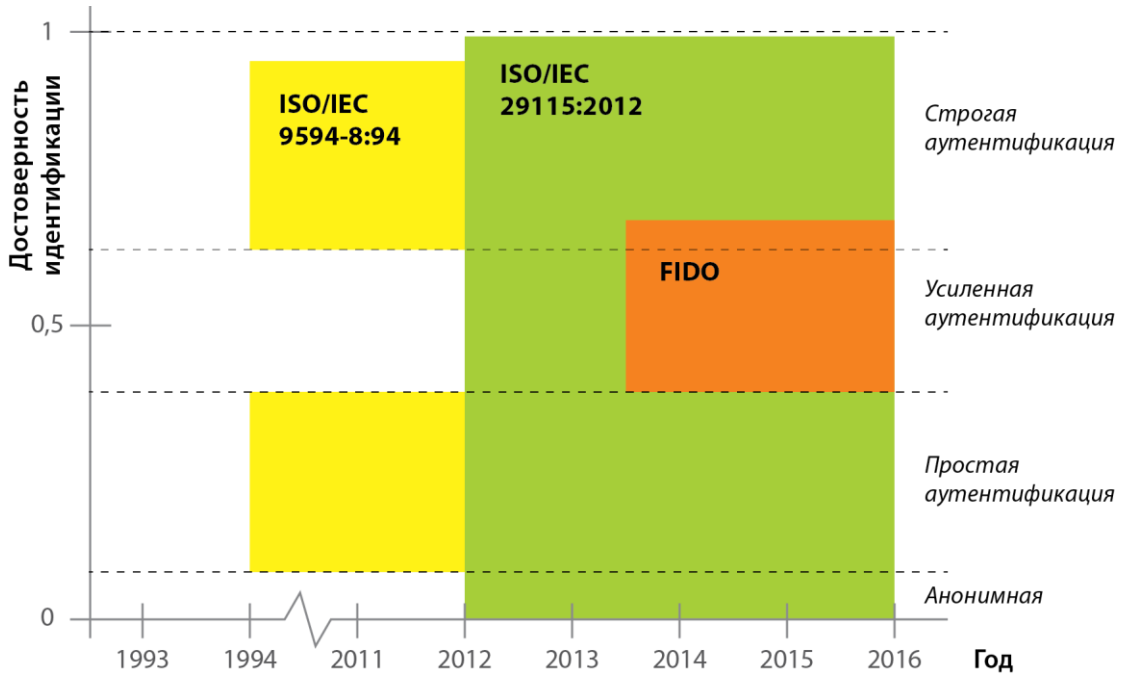

Рисунок 1.2 – Области охвата стандартами уровней достоверности аутентификации

Видно, что в отличие от ISO/IEC 9594-8:1994, стандарт ISO/IEC 29115:2013 охватывает все уровни достоверности идентификации. В то же время стандарт [66], хоть и оперирует термином «строгая аутентификация», зачастую подменяет это понятие двухфакторной аутентификацией, которая,

как показано в [67], может и не являться строгой. Так, в качестве двух факторов в [65] рекомендуется, например, использовать фактор знания и одну из (или сразу две) биометрических характеристик пользователя: отпечаток пальца, голос и т.п., или другую пару: фактор владения и поведенческую характеристику. Для специалиста ясно, что все биометрические характеристики являются идентифицирующей информацией, то есть информацией без подтверждения, и не могут напрямую рассматриваться в качестве аутентифицирующей информации. Любая биометрическая характеристика может служить лишь подтверждением, например, фактора владения.

В первой части ISO/IEC 24760 представлены термины и определения. Вторая часть ISO/IEC 24760-2 содержит рекомендации по реализации системы менеджмента идентификационных атрибутов, а также определяет требования по реализации общих принципов менеджмента. Положения второй части ISO/IEC 24760-2 применимы к любой информационной системе, в которой обрабатывается или хранится информация идентификационного характера. Данная часть предоставляет базу для реализации других международных стандартов, связанных с обработкой идентификационной информации, и содержит два основных раздела: «Эталонная архитектура» и «Требования к управлению ИИ». Третья часть стандарта ISO/IEC 24760-3 содержит руководство в части менеджмента идентификационной информации и снижения рисков в отношении идентификационной информации. Отдельный раздел стандарта посвящен мероприятиям по реализации адекватных мер, направленных на снижение рисков и устранение последствий утечек идентификационной информации, повреждения и потери доступности в рамках ее сбора, хранения, использования, передачи и удаления. В стандарте содержится краткий перечень политик доступа к идентификационной информации, которые раскрывают требование о необходимости ведения процедур ее безопасного менеджмента.

В рекомендациях ITU-T Y.2720 «Global information infrastructure. Internet protocol aspects and next-generation networks. NGN identity management framework» представлены основы менеджмента идентификационных атрибутов в

сетях нового поколения. Главной целью этого документа является описание структурного подхода к проектированию, определению и реализации решений в области менеджмента идентификационных атрибутов и содействие функциональной совместимости в гетерогенной среде.

Сопоставление с эталонной архитектурой менеджмента идентификационных атрибутов, определенной в ISO/IEC 24760, позволяет отметить, что в последнем стандарте представление об инфраструктуре системы менеджмента идентификационной информации получило принципиальное развитие: если в Y.2720 инфраструктура определялась преимущественно в терминах функций и возможностей, то в ISO/IEC 24760, она являет собой взаимоувязанную совокупность действующих субъектов, потоков информации, сервисов, хранилища, уровней доверия и т. п.

Группа стандартов под общим индексом ISO/IEC 9798 «Information technology – Security techniques – Entity authentication» представляет пользователям набор семейств протоколов и предназначенных для аутентификации сущности (субъектов и объектов). ISO/IEC 9798 состоит из шести частей. В каждой из частей стандарта рассмотрены механизмы односторонней и взаимной аутентификации, предлагающих различную строгость их реализации через введение соответствующего количества итераций информационного обмена (именуемых «проходами») соответствующими протокольными блоками данных, сформированными на основе применения того или иного криптографического алгоритма или примитива.

Реализация механизмов строгой аутентификации с применением:

– симметричных криптографических алгоритмов. В стандарте ISO/IEC 9798-2 рассмотрено 6 механизмов и до 4-х проходов протокольного обмена).

– электронной подписи и инфраструктуры открытых ключей, В стандарте ISO/IEC 9798-3 рассмотрено 10 механизмов и до 7-и проходов протокольного обмена.

– обеспечивающих контрольных функций криптографических алгоритмов (надежные отметки времен, надежные датчики случайных чисел). В стандарте ISO/IEC 9798-4 рассмотрено 4 механизма и до 3-х проходов протокольного обмена.

– первоначальных «нулевых знаний». В стандарте ISO/IEC 9798-5 рассмотрено 6 механизмов, базирующихся на различных криптографических алгоритмах и алгебраических операциях для аутентификации устройств, использующих информационные технологии

В стандарте ISO/IEC 9798-6 рассмотрено 8 механизмов и множественный взаимный обмен.

Рассмотрим первые три части международного стандарта ISO/IEC 9798 как в наибольшей мере относящиеся к исследуемой в диссертации области.

Первая часть стандарта ISO/IEC 9798-1 определяет модель аутентификации, общие требования и ограничения для механизмов аутентификации сущности, использующих средства защиты. Эти механизмы используются для подтверждения того, что сущность является тем, что она о себе заявляет.

В соответствии с обобщенной моделью (Рисунок 1.3) совсем не требуется, чтобы любой механизм аутентификации содержал все показанные сущности и реализовывал обмен данными во всех указанных направлениях.

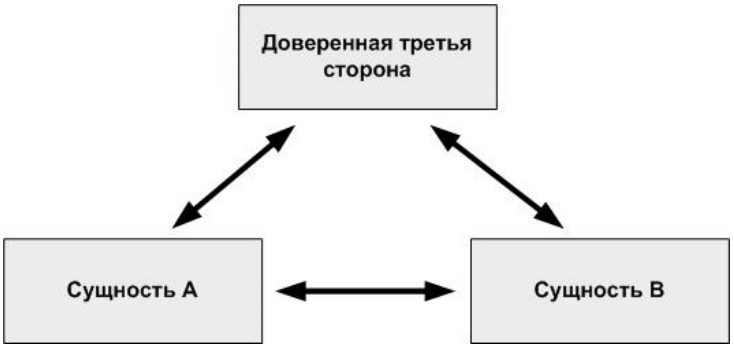

Рисунок 1.3 – Обобщенная модель аутентификации

Применительно к механизмам аутентификации, определенным в остальных частях ISO/IEC 9798, действуют следующие положения:

– для односторонней аутентификации: сущность А рассматривается в

качестве заявителя, а сущность В – в качестве регистратора и доверяющей стороны (контролера);

– для взаимной аутентификации: сущности А и В выступают в роли как заявителя, так и контролера.

В рамках процессов аутентификации сущности генерируют и обмениваются формализованными сообщениями – токенами. Информационный обмен включает передачу, по меньшей мере, одного токена для односторонней аутентификации и двух – для взаимной. При этом может потребоваться дополнительная передача для запроса о начале обмена, а также могут потребоваться дополнительные обмены данными, если в процесс аутентификации вовлекается доверенная третья сторона. Детальное описание этих механизмов и содержание операций информационного обмена в рамках процесса аутентификации приводится в последующих частях ISO/IEC 9798.

Вторая часть стандарта ISO/IEC 9798-2 определяет механизмы аутентификации сущности, использующие алгоритмы симметричного шифрования. Четыре из этих механизмов обеспечивают аутентификацию в рамках взаимодействия двух сущностей в условиях отсутствия доверенной третьей стороны: определены два механизма, которые обеспечивают одностороннюю аутентификацию сущности, и еще два механизма – для взаимной аутентификации двух сущностей. Наконец, оставшиеся механизмы требуют наличия доверенной третьей стороны для установления общего секретного ключа и реализуют взаимную и одностороннюю аутентификацию сущности.

Механизмы, определенные в международном стандарте ISO/IEC 9798-2, используют изменяющиеся во времени параметры, такие как временные метки, порядковые номера или случайные числа, для предотвращения возможности использования актуальной аутентификационной информации более одного раза или по истечении времени.

Односторонняя аутентификация характеризуется тем, что аутентифицируется только одна из сущностей. В условиях, когда не задействуется доверенная третья сторона и используются временные метки или порядковые номера,

для односторонней аутентификации необходимо выполнение протокола с одним проходом, а если применяется запросно-ответный протокол с использованием случайных чисел, для односторонней аутентификации нужно два прохода.

Взаимная аутентификация характеризуется тем, что обе сущности аутентифицируют друг друга в процессе взаимодействия. В условиях, когда не задействуется доверенная третья сторона и используются временные метки или порядковые номера, для взаимной аутентификации необходимо выполнение протокола с двумя проходами, а если применяется запросно-ответный протокол с использованием случайных чисел, для взаимной аутентификации нужно три прохода.

При привлечении доверенной третьей стороны любая дополнительная коммуникация между нею и сущностью требует использования двух дополнительных проходов в рамках коммуникационного обмена. В механизмах аутентификации с привлеченной третьей стороной не используется этап разделения секретного ключа между двумя сущностями до начала процесса аутентификации. Вместо этого используется доверенная третья сторона (Рисунок 1.3), с которой каждая из сторон A и B разделяют свой секретный ключ. В рамках этих методов одна из сущностей запрашивает ключ у доверенной третьей стороны.

В третьей части стандарта ISO/IEC 9798-3 определяются методы аутентификации сущности, использующие электронную подпись и основанные на асимметричных криптографических алгоритмах. При этом электронная подпись используется для проверки подлинности сущности. Для предотвращения возможности применения корректной аутентификационной информации по истечении отведенного времени используются изменяющиеся во времени параметры (метки времени, порядковые номера, случайные числа).

В случае использования меток времени или порядковых номеров, для односторонней аутентификации требуется выполнение одного прохода, а для взаимной – два. Если применяется запросно-ответный протокол с использова-

нием случайных чисел, для односторонней аутентификации нужно два прохода, а для взаимной – три или четыре в зависимости от применяемого метода.

В документе определены десять механизмов. Первые пять механизмов не предполагают вовлечение доверенной третьей стороны, которая должна быть доступна в режиме онлайн, а группа из оставшихся механизмов предполагает ее наличие. Обе эти группы включают по два механизма односторонней аутентификации и три механизма взаимной аутентификации.

В методах аутентификации, определенных в документе, аутентифицируемая сущность подтверждает свою подлинность, демонстрируя знание своего секретного ключа подписи. Это достигается тем, что сущность использует секретный ключ для подписи определенных сообщений. Подпись может быть проверена любой стороной с использованием открытого ключа проверки.

Международный стандарт ISO/IEC 10181-2 / ITU-T X.811 «Information technology – Open systems interconnection – Security frameworks for open systems: Authentication framework» посвящен применению сервисов безопасности в среде «открытых» систем, к числу которых, в частности, отнесены базы данных, распределенные приложения, системы открытой распределенной обработки и модель взаимодействия открытых систем; стандарт определяет основные концепции аутентификации, возможные классы механизмов аутентификации, сервисы выделенных классов, функциональные требования для протоколов по поддержке выделенных классов, общие требования менеджмента для аутентификации. Некоторые процедуры, описанные в рамках этого стандарта, обеспечивают безопасность с помощью применения криптографических методов. При этом определены следующие типы аутентификационной информации (Рисунок 1.4):

– аутентификационная информация (АИ) уровня обмена (exchange authentication information);

– АИ уровня предъявления (claim authentication information);

– АИ уровня контроля (verification authentication information).

В некоторых случаях с целью проведения процедуры обмена АИ заявителю может понадобиться обращение к доверенной третьей стороне (ДТС). В свою очередь, и контролер может обратиться к ДТС с целью проведения процедуры обмена АИ. В таких случаях ДТС может хранить АИ уровня контроля, относящуюся к взаимодействующей стороне.

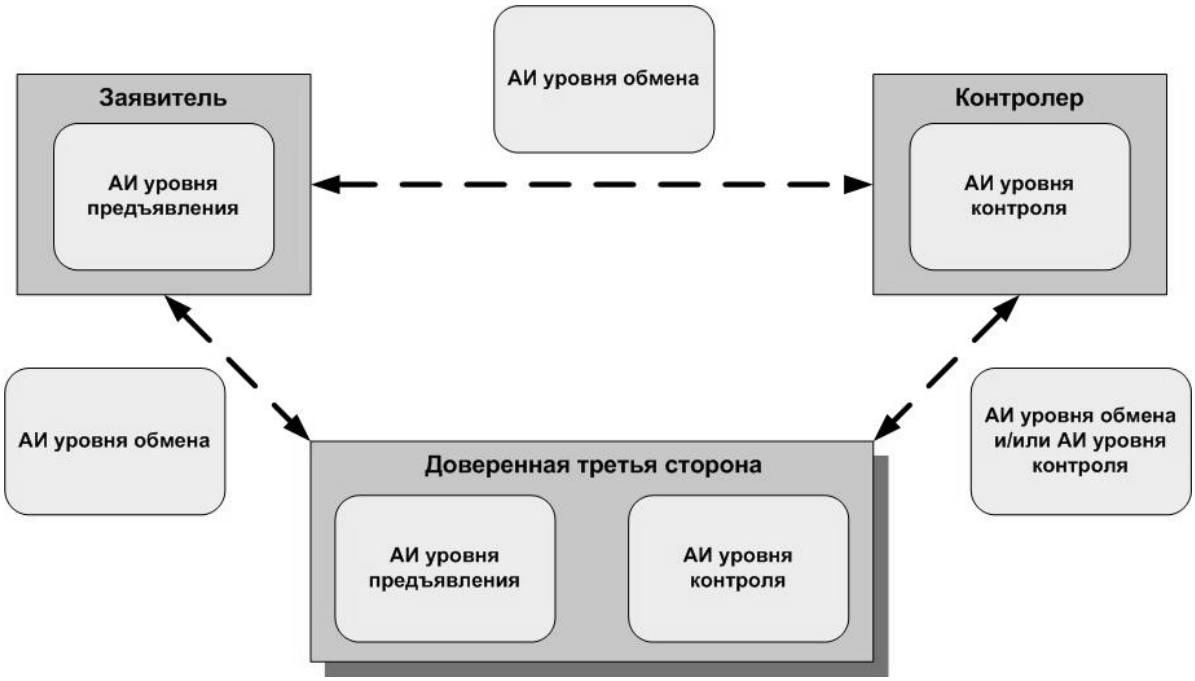

Рисунок 1.4 – Взаимосвязи между заявителем, контролером, проверяющей стороной и типами аутентификационной информации

АИ уровня предъявления является вспомогательной и используется при формировании аутентификационной информации уровня обмена, необходимой для аутентификации одного из участников информационного взаимодействия.

АИ уровня контроля является информацией, которая используется для проверки подлинности, заявленной в рамках АИ уровня обмена.

АИ уровня обмена представляет собой информацию, которой обмениваются между собой заявитель и контролер в течение процедуры аутентификации субъекта.

Механизмы аутентификации могут быть подвержены воздействию атак, реализация которых снижает их эффективность. В международном стандарте ISO/IEC 10181-2 / ITU-T X.811 рассматриваются механизмы аутентификации,

которые могут быть использованы для проведения процедуры аутентификации в фазе передачи данных. Эти механизмы классифицируются в зависимости от угроз, к блокированию которых они устойчивы.

Международный стандарт ISO/IEC 9594-8 / ITU-T X.509 «Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks [Directory authentication]» разработан для упрощения взаимодействия систем обработки информации в целях обеспечения служб каталога (directory services). При этом первая версия этого стандарта носила название «Основы аутентификации». Как правило, термин «каталог» используется для указания организованного набора информация или файлов, которые могут запрашиваться для получения конкретной информации. В более широком смысле в контексте стандартизации безопасности и электросвязи, термин «каталог» обозначает хранилище информации и предоставляет услуги каталога для упрощения связи и обмена информацией между объектами, людьми, терминалами, списками рассылки и т. д.

При работе в рамках каталога в центре внимания постоянно находится ЗИ, которая является главной целью управления подтверждением подлинности. ЗИ каталога – это главным образом вопрос защиты от несанкционированного раскрытия ПДн, но она также включает в себя обеспечение целостности данных и защиту активов, представляемых этими данными.

Каталог может допускать анонимный доступ к некоторой незначительной информации. Однако для получения доступа к более важным данным, требуется определенный уровень аутентификации пользователей. В документе предлагает несколько уровней аутентификации, включая следующие:

– только имя;

– имя и пароль, который передается в виде открытого текста;

– имя и защищенный пароль, т. е. пароль, который хешируется с какой-либо дополнительной информацией для гарантии того, что будет обнаружена любая попытка получить доступ к каталогу путем воспроизведения хешированного значения;

– надежная аутентификация, при которой отправитель подписывает определенную информацию при помощи цифровой подписи. Подписанная информация включает в себя имя получателя и некоторую дополнительную информацию, которая также позволяет обнаруживать попытки входа.

Для разного типа пользователей, имеющих доступ, требуются различные уровни защиты. Уровень аутентификации пользователя также влияет на права доступа для этого пользователя. Права доступа пользователя или группы пользователей зависят от уровня доверия к аутентификации. Получение важной информации или обновление записей обычно потребует более высокого уровня аутентификации, чем получение менее важной информации.

Инфраструктура открытых ключей упрощает управление открытым ключом для предоставления услуг аутентификации, шифрования, целостности и сохранности информации. Фундаментальной технологией для инфраструктуры с открытым ключом является шифрование с открытым ключом.

Международный стандарт ISO/IEC 9594-8 / ITU-T X.509 – это стандарт для строгой аутентификации, основанной на сертификатах открытого ключа. В дополнение к определению структуры аутентификации для инфраструктуры открытых ключей международный стандарт также описывает инфраструктуру управления полномочиями, которая используется для проверки прав и полномочий пользователей в контексте надежной авторизации. В стандарте определена инфраструктура открытых ключей, в которую включена спецификация объектов данных, используемых для представления как самих сертификатов, так и уведомлений об аннулировании выданных сертификатов, которые более не должны признаваться истинными. В стандарте ISO/IEC 9594-8 / ITU-T X.509 определены структура и поля атрибутных сертификатов, в которые включена спецификация объектов данных, используемых для представления как самих сертификатов, так и уведомлений об аннулировании выданных сертификатов. Также определены информационные объекты для хранения объектов инфраструктуры открытых ключей и инфраструктуры управления полно-

мочиями в каталоге, а также для сравнения представленных значений с хранящимися значениями. Кроме того, в документе определена структура для предоставления каталогом услуг аутентификации для его пользователей.

В международном стандарте ISO/IEC 29115 / ITU-T X.1254 «Information technology – Security techniques – Entity authentication assurance framework» отмечается, что многие электронные транзакции в системах на базе информационно-коммуникационных технологий или между такими системами должны осуществляться согласно требованиям безопасности, которые зависят от осознанного или заданного уровня уверенности в подлинности вовлеченных в эти процессы сущностей. Такие требования могут включать защиту активов или ресурсов от НСД, для чего может использоваться механизм контроля доступа, и/или обеспечение подотчетности на основе ведения журналов регистрации соответствующих событий. В стандарте представлена инфраструктура обеспечения доверия в отношении аутентификации сущности (Рисунок 1.5). Такое доверие связано с уверенностью во всех процессах и методах, используемых для установления и управления идентификационной информацией сущности при ее использовании в аутентификационных транзакциях.

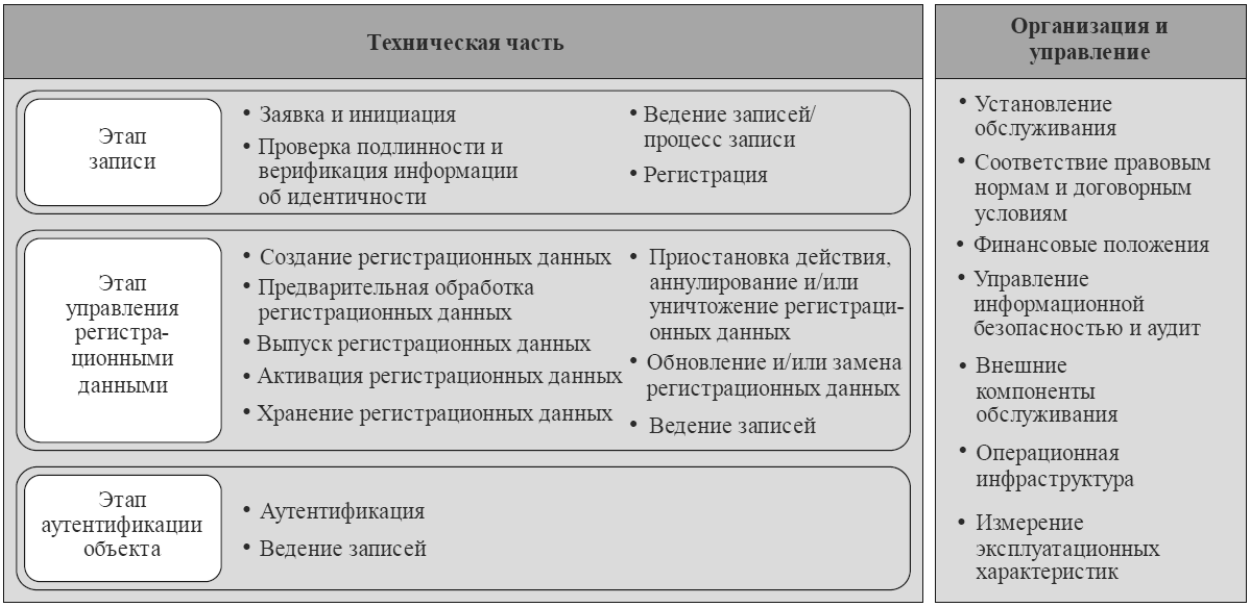

Рисунок 1.5 – Общее представление инфраструктуры обеспечения доверия в отношении аутентификации субъектов и объектов доступа

На основании определенных уровней доверия (levels of assurance, LoA)

представлено руководство в отношении методов контроля, процессов, деятельности в рамках менеджмента, а также критериев доверия, которые следует использовать для снижения опасности угроз аутентификации, в целях реализации LoA.

В международном стандарте также содержится руководство по приведению других инфраструктур доверия к определенным четырем уровням, а также руководство по обмену результатами транзакций, используемыми для аутентификации. В заключение в настоящей Рекомендации приводится подробное руководство по защите АИ, позволяющей проверить подлинность ИИ.

В документе представлена инфраструктура доверия, включая следующие положения:

– определены четыре уровня доверия в отношении аутентификации сущности;

– представлено руководство по отображению других схем доверия в отношении аутентификации на эти четыре уровня LoA;

– представлено руководство по обмену результатами аутентификации, которые основаны на четырех LoA;

– представлено руководство по методам контроля, которые должны использоваться в целях снижения опасности угроз для аутентификации.

Каждый LoA описывает степень уверенности в процессах, приводящих к аутентификации, включая сам процесс аутентификации, обеспечивая, таким образом, доверие в отношении того, что сущность, использующая конкретную ИИ, является той самой, для которой эта идентификационная информация была назначена. Сущность может быть как человеком, так и объектом, не являющимся физическим лицом.

LoA1 представляет собой самый низкий уровень доверия, а LoA4 – самый высокий (Таблица 1.3). Определение того, каким должен быть LoA в каждой конкретной ситуации, зависит от множества факторов. В основном опре-

деление требуемого LoA основывается на риске: последствия ошибки аутентификации и/или ненадлежащего использования регистрационных данных, причиненный в результате вред и воздействие, а также вероятность их возникновения. Более высокие LoA должны использоваться для более высокого предполагаемого риска.

Таблица 1.3 – Уровни доверия в соответствии с международным стандартом ISO/IEC 29115 / ITU-T X.1254

Уровень	Описание
1 – низкий	Незначительная уверенность или отсутствие уверенности в заявленной подлинности
2 – средний	Существенная уверенность в заявленной подлинности
3 – высокий	Высокая уверенность в заявленной подлинности
4 – очень высокий	Очень высокая уверенность в заявленной подлинности

Инфраструктура доверия определяет требования и руководства по реализации каждого из четырех LoA.

На уровне LoA1 имеет место минимальная уверенность в заявленной подлинности сущности, но после нескольких последовательных событий аутентификации возникает некоторая уверенность в том, что сущность подлинная. Этот LoA используется, когда ошибочная аутентификация сопряжена с минимальным риском. Особые требования к используемым механизмам аутентификации отсутствуют, они должны обеспечивать лишь некое минимальное доверие. Этот уровень не требует использования криптографических методов.

На уровне LoA2 имеет место значительная уверенность в заявленной подлинности сущности. Этот уровень используется, когда ошибочная аутентификация связана с умеренным риском. На этом уровне приемлемым является использование однофакторной аутентификации. Должны использоваться средства контроля, позволяющие снизить эффективность атак перехвата информации и подбора пароля в режиме реального времени. Должны быть также

реализованы средства контроля для защиты от атак, направленных на хранящиеся учетные данные.

На уровне LoA3 имеет место высокая уверенность в заявленной подлинности сущности. Этот уровень используется, когда ошибочная аутентификация связана со значительным риском. На этом уровне должна использоваться многофакторная аутентификация. Любая секретная информация, обмен которой осуществляется в рамках протоколов аутентификации, должна быть криптографически защищена как при передаче, так и в дежурном режиме (при этом LoA3 не требует применения запросно-ответного криптографического протокола). На этом уровне какие-либо требования к созданию или хранению учетных данных не предусматриваются; эти данные могут храниться или создаваться в компьютерах общего назначения или с помощью специализированного аппаратного оборудования.

LoA4 характеризуется очень высокой уверенностью в заявленной подлинности сущности. Этот уровень используется, когда ошибочная аутентификация сопряжена с очень высоким риском. На этом уровне обеспечивается наивысший уровень доверия в отношении аутентификации. Уровень LoA4 схож с уровнем LoA3, но на нем добавляются требования к собственноличному подтверждению подлинности для сущностей, являющихся людьми, и использование защищенных от проникновения устройств для хранения всех секретных криптографических ключей. Кроме того, персональные данные и другие сведения конфиденциального характера, включенные в протоколы аутентификации, должны быть криптографически защищены как при передаче, так и в дежурном режиме.

Выбор надлежащего LoA следует осуществлять на основе оценки риска транзакций или сервисов, в рамках которых сущности будут проходить аутентификацию. Международный стандарт ISO/IEC 29115 содержит пример матрицы оценки потенциальных последствий ошибочной аутентификации для разных LoA. Угрозы на этапе аутентификации включают общие угрозы и

угрозы, связанные с использованием учетных данных в рамках аутентификации. Общие угрозы аутентификации включают, в том числе, следующие: использование вредоносного ПО (например, вирусы, троянские программы, клавиатурные шпионы), социальная инженерия (например, подсматривание, кража аппаратных устройств и PIN-кодов), ошибки пользователей (например, ненадежные пароли, неиспользование мер защиты аутентификационной информации), ложный отказ, несанкционированный перехват и/или изменение данных аутентификации во время передачи, отказ в обслуживании, ненадежность процедур. За исключением случая использования многофакторной аутентификации, средства контроля общих угроз аутентификации не входят в область действия международного стандарта ISO/IEC 29115.

Существует большое число угроз в отношении учетных данных, содержащих ПДн, при их использовании для целей аутентификации. В документе перечислены некоторые распространенные категории угроз, имеющих место при использовании учетных данных, и приводятся конкретные примеры реализации этих угроз. Кроме того, международный стандарт ISO/IEC 29115 содержит перечень мер защиты от указанных категорий угроз.

Анализ международных и национальных стандартов, регламентирующих процессы ИА, показал:

– в рамках деятельности Международной организации по стандартизации (International Organization for Standardization), Международной электротехнической комиссия (International Electrotechnical Commission) и Международного союза электросвязи (International Telecommunication Union) разработана система международных стандартов, регламентирующих различные аспекты ИА;

– стандарты, входящие в состав системы международных стандартов, постоянно совершенствуются, а основные положения систематически пересматриваются в соответствии с существующими возможностями их технической реализации;

– в качестве базовых характеристик процесса ИА представляется целесообразным определить:

1) виды идентификации (первичная, вторичная);

2) факторы аутентификации и их использование в процессе аутентификации (однофакторная, двухфакторная, многофакторная аутентификации);

3) формы обмена АИ (односторонняя, взаимная аутентификации);

4) виды аутентификации (простая, усиленная, строгая аутентификация).

Дальнейший анализ осуществлен с учетом базовых характеристик процесса ИА.

Анализ НПА по ЗИ от НСД[1] в части ИА выполнялся по следующим направлениям:

– наличие в НПА норм, определяющих процессы ИА субъектов доступа;

– наличие в правовых нормах характеристик технической реализации процессов ИА субъектов доступа (в части механизмов, средств и видов).

Проведенный анализ включал:

– формирование перечня НПА по ЗИ от НСД, в которых регламентируется реализация процессов ИА;

– формирование критериев, в соответствии с которыми проводится анализ НПА;

– анализ НПА, регламентирующих процессы ИА субъектов доступа в соответствии с установленными критериями;

– обобщение результатов проведенного анализа.

В рамках анализа рассмотрены 123 нормативных правовых акта, регла-

[1] Кроме нормативно правовых актов по защите информации от несанкционированного доступа был проведен анализ документов, которые относятся к построению информационных систем федерального уровня, а также в которых возможно наличие правовых норм, регламентирующих процессы идентификации и аутентификации

ментирующие вопросы ЗИ в различных областях деятельности. Примеры рассмотренных актов, непосредственно касающихся темы ИА, приведены в списке источников [68, 69, 70, 71,72, 73, 74,75];

В качестве основных критериев анализа определены:

– наличие и документальное подтверждение правовых норм, в соответствии с которыми реализуются процессы ИА субъектов доступа в ИС;

– наличие и документальное подтверждение в правовых нормах характеристик технической реализации в части видов, механизмов и средств ИА субъектов доступа;

– способы, а также состав механизмов и средств ИА субъектов доступа, которые должны быть реализованы в ИС;

– виды аутентификации, необходимые для реализации в информационной системе. Если виды аутентификации не определены конкретно, то они могут формироваться по приведенным правилам (Таблица 1.4);

Таблица 1.4 – Правила определения вида аутентификации

Факторы аутентификации	Обмен аутентификационной информацией	Вид аутентификации
Однофакторная	Односторонний	Простая
Многофакторная	Односторонний или взаимный	Усиленная
Многофакторная	Взаимный	Строгая

Анализ рассмотренных нормативно-правовых актов (НПА) на предмет наличия правовых норм, регламентирующих процессы ИА субъектов доступа, показал:

– в подавляющем большинстве НПА по защите информации (ЗИ) от НСД процедуры ИА не определяются в качестве обязательных;

– некоторое количество НПА по ЗИ от НСД содержат правовые нормы,

определяющие необходимость реализации процедур ИА, но при этом характеристики технической реализации в части видов, механизмов и средств ИА субъектов доступа не рассматриваются;

– небольшая часть НПА по ЗИ от НСД содержат правовые нормы, определяющие необходимость реализации процедур ИА, и при этом регламентирующие их техническую реализацию в части видов, механизмов и средств ИА субъектов доступа;

– в НПА, содержащих правовые нормы в качестве характеристик технической реализации, определены простая (однофакторная, односторонняя) и строгая (двухфакторная, взаимная) аутентификации.

1.2 Краткий обзор научных работ, посвященных вопросам анализа процессов идентификации и аутентификации субъектов доступа

Методы и средства аутентификации (подтверждения подлинности предъявленных пользователем идентификаторов) относятся к категории классических механизмов управления доступом пользователей и ИБ как в корпоративных, так и в глобальных коммуникационных сетей [5- 9, 12, 39, 40, 76, 77, 78, 79, 80, 81, 82]. Вопросам управления доступом посвящено достаточно много научных работ. Из них можно выделить труды Н.А. Гайдамакина [6] и П.Н. Девянина [83]. В этих работах рассмотрены основные модели управления доступом, однако предложенные в их работах математические модели не включают в себя моделирование процессов ИА. При этом они учитывают возможность создания, изменения, удаления и аудита пользовательских учетных записей. Как правило, цели перечисленных работ акцентировались на решении общей проблемы управления доступом, заключающейся в допуске легальных пользователей к информации и защите от атак злоумышленников, пытающихся получить такой доступ. Заметим, что наибольший интерес у исследователей вызывали формальные модели безопасности предоставления доступа (дискреционная, мандатная, ролевая и др.), а проблемам ИА субъектов доступа

уделялось минимальное внимание. В отличие от них вопросы моделирования процессов аутентификации рассмотрены в работах [15, 31, 32, 37, 37, 84], рассмотрим эти работы подробнее.

Способ моделирования и исследования последовательных процессов ИА при необходимости обслуживания одновременного обращения 1000 запросов с помощью метода массового обслуживания представлен в работе [85]. При полной (100%) загрузке модуля аутентификации загрузка модуля идентификации определена как 90,7%. При этом вероятность отказа в аутентификации оценен как 2,2%. К сожалению, работа не получила дальнейшего развития.

Несомненно, весьма существенный научный вклад в развитие теории идентификации и аутентификации внес коллектив под управлением академика А.А. Грушо. Работы этого коллектива отличаются свежими идеями и строгим научным изложением. Если работа [9] посвящена теоретическим основам защиты информации в электронных системах данных, то в работе [10] часть книги непосредственно касается парольной аутентификации и протоколов аутентификации. Статья [86] явилась своего рода катализатором появления ряда статей разных авторов по аутентификации в задачах УЭВ. В одной из недавних работ [87] показана роль анализа и управления идентификационными данными субъекта доступа, находящимся в различных ИС, для организации процесса аутентификации, дающего достоверные результаты и защиту идентификационной и аутентификационной информации от злоумышленника.

Проблемы аналитического моделирования процессов аутентификации как часть задачи защиты информации от НСД рассмотрены с помощью применения сетей Петри-Маркова в работах [31, 32, 37]. В работах [31, 32] разработаны модели парольной аутентификации в задачах ЗИ от атак злоумышленника. Показано, что для управления вероятностью успешной реализации НСД по времени (с использованием статических данных) можно построить аналитическую модель НСД в ИС. Также показана эффективность использования математического аппарата на основе сетей Петри–Маркова на примере построения модели угрозы перехвата чужих паролей легальным пользователем

операционной системы [37].

В работе [88] приводится обзор основных способов удаленной аутентификации, однако содержание статьи носит описательный характер без сравнительного анализа приведенных способов и анализа рисков, несмотря на заявленное их наличие.

Достаточно интересен подход к оценке защищенности многофакторной аутентификации, разработанный в статье [89]. Однако постановка задачи в этой работе не совсем корректна. Под многофакторной аутентификацией в статье понимается последовательное предъявление аутентификационной информации (факторов), что неверно как с точки зрения определения (многофакторной аутентификацией называется одновременное использование всех факторов, точнее, использование следующего фактора при применении предыдущего и т.д.), так и по соображениям надежности (известно, что надежность последовательных процедур определяется надежностью самого слабого звена).

Из работ по оценке надежности ИС следует выделить исследования, проведенные под руководством А.Ю. Щеглова, например, квинтэссенцией ряда работ являются методические указания [90]. Однако в этой работе не рассматриваются ИА. В нескольких работах, созданных под руководством А.И. Щеглова, ИА упоминаются в названии, но работы посвящены решению других проблем. Так, в работе [91] фактически рассматриваются не процессы ИА, а формальные модели безопасности, применяемые для доступа к таблицам базы данных.

Начиная с 2016 г. среди научных работ стали чаще появляться статьи по применению биометрических технологий в целях ИА субъектов доступа. Среди множества работ, авторами которых являются представители компаний, производящих средства биометрической идентификации (рассмотрение которых выходит за рамки данного исследования) выделим несколько работ, в которых имеются некоторые, зачастую нестандартные научные идеи. Так, работа [92], являясь кратким переводом известных идей Филиппа Гриффина [93] о подмешивании показаний биометрического датчика в протокол обмена

криптографическими ключами (BAKE – Biometric authenticated key exchange), что может повысить идентификацию отправителя сообщения, «снизить риски неавторизованного доступа и защищенность идентификационных данных». Заметим, что как будет показано ниже во второй и третьей главах, добавление биометрических данных к применению всего лишь одного фактора знания (пароля) в протоколе аутентификации вряд ли может гарантированно выполнить задачи, перечисленные в цитате. Безусловно заслуживает внимания интересная идея адаптивной (RBA – risk-based authentication: риск-ориентированной) аутентификации, высказанная в работе [94]. Суть высказанной в статье идеи состоит в последовательном применении анализа данных об окружении точки доступа (Endpoint), поведении субъекта доступа и его уровня знаний его биометрических данных (Behavior &Biometrics), данных о пользователе (User data), связях субъекта и соответствующей аналитике, перед применением тех или иных методов аутентификации. В статье утверждается, что поведенческая биометрия и применение перечисленных аналитических данных может в ряде случаев даже заменить традиционные методы аутентификации на простую идентификацию без использования подтверждения субъектом, а для рисковых операций может потребоваться применение дополнительного фактора. При внимательном изучении материалов легко выяснить, что эта идея принадлежит известному коллективу авторов – Стефана Вифлинга (Wiefling, Stephan) Луиджи Лоякомо (Lo Iacono, Luigi) и Маркуса Дюрмута (Dürmuth, Markus), опубликованных в последние годы, развитие идеи приводится в [95, 96]. Такое положение объясняется тем, что теория аутентификации, также как и ее различные реализации, развивались преимущественно западными учеными и специалистами. К сожалению, мы пока мало чему можем их научить. Одной из причин может являться неразвитость методов анализа рисков, на основе которых обычно исследуется любой процесс и объект защиты, причем ИА не являются исключением. Продолжение анализа научных работ будет представлено в соответствующих контекстно связанных разделах глав.

Международные стандарты, безусловно, сыграли ведущую роль в развитии методов и инструментария относительно молодой (всего немногим более 20 лет) науки «Анализ рисков». Из более 100 международных и 45 отечественных стандартов, касающихся проблем оценки рисков, можно выделить несколько основополагающих документов по анализу методов оценки рисков.

В группу основных источников стандартов, методик и инструментов анализа рисков входят британский стандарт [97] и рекомендации по управлению рисками американского Национального института стандартов и технологий (NIST) [98]. В Российской Федерации вопросы стандартизации обеспечения безопасности ИС регламентируются базовыми положениями Федерального закона № 184-ФЗ «О техническом регулировании» [99] с изменениями [100, 101], а также переводными международными стандартами [102, 103, 104, 105, 106, 107, 108, 109, 110] и отраслевыми документами, такими как методика Банка России [111] и стандарт для железнодорожного транспорта на основе зарубежного и отечественного опыта [112]. Из известных отечественных научных работ по анализу рисков своей практической направленностью выделяются работы Г.Е Шепитько [113], однако его работы, также как и труды других авторов, развивая теорию и практику оценки рисков, достаточно далеки от исследования рисков ИА.

Вывод по разделу: комплексного анализа процессов ИА по критериям достоверности, надежности и безопасности в открытой литературе не обнаружено. Также при анализе не выявлено комплексных исследований проблем доверия к результатам ИА. Имеются отдельные работы по близким, но узконаправленным задачам (например, проблема доверия к криптографическим протоколам), которые будут рассмотрены в конце третьей главы. Многие из упомянутых исследований не получили дальнейшего развития. Это еще одно подтверждение актуальности данной работы.

1.3 Понятия и методическая основа исследовани идентификации и аутентификации

Понятия «надежность», «достоверность», «безопасность» и их применение при оценке характеристик процессов идентификации и аутентификации.

Базируясь на результатах [37] для вычислительных систем, проведем анализ основных понятий «надежность», «достоверность», «безопасность», а затем покажем взаимосвязь этих понятий применительно к теме исследования.

Рассмотрим понятие «надежность информационной системы». Поскольку система идентификации и аутентификации (СИА) является частью информационной системы, под надежностью работы СИА будем понимать функциональную надежность [35]. Это понятие состоит из трех составляющих частей: характеристик надежности, средств и угроз надежности (не смешивать с угрозами информационной безопасности, хотя пересечение, безусловно, имеется). На рисунке 1.6 представлены основные составляющие надежности работы информационной системы.

Рисунок 1.6 – Понятие надежности и его составляющие [35]

К основным характеристикам надежности относятся как традиционные характеристики безопасности информации (доступность, конфиденциаль-

ность и целостность), так и характеристики надежности самой системы (безотказность, сохранность и ремонтопригодность). Среди основных угроз надежности как традиционные (отказы, неисправности и ошибки), так и возможные атаки злоумышленников, которые могут приводить или не приводить к отказам и неисправностям. Следовательно, средства повышения степени надежности системы должны противодействовать основным угрозам.

Современные информационные системы обладают следующими основными свойствами: функциональное наполнение, производительность, управляемость, обеспечение безопасности, стоимость и надежность.

Надежность информационной системы - это способность предоставлять услуги, которым можно обоснованно доверять [35]. Обслуживание, предоставляемое системой, – это воспринимаемое пользователем ее поведение; пользователь — это другая система (физическая система либо человек), взаимодействующая с данной системой посредством служебного интерфейса. В данной работе будем полагать, что в процессе регистрации нового пользователя ИС пользователем может являться заявитель, а в процессах вторичной идентификации и аутентификации пользователем является зарегистрированный субъект доступа. Таким образом, задача надежности (а как показано выше, строго говоря, функциональной надежности) в данной работе состоит в том, чтобы исследовать процессы, автоматизированные в СИА, с целью выбора оптимального процесса для получения надежных результатов ИА.

Важнейшим понятием в теории надежности является понятие «отказ». В информационной системе, и, соответственно, в системе ИА, отказ происходит не всегда одинаково. Различные способы отказа системы называют состояниями отказа. Состояния отказа отражают предоставление ненадлежащего обслуживания с точки зрения сферы действия (значение и время отказа), восприятия пользователями (систематические или случайные отказы) и последствий для среды (несущественные, значительные или катастрофические отказы).

Попытки напрямую связать понятия отказа системы с характеристиками

ее безопасности всегда сталкивались с трудностями и не имеющими соответствия действительности результатами, поскольку этот вопрос находится на стыке двух параллельно развивающихся наук – теории надежности механизмов и теории информационной безопасности. Чтобы приблизиться к решению данной проблемы, вновь обратимся к рис. 1.6.

Безопасность не является единственной характеристикой надежности. В обобщенном смысле под безопасностью можно понимать отсутствие НСД к состоянию системы и информации, хранящейся, передаваемой и обрабатываемой системой. В то же время определение доступности и безотказности подчеркивают предотвращение отказов, а определение сохранности и безопасности – отдельных классов отказов (катастрофических отказов и несанкционированного доступа к информации соответственно). Следовательно, безотказность и доступность находятся в более тесной связи друг с другом, чем с сохранностью и с безопасностью. Безотказность и доступность условно можно объединить в одно понятие – предотвращение (минимизация) простоев в обслуживании, а фактически это широко используемое в настоящее время понятие обеспечения непрерывности обслуживания. Следует заметить, что при значительном количестве пользователей ИС система ИА может рассматриваться как система массового обслуживания (СМО). При этом такие характеристики, как безопасность и непрерывность обслуживания, могут иметь первостепенное значение при проектировании таких систем.

Под **достоверностью** результатов идентификации и аутентификации будем понимать полноту, точность (ГОСТ Р ИСО 15489-1–2007), актуальность и аутентичность получаемых в результате данных [114]. Как упоминалось выше, вопрос достоверности результатов идентификации и аутентификации не исследовался ранее. Мало того, незначительное число отечественных публикаций посвящено проблемам достоверности информации как таковой. В работах западных авторов [80-88] под достоверностью понимается качество информации как пригодность для использования в задачах принятия управленческих решений. Широко известен тезис о том, что управление качеством данных

определяет вектор развития информатизации общества [115]. Достоверность информации не является обособленной характеристикой, она определяет факторы риска, которые влияют на принятие управленческих решений [116]. Применительно к задаче идентификации и аутентификации субъекта доступа — это риски недостаточной точности и актуальности источника идентификационных данных, НСД, подмены источника, дестабилизирующих (деструктивных) факторов, риски ошибок в передаче и взаимодействии информационных систем и др. В данной постановке достоверность информационного ресурса (ИР) следует связать с его доступностью и целостностью его информации. Целостность ИР обеспечивается, если он нелегитимно не изменяется, доступность - если легитимный процесс получает ИР за приемлемое время. Все перечисленное должно быть обеспечено при функционировании системы обмена информацией в условиях случайных или преднамеренных информационных воздействий [117]. Итак, достоверность связана с одной стороны, с надежностью работы системы идентификации, с другой стороны – с основополагающими принципами безопасности информации.

Из задач информационной безопасности применительно к процессам ИА выделим две главных. Во-первых, как сервис безопасности, работа СИА должна быть спроектирована и построена на принципах обеспечения безопасности Secure by Design, т.е. сама быть безопасной и доверенной [116] согласно Приказу №131 ФСТЭК России [118] для обрабатываемой в ней информации и защищенной от внешних атак. Во-вторых, информация, которую обрабатывает СИА, содержит персональные данные субъектов доступа. Система идентификации и аутентификации должна быть спроектирована по второму широко применяемому в настоящее время принципу – Privacy by Design, ставящему своей целью обеспечение конфиденциальности обрабатываемых персональных данных. Обе перечисленные задачи ИБ решаются на базе анализа рисков, как основе учета всех факторов воздействия на информацию в СИА. Как было показано выше, анализ рисков как базовый инструмент, лежит и в

основе оценок надежности, безопасности и достоверности информации, в полной мере это относится к результатам идентификации и аутентификации субъектов доступа.

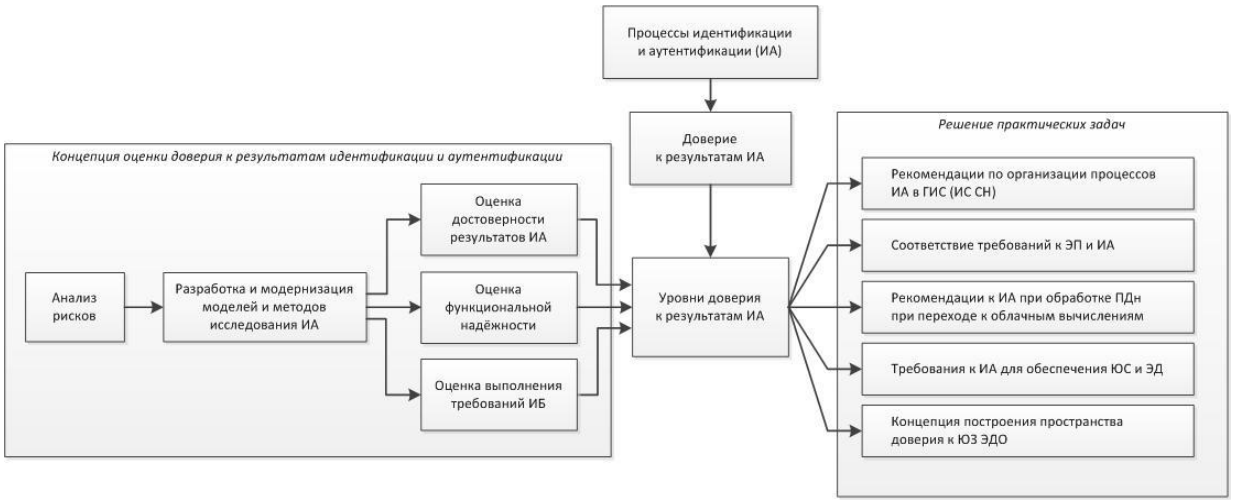

Рисунок 1.7 - Схема исследований данной работы.

Таким образом, схема построения данной диссертационной работы в концептуальном виде может быть представлена на рис. 1.7, где центральное место занимает анализ рисков как основной инструмент исследований достоверности, функциональной надежности и выполнения требований безопасности с целью создания методологии формирования уровней доверия к результатам ИА. Достижение поставленной цели позволит решить ряд актуальных прикладных задач.

Заметим, что достоверность, также как безопасность и надежность, не может быть абсолютной. Как правило, эти характеристики (**безопасность, надежность, достоверность**) в силу вероятности появления ошибок и сбоев, неопределенности параметров внешних ИС и информационного обмена, могут быть представлены в виде безразмерных характеристик, изменяющихся от нуля до единицы. Такой подход применяется и в данной диссертационной работе.

Одним из основных методов, используемых в исследованиях при оценке надежности, безопасности и достоверности процессов и получаемых в итоге

результатов работа идентификации и аутентификации являются методы анализа и управления рисками.

1.4 Теоретическое обобщение методов анализа рисков применительно к процессам идентификации и аутентификации

Основные этапы оценки и управления рисками включают (Рисунок 1.7):

– анализ риска;

– оценивание риска;

– снижение /контроль риска.

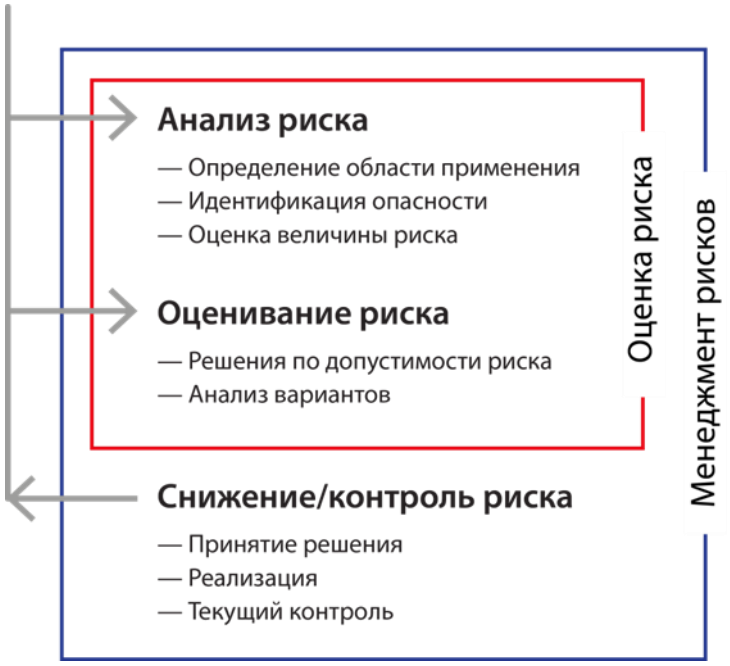

Рисунок 1.7 – Этапы анализа и управления рисками [119]

Из анализа рисунка следует, что стандарт [119] уточняет соотношение понятий оценки риска с часто употребляемым в настоящее время понятием менеджмента рисков.

Для выбора той или иной методики применительно к конкретным случаям необходимо систематизировать методы оценки рисков, и сформулировать требования к ней. Методы оценки рисков обычно классифицируют по типу получаемых с их помощью результатов: качественные, количественные и смешанные (гибридные).

На основе качественных методов, как правило, можно получить оценку

рисков в соответствии с простой шкалой уровней рисков, например: низкий, средний, высокий. Среди примеров качественных методов можно назвать методику и соответствующий инструментарий COBRA (первая версия разработана компанией C&A Systems Security в 1997 г. на основе стандарта [97]), методику и инструментальное средство RA Software Tool (части 3, 4 стандарта [97]) и стандарта[120], а также некоторые руководства Британского национального института стандартов BSI. К категории качественных методов можно также отнести пакет FRAP (Facilitated Risk Analysis Process) [121].

Количественные методы необходимы в случаях, когда предполагаемый ущерб от реализации рисков велик, а также для того, чтобы оценить альтернативные меры по обеспечению безопасности с целью выбора наилучшей защиты.

Методики оценки рисков можно классифицировать по типу процедуры принятия решений:

– одноэтапные, которые используются, как правило, на начальной стадии развития инфраструктуры организации, когда еще не выявлены ключевые факторы, влияющие на ИБ;

– многоэтапные, с предварительной оценкой ключевых параметров. Они известны по методикам и приняты к рассмотрению: потенциальный ущерб, вероятность реализации угрозы [120] или степень возможности реализации угроз ИБ [122], а также степень тяжести последствий от реализации угроз (величина ущерба) [111].

Следует заметить, что оценка рисков должна рассматриваться как определенный шаг на пути к выработке требований ИБ. Оценка риска, по международным стандартам, является итеративным и вариативным процессом, т.е. общая оценка риска должна привести к выводу о том, достигнут ли допустимый риск. Если после применения защитных мер этого не произошло, требования к ИБ следует усилить, а процесс оценки риска необходимо повторить до тех пор, пока не будет обеспечен его допустимый уровень. Если же риск не может быть снижен до необходимого уровня, то снижение осуществляется,

например, путем страхования или риск принимается [123, 124].

Существует ряд методов анализа факторов опасности, все их можно разделить на два вида: дедуктивный и индуктивный. В дедуктивном методе предполагается конечное событие, а затем отбираются те из них, которые могли бы его вызвать. В индуктивном методе рассматривается отказ компонента исследуемой системы, а последующий анализ обеспечивает идентификацию событий, которые данный отказ вызвали.

Среди дедуктивных методов можно выделить метод системного анализа рисков MOSAR (Method Organized for a Systematic Analysis of Risks). Он включает десять этапов. Анализируемая система при использовании данного метода рассматривается как некоторое количество подсистем, которые взаимодействуют. Для идентификации факторов опасностей, опасных ситуаций и опасных событий используются таблицы, которые позволяют разработать сценарии реализации рисков. Сценарии рисков сортируются по степени серьезности. В последующей таблице серьезность связывается с целями, на реализацию которых направлены меры по обеспечению безопасности, и определяются уровни эффективности технических и организационных мер. Затем меры по обеспечению безопасности включаются в логические деревья, а остаточные риски анализируются по таблице допустимости.

Еще один дедуктивный метод – FTA (Fault Tree Analysis – анализ дерева неисправностей) [125], где отправной точкой является событие, рассматриваемое как нежелательное. Этот метод дает возможность пользователю найти целый набор критических вариантов, которые приводят к нежелательному событию. Опасные или итоговые события сначала идентифицируются, затем все сочетания отдельных отказов показываются в логическом формате дерева неисправности. Оценивая вероятности отдельных отказов и используя соответствующие арифметические операции, можно рассчитать вероятность итогового события. Влияние изменения системы на вероятность итогового события оценить легко, поэтому метод FTA упрощает исследование воздействия альтернативных мер по обеспечению безопасности. Более подробно это метод

анализа будет рассмотрен ниже.

Технологический прогноз, основанный на методе Дельфи [126], представляет собой попытку предсказать развитие той или иной технологии на длительную перспективу (до 30 лет). Разработанная в 50-х годах корпорацией RAND техника метода Дельфи использована впервые для целей национального и отраслевого технологического прогнозирования в Японии, а впоследствии, в Германии, Франции, Великобритании, Испании, Австрии, Южной Корее. Суть метода в том, что большая группа экспертов опрашивается в несколько этапов, затем результат предыдущего этапа вместе с дополнительной информацией сообщается всем участникам. Во время третьего или четвертого этапа анонимный опрос концентрируется на тех аспектах, по которым пока никакое соглашение не достигнуто.

Среди индуктивных методов анализа факторов опасности и оценки риска следует отметить предварительный анализ факторов опасности, метод «что, если», анализ состояния и результатов отказа, моделирование неисправности в системах управления.

Назначение такого метода, как предварительный анализ факторов опасности (Preliminary Hazard Analysis), состоит в идентификации для всех этапов эксплуатационного периода факторов опасности, опасных ситуаций и опасных событий, которые могли бы привести к рискованному случаю. После идентификации возможности рискованного случая выводятся предложения о мерах по обеспечению безопасности и результат их применения.

Метод «что, если» применяется для относительно простых приложений, которые охватывают проектирование и использование оборудования. На каждом этапе задаются вопросы «что, если» и на них даются ответы, позволяющие оценить влияние отказов компонентов или методических ошибок на возникновение факторов опасности в механизме.

Цель анализа состояния и результатов отказа FMEA (Failure Mode and Effects Analysis) – оценить частоту и последствия отказа компонента. Этот метод требует более длительного времени, чем использование дерева дефектов,

потому что для каждого компонента рассматривается каждый вид отказа [122]. При методе моделирования неисправности в системах управления методики испытаний основаны на двух критериях: технология и сложность системы управления.

После идентификации факторов опасности должна быть выполнена оценка риска для каждого фактора опасности путем определения элементов риска. Риск, связанный с конкретной ситуацией или техническим процессом, складывается из сочетания следующих элементов (Рисунок 1.8):

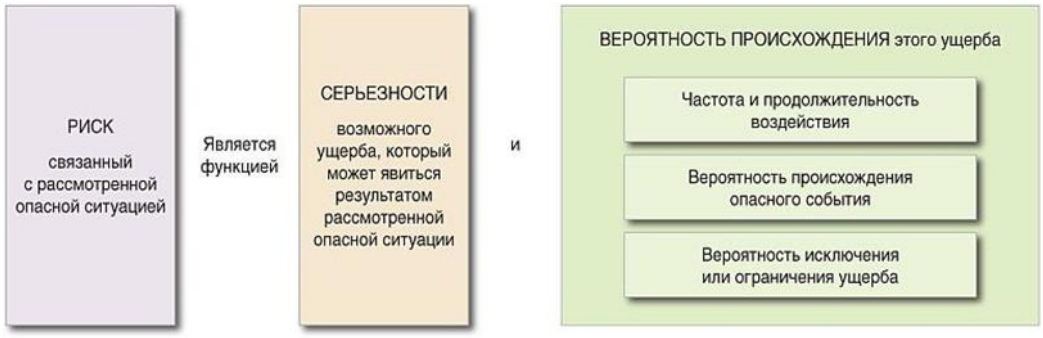

Рисунок 1.8 – Риск, связанный с конкретным фактором [122]

Рассмотрим каждый из элементов риска. Серьезность ущерба помогают оценить следующие показатели:

– характер объекта, который должен быть защищен: люди, собственность или окружающая среда;

– серьезность повреждений или последствия причинения вреда здоровью: небольшая (обычно обратимый вред), значительная (обычно необратимый вред), смерть;

– степень ущерба.

Вероятность происхождения (нанесения) ущерба оценивается с учетом частоты и продолжительности воздействия; вероятности наступления опасного события; возможности для предотвращения или ограничения ущерба. Практически во всех случаях на риск влияет человеческий фактор – он обязательно должен приниматься во внимание при оценке риска [120].

Таким образом, методов анализа рисков процессов ИА в открытых источниках не найдено. Требуется формирование концепции, методов, методик и математических моделей для проведения анализа рисков ИА при УЭВ. С другой стороны, разнообразие достаточно развитых к настоящему времени подходов и методов анализа рисков позволяет сделать оптимальный выбор приемлемых для оценки рисков ИА из существующих методов и предоставляет возможность на основе их анализа разработать методологию анализа рисков с учетом специфики процессов ИА и требований ИБ.

1.5 Анализ применимости методов оценки рисков к теме исследования

Основные методы анализа рисков рассмотрены в [106, 107]. Достаточно подробное теоретическое обобщение методов оценки рисков приведено в [127], однако при подготовке этой работы к печати из рассмотрения выпал опубликованный после выхода статьи [127] стандарт [124], в котором впервые системно изложен 31 метод анализа рисков. В данном разделе эти методы анализируются с точки зрения применимости к задачам оценки рисков ИБ для процессов аутентификации в ходе удаленного электронного взаимодействия.

Исходные данные. Для оценки применимости развитых к настоящему времени методов анализа рисков к процессам аутентификации при удаленном электронном взаимодействии использованы результаты работ [124], а также практический опыт исследований, проектирования, построения и сопровождения систем ИА в десятках крупных и средних организаций различного профиля деятельности, накопленный автором за 18 лет работы в этой сфере.

Рекомендации стандартов. Согласно стандартам [106, 107, 124] для анализа рисков сначала следует подробно описать область определения. С этой целью в [128] рассмотрены основные процессы аутентификации, в работе [129] рассмотрены проблемы идентификации и аутентификации в распределенных информационных системах, на основе чего разработана классификация средств [130] и процессов аутентификации [131], а в [132] проведен анализ

и представлена классификация систем ИА по признакам соответствия требованиям ИБ.

На втором этапе анализа рисков стандартами [106, 107, 124] рекомендуется провести работы по идентификации рисков. Здесь должны быть определены опасные события, частота и вероятность их наступления. Для СИА результаты таких исследований представлены в [133], причем следует отметить такой интересный результат, как вывод о необходимости введения уровней достоверности аутентификации, вытекающий из анализа угроз и уязвимостей процедур регистрации нового пользователя ИС. Также обоснованием введения УДА служит анализ процедур хранения и предъявления аутентификационной информации пользователя.

Следующим этапом оценки рисков рекомендуется провести непосредственно процедуру анализа рисков [106, 107, 124]. Результаты оценивания рисков ИА могут использоваться, с одной стороны, в качестве исходных данных для итеративного процесса анализа рисков и их снижения до приемлемого уровня, а с другой – итоговые значения рисков (после итераций) можно применять для уточнения границ достоверности аутентификации. В данной работе оценим применимость наиболее известных методов анализа рисков к процессам ИА, это может оказаться полезным для понимания возможных способов снижения рисков при построении и эксплуатации СИА, а также при выборе методов и средств ИА.

Рассмотрим методы анализа рисков в общем виде, акцентируя внимание на применимости входных и выходных данных для задачи оценки рисков ИА, в том числе при УЭВ. Для этого определим критерии применимости.

Критерии применимости методов анализа рисков. Для оценки и управления рисками аутентификации согласно рекомендациям, приведенным в стандарте [124], выбраны следующие критерии:

– оценка объёма подготовительных работ для последующего анализа конкретным методом из 31 приведенного в стандарте ГОСТ Р 31010;

– доступность исходных (входных) данных;

– оценка применимости выходных данных для последующего анализа;

– наглядность результатов;

– удобство анализа с применением данного метода.

Оценка применимости. Для проведения оценки методов анализа рисков произведён предварительный отбор методов по их назначению. Априори ненужные для анализа ИБ-рисков методы (например, метод оценки токсикологического риска и др.) сразу были исключены из рассмотрения. Также из списка методов изъяты те, которые в стандарте [124] не рекомендованы к применению для процессов идентификации риска и анализа риска (например, метод Монте-Карло, байесовский анализ и др.). В итоге из представленных в 31 метода оценки риска идентификации и аутентификации в таблицу вошли только 18 (Таблица 1.5). Для удобства восприятия в таблице использованы следующие принятые в международных и отечественных стандартах обозначения уровней рисков: Н – низкий, С – средний, В – высокий.

Таблица 1.5 – Оценка применимости методов анализа рисков

Номер метода	Метод	Объем подготовительных работ	Доступность входных данных	Применимость выходных данных	Наглядность результатов	Удобство анализа
1.	Мозговой штурм	Н	Н	С	С	С
2.	Структурированное интервью	Н	С	Н	С	Н
3.	Метод Дельфи	Н	Н	С	С	С
4.	Предварительный анализ опасностей (PHA)	Н	С	В	В	В
5.	Исследование опасности и работоспособности (HAZOR)	С	С	С	С	С
6.	Анализ воздействий (BIA)	С	С	С	С	С
7.	Анализ видов и последствий отказов	С	Н	В	С	В

	(FMEA)					
8.	Анализ дерева неисправностей (FTA)	H	C	C	B	B
9.	Анализ дерева событий (ETA)	B	B	B	B	B
10.	Попарный анализ «причина-последствие»	C	C	B	B	B
11.	Анализ уровней защиты (LOPA)	C	C	B	C	C
12.	Анализ дерева решений	B	C	C	B	C
13.	Анализ влияния человеческого фактора (HRA)	C	B	C	C	C
14.	Анализ «галстук-бабочка»	B	B	C	C	C
15.	Марковский анализ	B	B	C	B	B
16.	Матрица последствий и вероятностей	C	B	B	B	B
17.	Анализ эффективности затрат (CBA)	B	C	C	B	B
18.	Мультикритериальный анализ решений (MCDA)	B	C	B	B	B

Как следует из таблицы, для анализа рисков ИА имеется достаточно широкий набор приемлемых методов. Из общего количества N известных методов (N=31) для анализа ИА приемлемы восемнадцать, из них восемь методов могут использоваться практически для любых ИС и, соответственно, их компонентов, осуществляющих ИА. Выбор методов оценки рисков зависит от конкретных обстоятельств: масштаба и состава ИС, обрабатываемой в ней информации, состава и используемых средств аутентификации, наличия квалифицированных экспертов и т.д. В главах 2 и 3 приведены примеры анализа с применением перечисленных в таблице 1.5 методов.

1.6 Методы анализа надежности идентификации и аутентификации

Вопросы оценки надежности ИА пользователей активно обсуждаются специалистами, однако общепринятого научного подхода к исследованию этого весьма сложного процесса автору пока не выработано. Выполним краткий обзор способов исследования надежности и проанализируем их применимость для исследования аутентификации.

В рамках оценки надежности процессов ИА значительная часть исследований в последние два десятилетия посвящена надежности функционирования ИС. Для таких задач в условиях недостатка не только статистических данных, но и четко определенных состояний систем, наиболее развитыми оказались метод интервальных средних [134, 135] и социотехнический подход [136]. Существенный вклад в развитие методов оценок надежности внес последовательный ряд исследований, проведенных под руководством И.Б. Шубинского [35, 36]. В основном эти работы касаются разработки методов исследования **функциональной надежности** программного обеспечения, предложенные методы анализа в ряде случаев применимы и для рассмотрения процессов ИА [137]. Например, существует подход к анализу количества ошибок в ПО, которые приводят к частым сбоям и понижают надежность программного обеспечения. Для частоты появления ошибок стандартом [138] предлагается формула (1.1):

$$F = \frac{x - y}{n} \tag{1.1}$$

где F – частота появления ошибок;

x – количество неправильных строк программы, вычисляемой по модели надежности, выбранной главным конструктором;

y – количество строк программы, в которых ошибки выявлены и исправлены;

n – общее количество строк программного обеспечения.

Этим же стандартом предлагаются следующие шкалы оценок для значений появления ошибок:

$F < 10^{-4}$ – отлично,

$10^{-4} < F < 10^{-3}$ - хорошо,

$10^{-3} < F < 10^{-2}$ - удовлетворительно,

$F > 10^{-2}$ – плохо.

Существенная часть опубликованных результатов исследований надежности в области ИБ, как правило, носят отрывочный характер. Например, в работе [36] рассмотрены вопросы надежности защиты компьютерной информации от НСД. В работе показано, что применение теории надежности механизмов и машин «в лоб» приводит к результатам, не соответствующим практике. Этот результат объясняется тем, что применительно к процессам необходимо использовать не классическую теорию надежности (в современном языке называемую структурной надежностью), а функциональную надежность (ФН) [35].

Как показано в [137], ФН аутентификации напрямую связана с качеством реализации процессов как на стороне претендента, так и доверяющей стороны. Следовательно, в виде одного из методов исследования может быть применен процессный подход. При этом особое внимание необходимо уделять обеспечению доверенной среды. Выводом, полученным в этой работе, мы воспользуемся при рассмотрении ФН процессов ИА.

Исследование таких сложных процессов, как ИА, в котором кроме программного обеспечения, аппаратного обеспечения, системного и прикладного ПО, в нескольких типовых обязательных процедурах непосредственно участвует человек, не проводилось. В работе [139] показано, что утвержденных и общепризнанных научным сообществом моделей и методов исследования для процессов ИА пока нет. Также установлено, что для анализа надежности подобных процессов требуются новые подходы. Разработке таких подходов уделено особое внимание в настоящей работе.

ВЫВОДЫ ПО ГЛАВЕ 1

1.Анализ международных стандартов, отечественных и зарубежных научных работ по изучению и регулированию процессов идентификации и аутентификации пользователей государственных услуг, систем электронной коммерции и государственных предприятий показывает, что исторически первыми требования к идентификации и аутентификации для организации доступа пользователей к ИС на основе анализа рисков разработаны в США, где приняты стандарты, включающие в себя четыре уровня доверия к результатам идентификации и аутентификации, имеющие статус обязательных к исполнению государственными агентствами и их контрагентами. Канада, Австралия, ряд других стран лишь локализовали американские требования по безопасности аутентификации, которые де-факто являются наиболее проработанными. На основе стандартов ISO/IEC, американских стандартов и рекомендаций Международного союза электросвязи в последние 10 лет интенсивно разрабатываются и обновляются международные стандарты по идентификации и аутентификации в рабочих группах ISO и IEC. При этом последняя (2020 г.) версия одного из основных стандартов ISO/IEC 29115 полностью построена на американских стандартах NIST 800-63-3 и NIST 800-63-B издания 2017г. Тем не менее, опора на международные стандарты как наиболее полные и законченные документы, разработанные международным сообществом, позволяет вести научные разработки темы доверия к результатам идентификации и аутентификации с учетом достижений российских и зарубежных ученых и современной нормативно-правовой базы.

2.Анализ федеральных законов и подзаконных актов РФ показывает необходимость разработки **системы национальных стандартов по идентификации и аутентификации**, а также существенной модернизации отечественной нормативной базы по вопросам регулирования процессов идентификации и аутентификации. При разработке проектов федерального закона, подзаконных актов и сопутствующих регулирующих документов необходимо учитывать

научные разработки и мировой опыт. В частности, требуется нормативное введение уровней доверия к результатам идентификации и аутентификации в зависимости от результатов оценки рисков для тех или иных государственных информационных систем. При этом необходимо учитывать основные технологии идентификации и аутентификации, используемые или планируемые к применению в указанных информационных системах. Российская нормативная база по идентификации и аутентификации существенно отстает от международных стандартов, руководящих документов развитых стран. Необходимо разработать документы рекомендательного и исполнительного характера для обеспечения перспективы интенсивного развития программы «Цифровой экономики» на ближайшие годы с целью сокращения указанного отставания, что особенно актуально в связи с начавшейся интенсивной цифровизацией российской экономики. В отличие от рассмотренных международных стандартов в целях создания указанной нормативно-правовой базы необходимо разработка **критериев доверия** и научно обоснованных рекомендаций. Последняя задача особенно актуальна для объектов КИИ.

3.Анализ научных работ по безопасности и надежности идентификации и аутентификации показывает необходимость проведения системного исследования как системы идентификации и аутентификации целиком, так и глубокого анализа процессов и процедур, составляющих функционал систем идентификации и аутентификации. Установлено, что в качестве основного инструмента для проведения такого исследования должны лежать методы **анализа и управления рисками.**

4.Выявлена необходимость синтеза новых подходов к решению задач оценивания рисков идентификации и аутентификации, включающих в себя разработку **математических моделей, методик и алгоритмов** проведения соответствующих оценок. При этом нужно учитывать, что с увеличением количества зарегистрированных в ИС субъектов доступа системы идентификации и аутентификации кроме традиционных задач обеспечения конфиденциальности и целостности циркулирующей в системах информации должны удовлетворять

требованию обеспечения доступности, т.е. должны более строго подчиняться описанию в виде систем массового обслуживания, целостности программного обеспечения и конфиденциальности идентификационных данных пользователей.

5.Установлена потребность разработки новых подходов, методов и моделей, адаптированных к проведению анализа **функциональной надежности** работы систем идентификации и аутентификации как информационной подсистемы предприятия и основных процессов, происходящих на различных этапах идентификации и аутентификации.

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

7.Обоснована необходимость введения **уровней доверия** к результатам идентификации и аутентификации, использование которых может позволить существенно повысить эффективность управления доступом пользователей, в том числе в удаленном режиме, а также сократить сроки проектирования и ввода в эксплуатацию систем идентификации и аутентификации.

2 Методология формирования иерархии уровней доверия к результатам идентификации субъектов доступа

2.1 Общие положения. Этапы создания методологии

Под методологией будем понимать совокупность методов, способов реализации, которые представлены в виде последовательных этапов их применения для достижения основной цели: формирования иерархии уровней доверия к результатам идентификации субъектов доступа. Условно можно выделить четыре основных этапа развития методологии.

Первый этап – **аналитический**

1. Сбор информации. Источники:
    a. международные стандарты и НПА;
    b. результаты научных исследований (НИРы, статьи, научные семинары, форумы, научно-практические конференции);
    c. отечественные стандарты и НПА.
2. Анализ собранной информации
    a. Идентификация процессов [128], ролей, участников обмена идентификационной (ИИ) и аутентификационной информацией (АИ), особенностей ЖЦ ИИ и АИ [140,141,142,143,144];
    b. Выполнение аналитических обзоров международных стандартов [1,2, 3], международной НПА [145];
    c. Определение применения биометрии в ИА [146, 147];
    d. Классификация технологий и средств ИА [130, 131], задач аутентификации, систем ИА [132];
    e. Анализ применимости известных методов исследования к решению поставленной научной темы [82, 148, 133, 149]
3. Синтез концепции исследования уровней доверия к результатам ИА [**Ошибка! Закладка не определена.**, 139, 150, 151].
4. Формулирование научной проблемы.
5. Определение цели и задач исследования.

Второй этап – **методический**

1. Определение стратегии достижения цели.
2. Конкретизация плана решения вытекающих из цели задач – доверие определяется характеристиками: достоверность, надежность и безопасность [151].
3. Системный подход: в основе исследования достоверности, надежности и безопасности лежит анализ рисков [133, 152] (см. раздел 1.3).
4. Формулирование показателей и критериев [153, 154, 155]
5. Определение объекта и предмета, а также основного инструмента исследований.

Третий этап. **Разработка**

1. Идентификация типовых угроз, атак и рисков [156, 157, 67, **Ошибка! Закладка не определена.**,158].
2. Разработка многоуровневой модели исследования рисков идентификации и аутентификации [159, 160].
3. Разработка моделей [161, 162, 163], способов [164, 165, 166] и алгоритмов исследования [151].
4. Формирование иерархии доверия к результатам идентификации и аутентификации [167,150,153]

Четвертый этап. **Анализ результатов**

1. Подведение итогов, уточнение методологии, разработка оценки достигнутого уровня доверия [**Ошибка! Закладка не определена.**]
2. Решение прикладных задач с применением основных положений методологии
3. Постановка будущих задач в развитие созданной методологии
4. Выработка рекомендаций.

В наглядной форме этапы развития методологии формирования иерархии уровней доверия представлены на рис. 2.1.

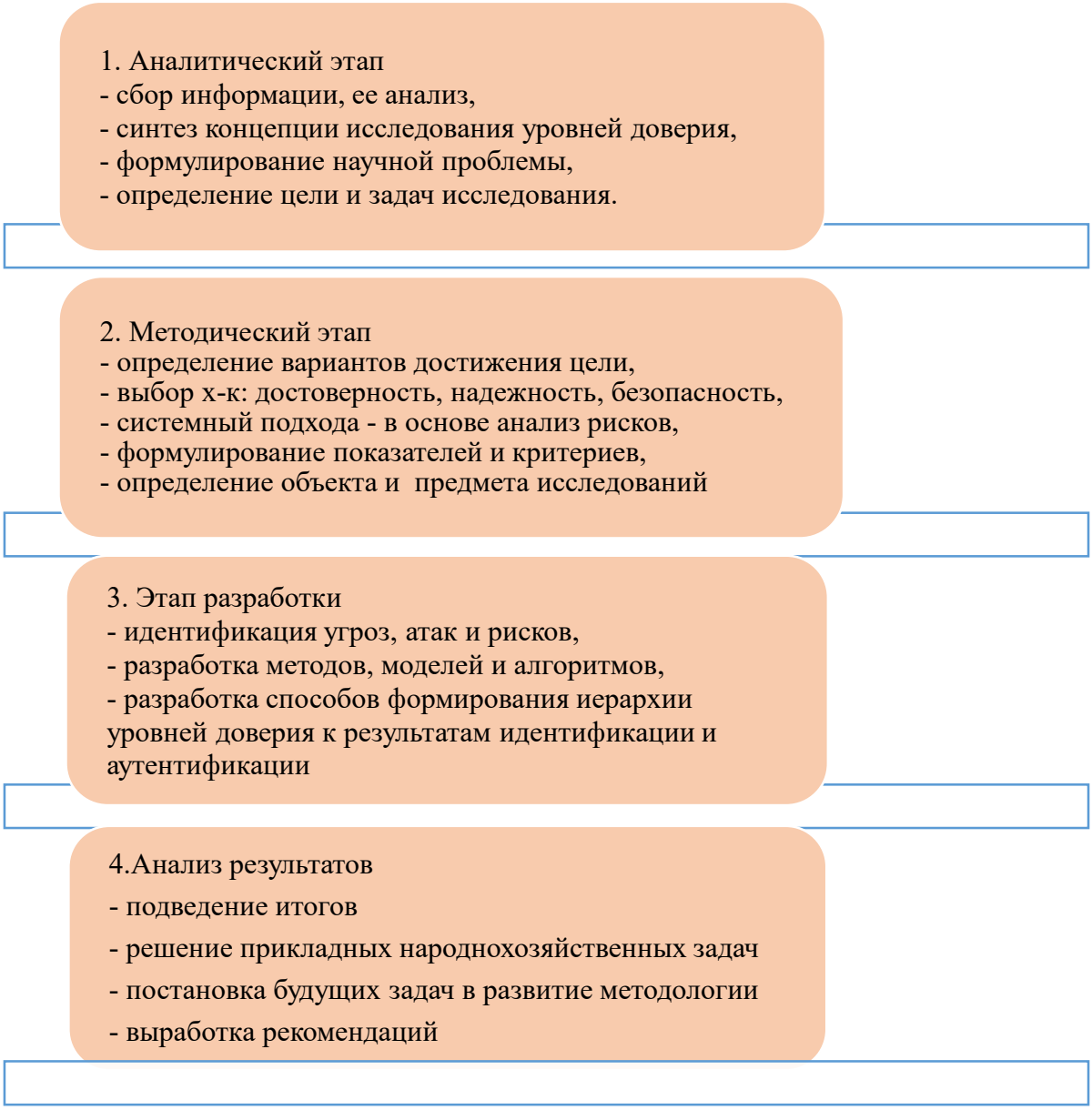

Рисунок 2.1 – Основные этапы создания методологии

Согласно результатам анализа, проведенного в первой главе, для исследования доверия к результатам идентификации необходимо определить характеристики процесса идентификации, позволяющие с помощью оценки рисков установить определенный уровень доверия к результатам. В качестве таких характеристик установлены функциональная надежность работы системы идентификации, достоверность первичной идентификации и безопасность персональных данных, которые хранятся и обрабатываются в процессе работы СИА. Предлагаемая методология представлена на рис.2.2

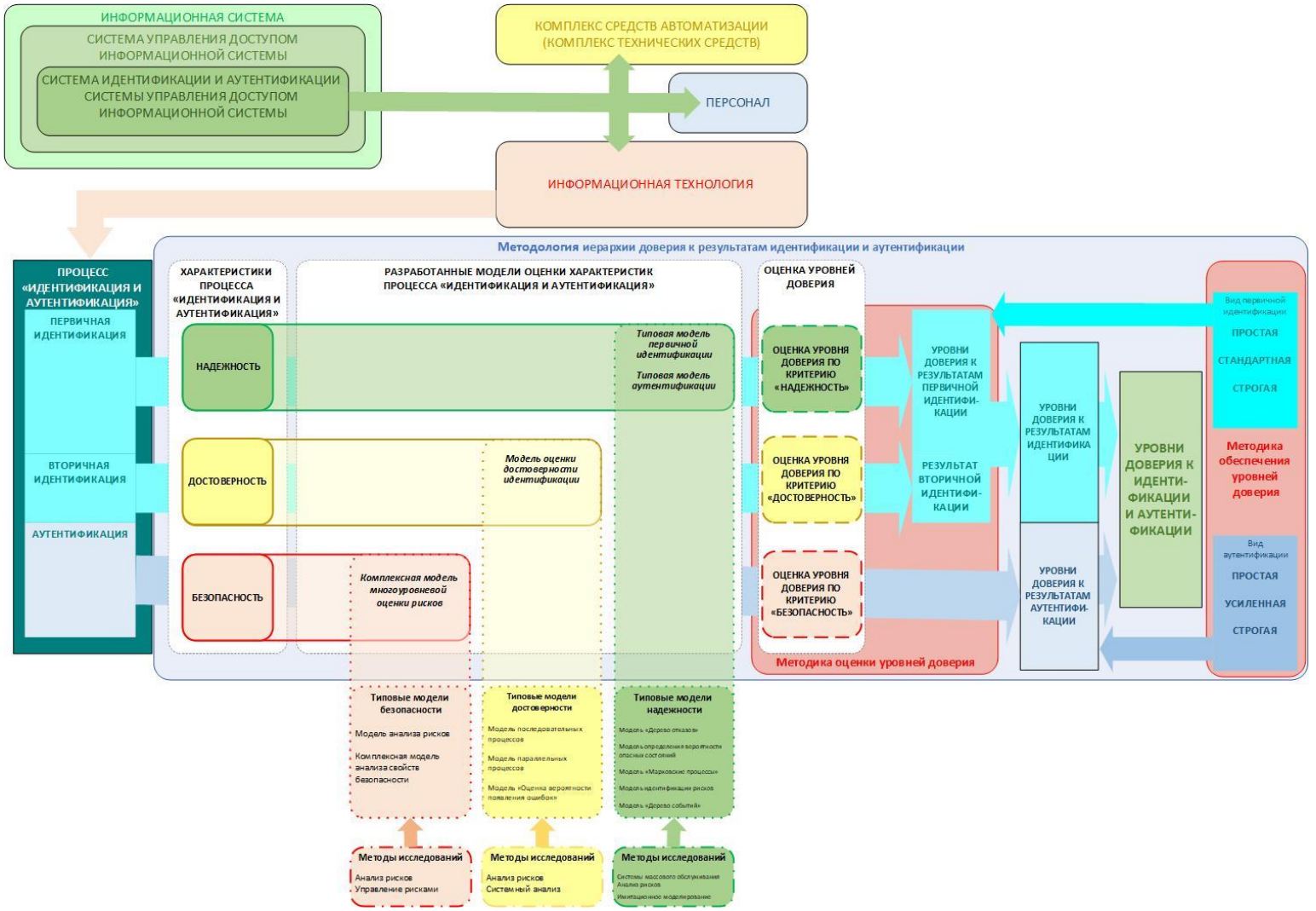

Рисунок 2.2 - Методология формирования иерархии доверия к результатам идентификации и аутентификации

Чтобы перейти к оценке уровней доверия к результатам идентификации (УДИ), сначала рассмотрим основные характеристики процесса идентификации субъекта доступа, участников процесса идентификации, возникающие при этом основные угрозы и риски. При этом согласно выводам, сделанным в первой главе, будем опираться прежде всего на международные стандарты.

2.2 Основные характеристики процесса идентификации субъектов доступа

Рассмотрим риски электронной идентификации граждан. В отчете Генеральной Ассамблеи ООН, опубликованном в 2011 г., отмечены следующие риски удаленной идентификации в целях доступа к информационным и платежным ресурсам:

– идентификация субъектов доступа – риск недостоверности собранной и подтверждённой ИИ о субъектах;

– удостоверение подлинности (ассоциация заявленных идентификационных данных с реальным субъектом) – риск возникновения ошибок первого и второго рода;

– конфиденциальность – риск раскрытия, несанкционированного или ненадлежащего использования ИИ личности;

– защищённость данных - риск возможного получения неуполномоченной стороной доступа к личным данным физических лиц;

– риск ответственности – правовая неопределённость в отношении ответственности, возникающая в связи с действием или бездействием со стороны участника системы идентификации;

– обеспечение надежности – взыскание убытков в случае сбоев и ошибок;

– риск несоблюдения нормативных положений – соблюдаются ли юридические требования по тщательной идентификации личности, получившей доступ, например, к банковским счетам и платёжным механизмам.

Рассмотри первые два риска подробнее. ИИ, поступающая от новых

пользователей любой ИС, должна быть верифицирована. Процедура регистрации может приводить к созданию одного или более идентификаторов зарегистрированного нового пользователя. Созданная ИИ заносится в хранилище в качестве зарегистрированного в домене идентификационного атрибута. В целях предоставления доступа к информационным ресурсам за процедурой идентификации следует процедура аутентификации, которая тесно связана с идентификацией. Целью аутентификации является подтверждение подлинности представленного идентификатора и проверке принадлежности идентификатора и аутентификатора конкретному субъекту.

Успешная аутентификация субъекта в конкретной ИС на некотором уровне доверия позволяет заинтересованным сторонам получить уверенность в том, что результат верификации является корректным и пригоден для использования. Уровни доверия к результатам аутентификации определяет международный стандарт [59].

Система менеджмента идентификационных атрибутов, соответствующая [61, 63], должна определять для каждого из своих процессов аутентификации:

– политики верификации ИИ;

– механизмы установления действительности (validity) и правильности аутентифицированных идентификационных атрибутов;

– срок действия аутентифицированных идентификационных атрибутов;

– механизмы журналирования и аудита, этапы обработки и результаты обработки.

Система менеджмента идентификационных атрибутов должна определять механизмы сохранения целостности и достоверности хранящихся в ней атрибутов.

Рассмотрим подробнее процесс идентификации.

Идентификация включает первичную идентификацию (ПИ), однократно

проводимую в момент регистрации нового пользователя, и вторичную идентификацию (регулярно повторяющуюся), выполняемую при каждом новом запросе на доступ.

ПИ физических лиц может являться одновременно частью как процесса идентификации, так и процесса аутентификации (если вслед за процессом идентификации осуществляется процесс аутентификации).

Целью ПИ является присвоение физическому лицу доступа идентификатора, являющегося уникальным в конкретной ИС и однозначно определяющим соотнесенную с ним ИИ. По сути, ПИ должна ответить на вопрос, то ли это физическое лицо, за кого себя выдает. Уровень и глубина проверки предоставленной физическим лицом ИИ определяется правилами регистрации нового пользователя, принятыми в данной ИС.

ПИ субъектов доступа - физических лиц должна завершаться регистрацией ИИ и присвоением уникального идентификатора доступа или обоснованным отказом. Причиной отказа в регистрации может являться недостаточный объем представленной физическим лицом ИИ или отсутствие ее подтверждения. При необходимости возможна регистрация физического лица, для которого подтверждение содержания ИИ при ПИ не осуществлялось. При этом ему присваивается уникальный идентификатор, но само физическое лицо определяется как «аноним».

Классификация идентификаторов, присвоенных субъекту доступа при регистрации

Рассмотрим основные идентификаторы, присваиваемые субъекту доступа при регистрации в ИС.

К первой группе отнесём свойства идентификаторов как характеристик принадлежности (собственности): универсальный (У), формируемый и выдаваемый на федеральном уровне, корпоративный (К) и личный (Л).

Ко второй группе отнесём свойство идентификаторов распознавать личность владельца: анонимный (Х) или персональный (П).

Третья группа свойств идентификаторов характеризует доступ владельца к ресурсам: одноразовый (О) или многоразовый (М).

Анализ показывает, что в физическом и виртуальном мире из 12 возможных реализуется всего 7 комбинаций (Таблица 2.1).

Таблица 2.1 – Классификация систем идентификации по трем свойствам, характеризующим идентификаторы пользователя

	Типы систем идентификации						
виды идентификаторов	1	2	3	4	5	6	7
универсальный (У), корпоративный (К), личный (Л)	У	У	У	К	К	К	Л
анонимный (Х) или персональный (П)	УХ	УП	УП	КХ	КХ	КП	ЛП
доступ одноразовый (О) или многоразовый (М)	УХМ	УПО	УПМ	КХО	КХМ	КПМ	ЛПМ
аналог (пример) в реальном (физическом) мире	деньги	запись в ЗАГСе	паспорт	билет в кино	абонемент	Бумажный пропуск	биометрия
виртуальный (электронный) пример	анонимный пользователь Интернета	генератор ОТР	реестр ИНН, СНИЛС	электронный билет	пополняемая карта	смарт-карта с цифровым сертификатом в виде пропуска	биометрия на карте или сервере

Приведём несколько примеров, использующих комбинации вышеперечисленных свойств идентификаторов. Так, УХМ означает универсальный анонимный идентификатор многоразового действия. В физическом мире это может быть купюра установленного образца (деньги). Денежный знак анонимен, принимается везде (универсален). Опустив монетку в монетоприемник, можно пройти в трамвай, вестибюль метро (в недавние времена), на аттракцион, в туалет и т.п. В виртуальном мире такому способу идентификации «аноним»

соответствуют платные услуги, не требующие идентификации пользователя, например, приобретение билетов в кино или театр.

УПМ. Аналогом такого пропуска в бумажном мире является удостоверение личности, оформленное уполномоченным федеральным органом. Это может быть гражданский паспорт, лицензия на право управления транспортным средством (права), военный билет и т.п. В цифровом мире документу, принимаемому везде, также будет соответствовать идентификатор, содержащийся в базах данных (реестрах) федерального уровня. Примерами являются ИНН, СНИЛС, электронный паспорт, полис ОМС и т.п.

Примером КПМ (корпоративного персонального многоразового идентификатора) в физическом мире является бумажный пропуск на территорию учреждения или организации, в электронном мире такому идентификатору соответствует USB-ключ или смарт-карта, содержащая цифровой сертификат доступа и выполненная в виде пропуска в корпоративном исполнении. Присвоенный в корпоративной информационной системе идентификатор содержится в цифровом сертификате доступа в поле «уникальный идентификатор субъекта». По мере развития программы «Цифровая экономика» количество КПМ будет расти. КПМ могут быть отраслевыми. К началу 2020 г. институты кредитно-финансовой отрасли (КФО) близки к решению о введении единообразного идентификатора для всех участников взаимодействия в КФО.

Процесс первичной идентификации. ПИ нового пользователя ИС проводится в несколько этапов. На первом этапе заявитель предъявляет ИИ. На втором этапе достоверность ИИ и степень ее связанности с заявителем должны быть проверены. В случае положительных результатов проверок на третьем этапе в ИС регистрируется новый пользователь, которому присваивается уникальный идентификатор для данной ИС, а связанная с ним ИИ и результаты проверок заносятся в хранилище.

На основе анализа рекомендаций [61, 63] определим основные составляющие процесса идентификации:

а) предъявление претендентом идентификационных атрибутов регистрирующей стороне (регистратору);

б) проверка регистратором предъявленной ИИ;

в) сбор подтверждающей ИИ;

г) верификация предъявленной ИИ на предмет достоверности, т.е. определение того, что идентифицирующие атрибуты соответствуют необходимому уровню подтверждения идентификационных данных, который должен быть достигнут;

д) валидация ИИ и определение степени связанности ИИ субъекта с заявленными идентифицирующими атрибутами.

е) принятие решения о достаточности и достоверности ИИ;

ж) внесение субъекта в реестр: присвоение уникального идентификатора и способа (способов) предъявления секрета (если регистрация предназначена для предоставления в последующем доступа к информационным ресурсам) новому пользователю данной ИС.

Таким образом, в процессе идентификации участвуют несколько взаимодействующих сторон: заявитель (претендент на право стать пользователем), регистратор, принимающий от претендента ИИ, делающий запросы в целях верификации полученной ИИ в уполномоченные органы для получения от них официальных подтверждений (свидетельств), а также принимающий решение об уникальности, достоверности и достаточности полученной таким образом ИИ и степени связанности данной ИИ с личностью заявителя для того, чтобы зарегистрировать его в качестве нового пользователя ИС. При этом заявитель и регистратор являются активными участниками информационного взаимодействия, а уполномоченные органы – пассивными, поскольку информация от них получается регистратором только по его запросу. Степень уверенности регистратора в достоверности и надежности результатов процесса идентификации напрямую зависит от условий и правил выполнения действий а) – ж). Для более глубокого понимания этого утверждения рассмотрим весьма важное понятие уровней доверия к результатам идентификации.

2.3 Понятие уровней доверия к результатам идентификации

Доверие к результатам идентификации является в определённой мере гуманитарно-философским понятием, поскольку согласно [168] измеряется не количественными показателями, а затраченными усилиями и вполне определёнными действиями.

Если определять коротко, то доверие к результатам идентификации личности заявителя определяется качеством идентификации и соблюдением в процессе идентификации требований безопасности. Что понимается под качеством идентификации? Прежде всего, это надёжность и достоверность полученных результатов. Доверие к идентификации в значительной степени определяется степенью связанности характеристик идентификации (идентификационных атрибутов) с конкретным физическим лицом. Для этого используется система подтверждений.

Доверие к результатам первичной идентификации (ПИ) требуется для установления доверенных отношений с взаимодействующими объектами, и предоставления доступа к их услугам [169]. При этом уровни доверия к ИИ должны соотноситься с уровнями риска предоставления доступа или отказа в доступе. Согласно [63] доверие к результатам ПИ может достигаться различными способами. Поскольку целью ПИ является установление (подтверждение) соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными, то есть установление регистратором факта того, что субъект является тем, за кого себя выдает, в процессе регистрации для конкретной среды функционирования каждый субъект (объект) доступа должен иметь единственный (уникальный) набор значений идентификационных атрибутов, связанный с присвоенным при регистрации идентификатором доступа, что обеспечивает однозначную идентификацию данного субъекта (объекта) доступа. Кроме уникальности набора идентификационных атрибутов доверие к результатам ПИ зависит от результатов проверки их существования в электронных реестрах, их актуальности и достоверности путем вери-

фикации и получения свидетельств, а также установить связь между субъектом (объектом) доступа и предъявленными идентификационными данными. Доверие к результатам ПИ может в значительной степени зависеть от надёжности поставщика (источника) ИИ (примером источника ИИ является уполномоченное должностное лицо МВД, отвечающее за актуальность электронного реестра паспортов). При этом первичную запись в указанный реестр, как правило, выполняет отделение МВД, выдавшее паспорт заявителю и сделавшее соответствующую запись в реестр паспортов МВД. Аналогично источником ИИ является электронный реестр ИНН в системе ФНС для предъявленного ИНН и реестр ПФР для СНИЛС. Если источник ИИ не является надёжным, то предъявленные заявителем идентификационные атрибуты должны быть подтверждены (заверены) другим поставщиком ИИ, который является надёжным источником. Роли сторон и процессы подтверждения идентификационной информации подробно описаны в стандарте [170]. Кроме того, доверие к результатам идентификации может достигаться с помощью механизмов аутентификации, поскольку одной из задач аутентификации является подтверждение идентификационной информации. Для обеспечения подлинности ИИ используется механизм представления свидетельств идентичности, которые разделяются на официальные свидетельства, получаемых из надёжных источников и подтверждающие свидетельства.

Официальные свидетельства являются подтверждениями для установления идентичности, полученными из государственных баз данных (электронные реестры в базах данных МВД, ПФР, ФНС - как показано в примерах выше), достоверность данных в которых определяется НПА и контролируется в соответствии с текущим законодательством [154].

В случаях, когда для идентификационного атрибута доступ к официальным свидетельствам отсутствует или необходимость в них для требуемого уровня подтверждения идентификационных данных отсутствует, риск может быть уменьшен путем верификации подтверждающих свидетельств.

Свидетельство идентичности, как правило, включает:

– подтверждающую информацию, предоставляемую физическим лицом (заявителем);

– свидетельство, содержащее подтверждающую информацию или связанное с подтверждающей информацией физического лица;

– информацию о хранилищах, содержащих подтверждающую информацию субъекта;

– подтверждающую информацию, предоставленную другими известными источниками.

Таким образом, доверие к результатам ПИ согласно международным стандартам [61, 63, **Ошибка! Закладка не определена.**] и национальным стандартам [168, 171] определяется выполнением требований к ПИ при регистрации нового пользователя системы. Требования должны включать в себя уникальность предъявленного набора идентификационных атрибутов, доказательства их существование в электронных официальных реестрах или выполнение правил их подтверждения с помощью свидетельств идентичности, а также установление связи проверенных регистратором электронных идентификационных данных (цифрового профиля) с личностью заявителя.

Стандарты [61, 63, 171] определяют три уровня доверия к результатам идентификации физических лиц: низкий, средний, высокий.

Для **низкого** уровня доверия к результатам ПИ характерен низкий уровень уверенности в заявленной или предъявленной ИИ физического лица. При этом ИИ должна быть уникальной в конкретной ИС, а физическое лицо считается предположительно привязанным к ИИ, поскольку требований к проверке связи ИИ с личностью субъекта не предъявляется. На первом уровне доверия также не предъявляется требований к верификации ИИ.

Для **среднего** уровня доверия характерна средняя уверенность в предъявленной ИИ. При этом ИИ должна быть уникальной в конкретной ИС, а у физического лица должна быть некоторая привязка к ИИ, поскольку требованием к проверке привязки является использование одного фактора из трех возможных (знание, владение, обладание биометрическими особенностями). На

втором уровне доверия необходимо верифицировать идентификационные атрибуты в подтверждающих свидетельствах.

Для **высокого** уровня доверия к результатам ПИ обязательна высокая уверенность в заявленной или предъявленной ИИ. При этом ИИ должна быть уникальной в конкретной ИС, а у субъекта должна быть сильная привязка к ИИ, поскольку требованием к проверке привязки является использование не менее двух факторов из трёх возможных (знание, владение, обладание биометрическими особенностями). На третьем уровне доверия верифицировать идентификационные атрибуты в официальных свидетельствах необходимо обязательно. Систематизация вышеизложенного представлена в таблице 2.2

Таблица 2.2 – Общая характеристика уровней доверия к результатам первичной идентификации

Первичная регистрация субъекта (объекта) доступа			Необходимость подтверждения идентификационных данных	Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным	Уровень доверия к результатам первичной идентификации	Возможность регистрации субъекта (объекта) доступа
Уникальность идентификационной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных	Привязка идентификационных данных				
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Не рассматривается	Не рассматривается	Не рассматривается	Отказ в регистрации субъекта (объекта) 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 заверяется подтверждающими свидетельствами	Привязка с использованием одного фактора	Необходимо подтверждение	Умеренная уверенность	Средний уровень доверия	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование подтверждается официальными свидетельствами	Привязка с использованием двух и более факторов	Необходимо подтверждение	Значительная уверенность	Высокий уровень доверия	Регистрация субъекта (объекта) доступа

Подтверждение ИИ представляет собой процесс верификации идентифицирующих атрибутов, которые будут вводиться в систему менеджмента ИИ, и установления того, что идентификационные атрибуты относятся к физическому лицу, которое будет зарегистрировано в ИС.

Подтверждение идентификационных данных включает:

– определение порядка и правил подтверждения ИИ;

– определение состава подтверждения ИИ, границ и условий, в которых будет осуществляться взаимодействие физического лица и его ИИ;

– определение идентификационных атрибутов, которые нужно получить и подтвердить;

– определение вспомогательных атрибутов, получение которых будет осуществляться для подтверждения ИИ;

– установление уровня подтверждения ИИ, который необходим для регистрации идентификационной информации в ИС.

При каждом подтверждении ИИ осуществляется:

– сбор подтверждающей информации и определение подлинности полученных идентификационных атрибутов;

– определение соответствия полученных идентификационных атрибутов необходимому уровню подтверждения ИИ, который должен быть достигнут;

– привязка физического лица к предъявленным идентификационным атрибутам.

Стандарт [61] и отечественный ГОСТ Р 58833 определяют три уровня **доверия** к **подтверждению** ИИ.

Первый уровень подтверждения ИИ характеризуется низкой уверенностью в заявленной или представленной ИИ. На этом уровне имеется предположение о существовании уникального набора ИИ и существовании привязки физического лица к ИИ.

Второй уровень подтверждения ИИ характеризуется средней уверенно-

стью в заявленной или представленной ИИ. На этом уровне имеется умеренный уровень подтверждения ИИ и существует некоторая привязка физического лица к ИИ.

На третьем уровне подтверждения ИИ должна быть достигнута высокая уверенность в предъявленной ИИ. У субъекта должно быть строго подтверждено существование ИИ и существует сильная привязка к ИИ.

Привязка электронных идентификационных данных к конкретной личности может осуществляться в удаленном режиме или при личном общении. При этом в качестве механизмов привязки ИИ могут использоваться следующие факторы:

– фактор знания (что-то, что субъект знает): привязка устанавливается с использованием информации, не являющейся общедоступными сведениями. Это может включать верификацию относительно свидетельств идентичности, отличных от предоставленных свидетельств.

– фактор владения (что-то, чем субъект обладает): привязка устанавливается с использованием фактических (документальных) свидетельств, содержащих ИИ, которая будет верифицироваться относительно свидетельства идентичности.

– биометрический фактор (что-то, что свойственно субъекту, или что-то, что субъект обычно делает): привязка устанавливается путем сопоставления биологической или поведенческой характеристики с эталонной.

Таким образом, на первом уровне подтверждения ИИ привязка физического лица к его ИИ не требуется. Это означает, что физическое лицо может предъявить ИИ другого физического лица. На втором уровне подтверждения ИИ необходимо проверить привязку ИИ к физическому лицу, используя один из перечисленных факторов. На третьем уровне подтверждения необходимо обязательно проверить привязку ИИ к физическому лицу, используя не менее 2 различных факторов. Стандарт [170] предупреждает, что использование фактора знания рекомендуется применять не более одного раза.

Целью вторичной идентификации является распознавание пользователя,

запросившего доступ к ресурсам АИС. При этом должна выполняться проверка существования идентификатора, предъявленного пользователем, в перечне идентификаторов, присвоенных при первичной идентификации. При совпадении предъявленного и зарегистрированного идентификаторов процесс вторичной идентификации считается успешно пройденным и управление передается в блок аутентификации.

Обобщение изложенного в данном параграфе процесса идентификации согласно рассмотренным международным стандартам приведено в таблице 2.3.

Таблица 2.3 – Общая характеристика уровней доверия к результатам идентификации

Первичная идентификация субъекта (объекта) доступа			Вторичная идентификация субъекта (объекта) доступа	Уверенность в том, что субъект (объект) доступа соответствует идентификационной информации	Уровень доверия к результатам идентификации субъекта (объекта) доступа
Соответствие заявленных идентификационных данных требованиям к первичной идентификации	Подтверждение заявленных идентификационных данных	Возможность регистрации субъекта (объекта) доступа			
Не соответствуют	–	Отказ в регистрации субъекта (объекта) доступа	–	–	–
Не соответствуют	Не подтверждаются	Регистрация субъекта доступа как анонима	Выполнена успешно	Уверенность отсутствует	Не достигнут низкий уровень доверия
Соответствуют	Не подтверждаются	Регистрация субъекта (объекта) доступа	Выполнена успешно	Некоторая уверенность	Низкий уровень доверия
Соответствуют	Подтверждаются	Регистрация субъекта (объекта) доступа	Выполнена успешно	Умеренная уверенность	Средний уровень доверия

Соответствуют	Подтверждаются официально	Регистрация субъекта (объекта) доступа	Выполнена успешно	Значительная уверенность	Высокий уровень доверия

Применение биометрических характеристик в процессах идентификации

Несмотря на обилие международных нормативных документов, регулирующих процессы ИА с применением биометрии, вопросы достоверности идентификации личности по биометрическим признакам еще до конца не изучены. Обычно при сравнении методов идентификации рассматривают только точность самой технологии идентификации (опираясь на значения, заявленные производителем). В отличие от такого подхода в данной работе процедура идентификации рассматривается в виде процесса принятия решения класса "да/нет" с учётом возможных погрешностей и ошибок, как при первичной регистрации идентификаторов объектов, так и непосредственно в процессе идентификации.

Все биометрические методы основаны на вероятностных и статистических методах. Надёжность методов может оцениваться несколькими способами, в наиболее распространённом подходе в качестве основных характеристик можно принять ошибки первого и второго рода. Ошибка первого рода (FRR - False Rejection Rate) – это вероятность ложного отказа в доступе пользователю, имеющему право доступа. Ошибка второго рода (FAR - False Acceptance Rate) – это вероятность ложного доступа, когда система ошибочно опознает чужого как своего. Одним из критериев работы системы может являться подход, заключающийся в следующем: система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется сравнительная характеристика EER, определяющая точку пересечения графиков FRR и FAR.

Основными методами, использующими статические биометрические характеристики человека, являются идентификация по папиллярному рисунку

на пальцах, по радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. Также существует семейство методов, использующих динамические характеристики: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке. Более 50% промышленных решений, разработанных мировым сообществом по идентификации личности с применением биометрических методов, занимают продукты по идентификации с помощью отпечатка пальца, около 20% – по геометрии лица, на все остальные технологии приходится около 30%.

Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. Ряд биометрических технологий находится в стадии разработки, некоторые из них считаются весьма перспективными. К ним относятся технологии на основе термограммы лица в инфракрасном диапазоне излучения, характеристик ДНК, клавиатурного почерка, анализа структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи), анализа отпечатков ладоней, формы ушной раковины, характеристик походки человека, индивидуальных запахов человека, распознавания по расположению вен. Оценки качества работы ряда перспективных систем приводятся в [172], а обоснованность принятия вариативного решения (идентификация личности по анализу ДНК) приводится в [173]. Рассмотренный в работе [147] подход к анализу идентификации позволяет оценить достоверность и надёжность различных методов биометрии в сравнении с другими методами идентификации. Как показано в работе, применение биометрии не решает проблем надежности идентификации для систем с большим количеством пользователей, но может повысить достоверность идентификации субъектов при организации доступа к системам с числом пользователей, измеряемым сотнями, а также к критически важным системам как часть системы контроля и управления физическим доступом или в качестве дополнительного фактора аутентификации.

Установлено, что промышленная готовность, надёжность и функцио-

нальная устойчивость работы средств биометрической идентификации в целом пока не слишком высока, а достоверность идентификации личности – одного порядка с широко применяемыми в качестве идентификаторов СНИЛС, ИНН и т.д. Для систем с большим числом зарегистрированных пользователей применимость биометрии вызывает сомнения из-за невысокой точности идентификации, существенного увеличения времени отклика с ростом числа зарегистрированных в системе субъектов и большой стоимости. Для широкого класса систем биометрическая идентификация пригодна к использованию как усиление защиты (третий фактор аутентификации) или в качестве устройств, работающих на территории контролируемой зоны в специально отведённых зонах (как часть СКУД).

Международные стандарты не рекомендуют использование биометрических характеристик в виде основного фактора для идентификации, их можно использовать только как вспомогательные в силу ряда ограничений на их применение.

Как уже указывалось выше, биометрические характеристики имеют вероятностную природу, процедура сравнения предъявленной характеристики с эталонным образцом в стандарте [174] рекомендуется проводить не на сервере, а локально. В материалах WG5 подкомитета ISO SC 27 установлено, что сравнение лучше производить по типу "один к одному" (1:1). Идеально для этого подходит личный HSM, например, в виде смарт-карточного чипа, выполненного по технологиям Privacy by Design и Security by design одновременно. В крайнем случае, сравнение может выполняться на компьютере, но вероятность атак на такой компьютер необходимо тщательно просчитывать. Статистика говорит о том, что базы данных биообразцов часто подвержены атакам.

Так, в стандарте [175] указано:

– биометрическая характеристика False Match Rate (FMR) не обеспечивает конфиденциальности в процессе аутентификации. Также FMR не обеспечивает защиту от спуфинга (когда злоумышленник выдает себя за легального

пользователя);

– биометрическое сравнение имеет вероятностную природу и впрямую одна только биометрия не может быть применена к аутентификации, поскольку для аутентификации необходим детерминированный ответ;

– для применения «чистой» биометрии в процессах идентификации и аутентификации для задач управления доступом международные стандарты только создаются, поскольку эти технологии и методы пока не имеют широкого применения;

– биометрическая характеристика сама не содержит секрет и неспособна генерировать секрет. Для аутентификации секрет как способ подтверждения предъявленных идентификационных данных необходим.

– базы данных, содержащие биометрические характеристики, подвержены простым атакам, особенно базы образцов.

Учитывая вышеизложенное, можно сделать следующие промежуточные выводы:

– биометрия для идентификации может использоваться только в дополнение к другим идентификационным атрибутам (например паспорт, СНИЛС, ИНН). «Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентифицирующих атрибутов» [174, раздел B4], при этом уровень доверия к результатам биометрической идентификации не может быть высоким ввиду отсутствия официальных подтверждений и вероятностной природы биометрии;

– биометрия может использоваться для предотвращения дублирования записи, связанной с конкретным субъектом, в реестре (сравнение биометрического образца субъекта с другими биометрическими образцами в контексте обнаружения и предотвращения дублирования. Собранная биометрическая информация должна быть достаточной и эффективной для исключения дублирования идентификационных данных [174, п.4.8];

– в процессе подтверждения идентификационных данных биометрические данные могут быть применены с целью обнаружения попыток субъекта

сделать заявки на множественные регистрации с различными идентификационными данными или сделать заявку на регистрацию с идентификационными данными другого субъекта;

– биометрия может использоваться для установления привязки идентификационной информации к конкретной личности: привязка устанавливается путем сопоставления биологической или поведенческой характеристики, наблюдаемой подтверждающей стороной, с эталонной биометрической информацией, которая, как известно, соответствует субъекту [174, раздел 5.5];

– биометрия может успешно применяться для обеспечения неотказуемости субъекта от факта регистрации, особенно в случае ведения видеозаписи процесса регистрации с проведением снятия биометрических характеристик субъекта.

Таким образом, международные стандарты [61, 63, 174 - **Ошибка! Закладка не определена.**] рекомендуют использование биометрии в целях идентификации субъектов дозированно.

Критика рассмотренного подхода, изложенного в международных стандартах

Таким образом, в международных стандартах для получения уверенности в том, что заявитель является тем, за кого себя выдает, рекомендуется сначала проверить на уникальность совокупность предъявленных им идентификационных атрибутов, затем проверить их существование в официальных реестрах, регистрах и кадастрах, верифицировать их с целью получения подтверждения их значений из официальных источников, затем убедиться в том, что полученные в результате подтвержденные цифровые идентификационные данные принадлежат данному субъекту (связаны непосредственно с ним). Указанная логическая цепочка действий не вступает в противоречие с действующим законодательством Российской Федерации и может быть принята за основу при построении и получения доверия к результатам типовых бизнес-процессов первичной идентификации субъектов доступа.

Однако при этом некоторые существенные моменты остаются за кадром. Например, проблема оценки рисков, связанных с идентификацией субъекта, стремящегося стать новым пользователем, переносится на организации. Так, согласно [63] процесс идентификации должен строиться на основе следующих принципов:

- риски, связанные с использованием идентификационных атрибутов субъекта, должны быть оценены и обработаны в степени, необходимой для их принятия;
- ИИ должна быть верифицирована для обеспечения достаточного уровня уверенности в ее достоверности и надежности для целевого использования;
- для целей идентификации физических лиц не должно собираться ИИ больше, чем это минимально необходимо.

Первый принцип согласуется с положениями стандартов серии ISO/IEC 270XX, второй – с целевой функцией процесса идентификации, третий отвечает требованиям 152-ФЗ «О защите персональных данных». При этом для организаций Российской Федерации в отсутствие утвержденных методик оценки рисков выполнение первого принципа уже может представлять существенные затруднения. Для разрешения этой проблемы рассмотрим основные угрозы и риски идентификации.

2.4 Угрозы и риски идентификации

Как упоминалось выше, идентификация разделяется на первичную, проводимую однократно в процессе регистрации, и вторичную, которую зарегистрированный в информационной системе пользователь проходит при каждой попытке доступа. Сначала рассмотрим угрозы первичной идентификации, потенциально возникающие в процессе регистрации.

Напомним, что участниками обмена информацией в процессе регистрации являются заявитель, регистратор, проверяющая сторона.

Основываясь на анализе международных стандартов [57-63], из общего пространства угроз выделим типовые угрозы, относящиеся к участникам процесса регистрации, рассмотренным в работе [154].

Так, со стороны **заявителя** возможны угрозы «маскарада» - попытки идентификации под чужим именем и последующий отказ от факта регистрации. В таблице 2.4. приведены варианты указанных угроз и методы их парирования из работы автора [158].

Таблица 2.4. - Угрозы, связанные с регистрацией, со стороны заявителя

Угроза/Атака	**Примеры**	**Методы парирования**
Фальсифицированное свидетельство подтверждения идентификационных данных	Заявитель предоставляет неверные идентификационные данные, используя поддельные документы, например, паспорт.	Проверка подлинности свидетельства. Верификация свидетельства. Запрос в орган, издавший свидетельство.
Мошенническое использование идентификационных данных другого лица	Заявитель предъявляет чужие документы, например, паспорт.	Сличение фотографии на официальном свидетельстве с заявителем. Ведение видеозаписи процесса регистрации.
Отрицание регистрации	Пользователь отрицает регистрацию, заявляя, что он не регистрировался в данной информационной системе.	Ведение видеозаписи процесса регистрации. Запись биометрических характеристик заявителя во время регистрации. Протоколирование и хранение записей согласно требованиям закона.

Перечислим типовые угрозы действиям **регистратора**:

- недостоверность собранной на основе предъявленной заявителем информации;
- недостоверность подтвержденной информации на основе предъявленной заявителем информации – один из самых опасных случаев мошенничества, когда заявитель представляет проверенные данные другого лица как свои, а регистратор получает и принимает их;
- угроза раскрытия личной информации пользователей (ПДн). Злоупотребления личной идентификационной информацией в системе менеджмента идентификационных данных для бизнес-целей, отличных от тех, которые идентифицированы в документально оформленных правилах работы регистратора;

- атаки класса MitM, в частности, с целью подмены официального подтверждения или источника (органа выдачи) официальных свидетельств;
- ошибки связывания идентификационных данных с заявителем;
- наличие значительных ошибок первого и второго рода.

Перечисленные угрозы и методы их парирования представлены в таблице 2.5.

Таблица 2.5 - Угрозы, связанные с действиями регистратора, и методы их парирования

Угроза/Атака	**Примеры**	**Методы парирования**
Неполнота или недостоверность собранной на основе предъявленной заявителем информации	Не проверена подлинность предъявленных свидетельств. Не получены официальные подтверждения предъявленных идентификационных данных. Собранные данные не могут гарантировать уникальности цифрового образа заявителя.	Проверка уникальности и подлинности свидетельств. Обязательная верификация свидетельств.
Недостоверность подтвержденной информации на основе предъявленной заявителем информации	Получены подтверждающие свидетельства на предъявленный заявителем паспорт чужого лица с переклеенной фотографией и другие данные того же лица.	Обучение сотрудников, выполняющих регистрацию. Приобретение оборудования, позволяющего обнаружить подделку. Ведение видеозаписи процесса регистрации.
Угроза раскрытия личной информации пользователей (угроза конфиденциальности)	Недостаточная защита от НСД личной информации субъектов доступа. Передача идентификационной информации по открытым каналам. Действия инсайдера.	Организационно-технические мероприятия по предотвращению утечек собранных идентификационных данных субъектов доступа.
Атаки класса «человек посередине» (MitM)	Подмена официального подтверждения или источника (органа выдачи) официальных свидетельств	Применение протоколов защиты каналов со строгой взаимной аутентификацией сторон при верификации
Ошибки связывания цифровых идентификационных данных с личностью заявителя	Применение только фактора знания для связки предъявленных цифровых идентификационных данных с заявителем	Получение подтверждений из заслуживающих доверия источников. Применение биометрии при условии ведения видеозаписи процесса регистрации.

		Проведение анализа подтвержденных поведенческих характеристик.
Наличие значительных ошибок первого и второго рода	Применение только биометрии. Наличие ошибок в базах государственных органов (для больших систем)	Запрос и верификация дополнительных идентификационных данных для необходимой уверенности в том, что заявитель является тем лицом, за кого себя выдает.

Также приведем угрозы **проверяющей стороне**:

- атака на каналы передачи данных;
- фальсификация источника подтверждения.

Методы парирования этих угроз состоят в применении взаимной аутентификации сторон и защиты каналов передачи данных.

Базируясь на анализе перечисленных типовых угроз, можно составить модель угроз применительно к конкретной ИС и реализованных в ней бизнес-процессов. При этом перечень угроз может быть расширен, исходя из анализа рисков. Например, при удаленной регистрации (без личной явки нового пользователя), как минимум, к перечисленным выше добавятся угрозы представления (предъявления муляжа при снятии биометрических характеристик), возможности подделки (поскольку предъявляются не оригиналы, а копии официальных свидетельств), угроза отказа от регистрации, невыполнения обязательств по ответственности в случае конфликтных ситуаций и др.

При этом оценка рисков может проводиться на основе рекомендаций стандарта [124] с использованием традиционного подхода: риск оценивается как произведение частоты нежелательных событий на величину последствий:

$$R = \sum_{i=1}^{n} [F_{\text{BOC}i}(C_i, P_i)], \qquad (2.1)$$

где R – величина риска,

P_i – вероятность возникновения i-го вероятного опасного события (ВОС),

C_i – величина потенциального ущерба в результате реализации i-го ВОС,

$F_{\text{ВОС}i}$ – функционал, связывающий вероятность P_i и ущерб C_i ,

n – количество ВОС.

В подавляющем числе оценок риска для простоты вычислений полагают:

$$F_{\text{ВОС}i} = C_i * P_i \qquad (2.2)$$

В случае накопленной статистики инцидентов, в результате анализа которых выявлены уязвимости, можно применить подход оценки рисков, изложенный в [120]:

$$R = \sum_{i=1}^{n} P_i * U_i * C_i, \qquad (2.3)$$

где U_i – вероятность уязвимости, соответствующей i-тому ВОС.

Тогда при последовательном применении формул (1) и (2) оценка риска может быть проведена по принципу «сверху и снизу» [98]. На практике такой расчет проводится редко, поскольку выявленные уязвимости закрываются сразу после их выявления по итогам анализа инцидентов безопасности. Тем не менее, подобный анализ позволяет подключить механизм управления рисками, пример которого для аутентификации приведен в работе [152].

Основные категории рисков идентификации при регистрации нового пользователя информационной системы

На основе проведенного выше анализа выделим три основные категории угроз для процесса регистрации: выдача претендентом себя за другое лицо (субъект не является тем, за кого себя выдает), отказ легального пользователя от регистрации и, наконец, компрометация инфраструктуры создания и подтверждения идентификационных данных. В данном разделе рассмотрим угрозы выдачи себя за другое лицо и отказа от участия в регистрации, поскольку вопрос угроз для инфраструктуры хорошо изучен и решается с помощью традиционных мер защиты информации (например, защита от вторжений, ведение учета, независимый аудит и др.).

На основе вышеизложенного и личного опыта автора сформулируем некоторые наиболее вероятные и опасные риски первичной идентификации, связанные с категорией «субъект не является тем, за кого себя выдает»:

1. Риск подмены владельца (предъявляются подлинные документы на другого субъекта – схожесть фотографии, грим-маскировка).
2. Риск подлинности предъявленных документов и свидетельств (предъявляются поддельные документы с фотографией и другими данными заявителя).
3. Риск отказа легального пользователя от регистрации.
4. Недостоверность собранной идентификационной информации, в том числе подтвержденной в процессе верификации.
5. Риск ошибок связывания цифровой идентификационной информации с личностью субъекта доступа.
6. Риск ошибок идентификационных данных, в частности, статистические ошибки 1-го и 2-го рода (характерны для наличия значительных по объему идентификационных данных в БД, а также при использовании биометрии с механизмом сравнения на сервере).
7. Риск доступа к личным данным неуполномоченного лица (вероятность раскрытия и/или модификации идентификационных данных), то есть риск нарушения целостности и\или конфиденциальности ПДн.
8. Остальные риски.

Для удаленной первичной идентификации (регистрация нового пользователя в конкретной ИС в удаленном режиме, в том числе без личного присутствия) все указанные риски остаются, при этом риски 1, 3 и 5 обычно существенно выше, чем при личной явке субъекта к регистратору [121,144].

Анализ рисков

Для обработки и анализа рисков идентификации воспользуемся стандартом [124]. Согласно этому документу, оценка риска позволяет ответить на следующие основные вопросы:

- какие события могут произойти и их причина (идентификация опасных событий);
- каковы последствия этих событий;

- какова вероятность их возникновения;

- какие факторы могут сократить неблагоприятные последствия или уменьшить вероятность возникновения опасных ситуаций;

- является уровень риска приемлемым, или требуется его дальнейшая обработка?

Оценка риска - процесс, объединяющий идентификацию рисков, анализ и сравнительную оценку полученных рисков с теми, которые могут приняты. Если риски не могут быть приняты для конкретной организации, применяются меры по снижению рисков или перекладыванию их на третьи лица или страхование рисков. Остановимся на идентификации рисков ПИ.

Идентификация риска (ИР) - процесс определения элементов риска, составления их перечня и описания каждого из элементов риска. Процесс ИР включает в себя идентификацию причин и источников опасных событий, ситуаций, обстоятельств или риска, которые могут оказать существенное воздействие на достижение целей системы идентификации, и характер этих воздействий. Идентификация рисков является одной из самых важных составляющих процесса анализа рисков, от корректности проведения ИР существенно зависит результат анализа рисков.

Идентификация рисков

Обозначим первое из рассматриваемых ВОС1 – риск подмены владельца (предъявляются подлинные документы на другого субъекта – схожесть фотографии, грим-маскировка). Элементами риска могут являться подбор лица, похожего на владельца документов, для совершения подлога лица и/или нанесения грима для придания схожести лица с владельцем. При удаленной идентификации злоумышленником может применяться маска, изготовленная по фотографиям или видеоматериалам.

Основной причиной ВОС1 является желание злоумышленников совершить определенные заранее действия от имени владельца (перевод денежных средств, операции с собственностью и т.д.).

Источником опасного события может являться информация, полученная злоумышленниками, о потенциальной возможности совершения противоправных действий. Характер воздействий в данном случае можно кратко обозначить «маскарад». Обстоятельства воздействия могут быть разные, например, невнимательность регистратора (например, оператора МФЦ) при личном приеме граждан, наличие специально инсценированных помех, использование методов социальной инженерии. При удаленной идентификации в число обстоятельств воздействия дополнительно могут войти использование недостатков и уязвимостей процесса приема сканов документов и биометрических данных.

Для ВОС2 основным элементом риска является подделка документов, причина опасных событий может совпадать с предыдущим риском, источниками опасных событий должны являться не только наличие у злоумышленников информации о потенциальной возможности совершения действий от имени владельца, но и возможность подделки документов. При этом в отличие от рассмотренного выше ВОС1 характер воздействий в виде подделки официального документа подпадает под действие ч.3 ст.371 УК РФ. Другими словами, потенциальная выгода от действий злоумышленников должна быть выше, чем в ВОС1, поскольку ответственность за мошенничество в данном случае выше. Обстоятельствами воздействий при реализации ВОС2 могут быть являться отсутствие обученного распознавать поддельные документы персонала и необходимого для этого оборудования.

Если подобным образом идентифицировать выделенные выше основные риски, результаты могут быть представлены в виде таблицы 2.6. При этом предположим, что вероятность реализации остальных вероятных опасных событий существенно меньше, чем ВОС1-ВОС7.

Таблица 2.6 – Пример идентификации основных типовых рисков первичной идентификации

№ 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 необходимого оборудования
3	Отказ от регистрации	Уход от ответственности	Зарегистрированный пользователь	Непризнание участия в регистрации и личной подписи	Неточное исполнение регламента регистрации или его несовершенство
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	Неточное исполнение регламента регистрации или его несовершенство

				знаний, пассивность регистратора	
6	Отсутствие однозначной уникальности идентификационных атрибутов	Ошибки первого и второго рода	Ошибки оператора официальных 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 привилегированных пользователей ИСПДн, отсутствие технических мер	Несанкционированный доступ, кража ПДн из ИС или при передаче внешним контрагентам	Наличие предварительного сговора или тщательного планирования события

В таблице 2.6 представлен пример идентификации основных рисков первичной идентификации заявителя в процессе его регистрации в информационной системе (ИС). В зависимости от назначения ИС, состава обрабатываемой информации и корректности процессов проверки и подтверждения предъявляемой заявителем идентификационной информации состав ВОС и их актуальность для конкретной информационной системы могут претерпевать существенные изменения. Например, для пользователей корпоративных систем с обученными специалистами отдела кадров и наличием службы внутренней безопасности ВОС1-ВОС3 встречаются весьма редко, а для открытых ИС класса оказания государственных услуг гражданам в электронном виде эти ВОС наиболее актуальны. Рассмотрение вероятностных значений ВОС для некоторых типовых информационных систем оставим на следующую статью в продолжение данной темы.

Оценка потенциального ущерба

Согласно [**Ошибка! Закладка не определена.**] в результате ошибок идентификации, допущенных регистратором в процессе верификации предоставленной заявителем идентификационной информации, возможны следующие категории ущерба для организации:

1) затруднительное положение или причинение ущерба положению или репутации;
2) финансовые потери или платежные обязательства организации;
3) ущерб, наносимый общественным интересам или программам организации;
4) несанкционированное разглашение чувствительной информации;
5) административные, гражданские или уголовные правонарушения;
6) личная безопасность.

В отечественной нормативно-правовой базе, в частности, в отраслевых рекомендациях, более развито понятие уровня тяжести последствий в результате реализации ВОС [111,112]. Учитывая опыт, изложенный в приведенных источниках, для процесса ПИ предлагается ввести следующие уровни ущерба (тяжести последствий):

- критический,
- существенный,
- несущественный,
- незначительный.

Поскольку информационные системы могут существенно отличаться не только по назначению и составу обрабатываемой информации, но и по методам ПИ, предлагается ввести три условных категории ИС:

- корпоративные системы с обученными сотрудниками отдела кадров, обязательной личной явкой нового сотрудника на собеседования и в отдел кадров с предоставлением нескольких документов (паспорт, трудовая книжка, диплом об образовании, военный билет и т.д.) при оформлении на работу;

- информационные системы открытого типа (например, для оказания государственных услуг), но с обязательной личной явкой для регистрации в данной ИС в качестве нового пользователя;
- информационные системы открытого типа без личной явки для регистрации.

При этом на основе исследований [134,135] предлагается ввести простую шкалу вероятности возникновения ВОС:

- очень частое, с вероятностью P_i возникновения любого ВОС в год $P_i \geq 10^{-2}$,
- частое $10^{-3} \leq P_i < 10^{-2}$,
- вероятное $10^{-4} \leq P_i < 10^{-3}$,
- случайное $10^{-5} \leq P_i < 10^{-4}$,
- редкое $10^{-6} \leq P_i < 10^{-5}$,
- крайне редкое $10^{-7} \leq P_i < 10^{-6}$,
- маловероятное $10^{-8} \leq P_i < 10^{-7}$,
- весьма маловероятное $P_i < 10^{-8}$.

Оценка величины ущерба и вероятности реализации для рассматриваемых ВОС представляет собой сложную задачу. Для решения этой задачи применялся метод Дельфи. Усредненные результаты опроса 12 экспертов, где величина ущерба представлена в безразмерном виде, приводятся в таблице 2.7.

Таблица 2.7 – Результаты опроса экспертов по относительной величине и частоте ущерба

	Оценка размера ущерба		Оценка вероятности реализации ВОС		
№ ВОС	Минимальный размер ущерба	Максимальный размер ущерба	Корпоративные ИС,	Открытые ИС с личной явкой на регистрацию	Открытые ИС без личной явки на регистрацию
1	1	30	10^{-8} -10^{-6}	$10^{-5} – 10^{-4}$	$10^{-3} – 10^{-2}$
2	3	50	10^{-7} -10^{-5}	$10^{-5} – 10^{-3}$	$10^{-3} – 10^{-2}$
3	0,2	10	10^{-10} -10^{-8}	$10^{-8} – 10^{-6}$	$10^{-4} – 10^{-2}$
4	0,1	2	10^{-8} -10^{-6}	$10^{-6} – 10^{-4}$	$10^{-6} – 10^{-4}$
5	0,3	3	10^{-9} -10^{-7}	$10^{-6} – 10^{-4}$	$10^{-5} – 10^{-2}$

6	0,01	0,05	10^{-8} -10^{-7}	10^{-6} – 10^{-4}	10^{-4} – 10^{-2}
7	0,5	20	10^{-8} -10^{-6}	10^{-5} – 10^{-3}	10^{-5} – 10^{-3}

Проведем оценку допустимых значений риска и интервальной оценки значений рисков, а также частоты типовых ВОС. Как показано в работах [176,177], наиболее эффективным инструментом оценки технологических рисков на железнодорожном транспорте является применение критерия риска в виде принципа ALARP («низкий, насколько реально возможно») и способа построения матриц рисков, разработанного в работе [178]. В данном разделе методы анализа рисков, внедренные на железнодорожном транспорте, применяются для оценки рисков первичной идентификации при регистрации новых пользователей различных информационных систем.

Критерии риска и методы оценки риска

Согласно разделу 4.3.3. стандарта [124] выбор критерия риска и методов оценки риска является главной задачей при формировании целей управления риском. Для определения критериев риска необходимо определить:

- характер и тип последствий реализации ВОС, а также способы их оценки;
- методы оценки ВОС;
- методы установления уровней риска;
- критерии принятия решений при необходимости обработки риска;
- критериев приемлемости риска;
- возможности одновременного возникновения различных видов опасных событий и особенности соответствующего риска.

В стандарте [179] рассмотрены три подхода к заданию допустимых уровней рисков в соответствии с наиболее часто используемыми принципами (критериями риска): MEM, GAMAB и ALARP.

Принцип MEM (Minimum endogenous mortality – минимальная эндогенная смертность) заключается в условии «угроза, связанная с новой системой, не должная превышать имеющуюся цифру минимальной эндогенной смертности». Для рассматриваемых типов ИС применительно к процессу первичной

идентификации этот принцип может быть переформулирован как «безопасность новой ИС должна быть не хуже предыдущей». К сожалению, этот принцип в данном исследовании не применим, он может применяться только при проектировании новых ИС и модернизации старых систем.

Такой подход справедлив и для принципа GAMAB (Globalement au moins aussi - в целом, по крайней мере, также), который также опирается на достигнутый в существующей системе уровень рисков и говорит о необходимости совершенствования проектируемой ИС через требование «по крайней мере».

Следовательно, наиболее подходящим к рассматриваемым ВОС представляется принцип ALARP (As low as reasonably practicable - низкий, насколько реально возможно), который изображен на рис. 2.3.

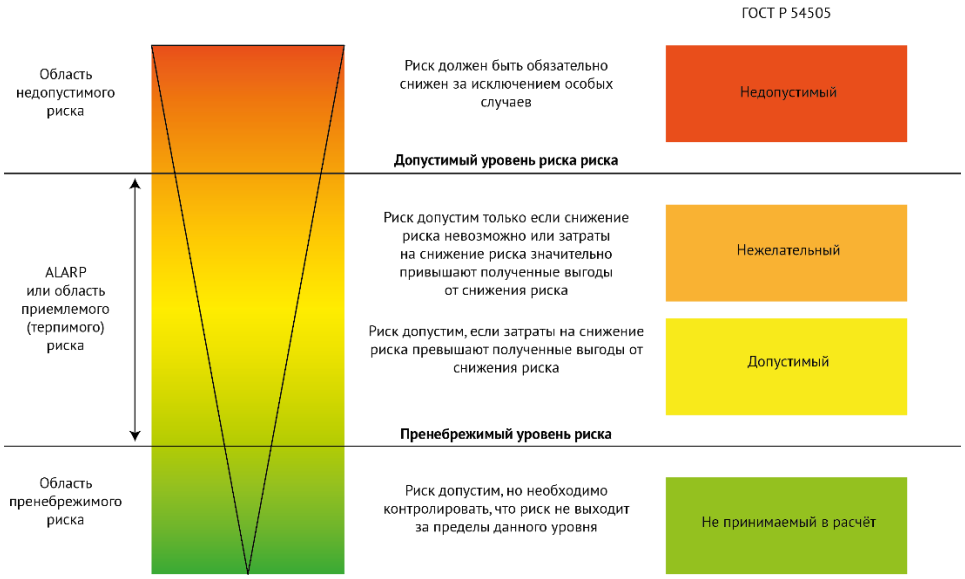

Рисунок 2.3 – Оценивание риска на основе принципа ALARP

Некоторые риски настолько велики, а последствия настолько неприемлемы, что они недопустимы и не могут быть ни в коем случае оправданы. Верхняя граница определяет уровни риска, которые являются недопустимыми. Если уровень риска не может быть опущен ниже этой границы, тогда риск должен быть исключен. Нижняя граница диаграммы устанавливает ши-

рокую область применения, в которой уровень риска считается настолько низкой, что все усилия по его еще большему снижению, скорее всего, не будут оправданы. Зона между верхней и нижней границей называется областью ALARP. Следует подчеркнуть, что недостаточно определить, что какой-либо вид риска расположен в области ALARP. Его следует сделать настолько низким, насколько это достижимо на практике.

Проведем оценку рисков первичной идентификации с помощью построения матриц рисков для рассматриваемый ВОС.

Построение матриц рисков

В качестве методической основы возьмем способ построения матриц рисков и оценивания рисков, разработанного в АО «НИИАС» коллективом специалистов под руководством проф. И.Б. Шубинского [176-179] и реализованного в программном обеспечении проекта УРРАН [180]. Коротко изложим суть способа [178], разработанного в НИИАС с целью снижения погрешности представления результатов расчетов при заданных стандартом [179] параметров матрицы рисков (4 интервала значений ущерба c_1, c_2, …, c_n по горизонтали и 6 интервалов частоты возникновения нежелательного события f_1, f_2, …, f_n по вертикали).

Приняв, что риск оценивается как произведение частоты нежелательных событий на величину последствий $R=F\times C$, предложено введение логарифмических координат, в которых величина R=const представляется в виде прямой линии (в отличие от стандартного графика связи f_i и c_i, где значения R_i=const представляют собой гиперболы).

Параметры ячеек матрицы и горизонтальный шаг между прямыми R_i= const с заданным тангенсом угла наклона $tg\ \gamma = -\frac{\beta}{\alpha} = -2$, при условии α+β=1 предложено рассчитывать динамически в зависимости от заданных входных величин. Расчет значений координат углов ячеек матрицы рисков начинается с верхнего правого угла – начиная с максимальных уровней A_3 и B_2 (рис. 2.4).

Алгоритм вычисления координат углов ячеек матрицы рисков в целях повышения точности разработан с условием, что каждую ячейку прямая R=

const должна делить не более, чем на две не равные по площади части.

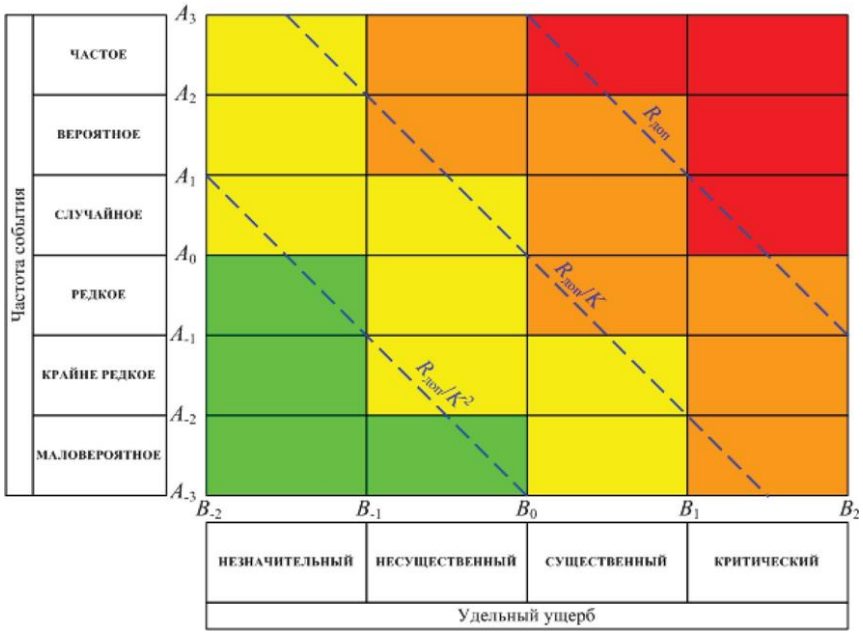

Рисунок 2.4 – Принцип построения матрицы рисков [178].

Входными данными для расчетов являлись интервальные оценки вероятности возникновения нежелательного события $ВОС_i$, i=1, 2,… ,7 и соответствующего удельного размера последствий из таблицы 4 работы [158]. Таким образом, все входные параметры расчета являются безразмерными параметрами, нас интересуют относительные величины риска и их соотношение для выбранного в работе [158] ряда параметров $ВОС_i$ для проведения параметрических расчетов. В связи с этим однозначную оценку риска в координатах «частота (вероятность) - последствия» получить не представляется возможным. Для оценки фактического уровня риска за заданный интервал наблюдения необходимо располагать данными о количестве нежелательных событий и удельном (на 1 событие) размере последствий (то есть, требуется точечная оценка, «точка риска»).

Тем не менее, представленные данные позволяют определить область на координатном пространстве матрицы рисков, в которой, в соответствии с экспертными оценками, будут находиться точки риска. Допустимый уровень риска $R_{доп}$ определяется из соображений доверительной вероятности 0,9, т.е. 90% площади риска отделяется наклонной линий (логарифмом кривой риска).

Ниже этой наклонной прямой находится область ALARP. Угол наклона аналогичен углу наклона прямых $R_{доп}$, $R_{доп}/K$ и $R_{доп}/K^2$ (на рис.2.4 верхняя, средняя и нижняя наклонные прямые в заштрихованной зоне). Эти данные также позволяют задать для риска каждого вида допустимый уровень риска (экспертными методами). Результаты установления допустимого уровня риска и представления области, в которой для выбранного вида риска будут находиться точки риска, представлены в результатах расчета. Пример расчета приводится на рис. 2.5.

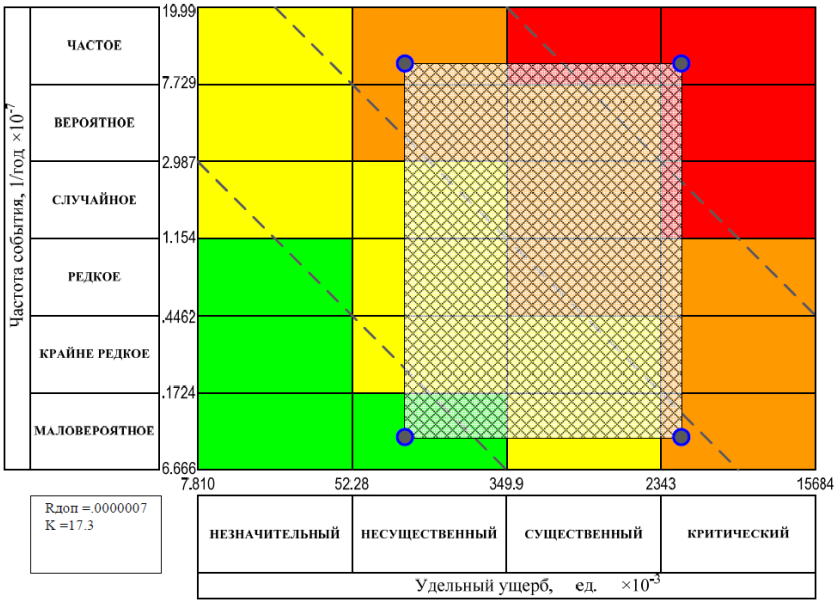

Рисунок 2.5 – Пример построения матрицы рисков. ВОС2 для корпоративных ИС.

Дальнейшая обработка результатов расчетов представлена в следующем разделе.

Обработка результатов расчетов

Как показано на рис. 2.5, каждая полученная в результате расчета матрица рисков содержит заштрихованную зону заданного интервала значений частоты (вероятности) ВОС и интервала потенциального ущерба из работы [158].

Для определения средних значений ущерба $C_{ср.}$ и частоты $f_{ср.}$ в результате реализации ВОС необходимо найти центр тяжести заштрихованной зоны

и определить ее координаты. Искомая точка и ее координаты находятся методом пересечения диагоналей заштрихованного прямоугольника. Результаты расчета указанных средних значений сведены в таблицу 2.8. Для каждого ВОС в таблице указана величина допустимого риска $R_{доп.} = C_{ср.} \times f_{ср.}$

Таблица 2.8 – результаты обработки данных расчета

ВОС	*C*min	*C*max	*C*ср.	*f*ср.	*R*ср.	*R* доп.	*R*ср./ *R* доп.
ВОС1_корп	1	30	7,75	0,0000001	0,000000775	0,0000511	1,52%
ВОС1_с_л	1	30	7,75	0,0000039	0,000030225	0,000156	19,38%
ВОС1_б_л	1	30	6,387	0,003	0,019161	0,0858	22,33%
ВОС2_корп	3	50	16,31	0,0000001	0,000001631	0,00007	2,33%
ВОС2_с_л	3	50	11,544	0,000035	0,00040404	0,002	20,20%
ВОС2_б_л	3	50	14,633	0,003221	0,047132893	0,2	23,57%
ВО3_корп	0,1	10	1,52	1,053E-07	1,60056E-07	5,11E-06	3,13%
ВО3_с_л	0,1	10	1,52	0,0000001	0,000000152	0,000001	15,20%
ВО3_б_л	0,1	10	1,72	0,001	0,00172	0,01	17,20%
ВОС4_корп	0,1	3	0,848	9,53E-09	8,08144E-09	0,0000007	1,154%
ВОС4_б_л	0,1	3	0,848	0,00001	0,00000848	0,00007	12,11%
ВОС4_с_л	0,1	3	0,848	0,00001	0,00000848	0,00007	12,11%
ВОС5_корп	0,1	3	0,848	0,0000001	8,48E-08	5,11E-06	1,66%
ВОС5_с_л	0,1	3	0,848	0,00001	0,00000848	0,00007	12,11%
ВОС5_б_л	0,1	3	1,7	0,0003766	0,00064022	0,005	12,80%
ВОС6_корп	0,01	0,05	0,027	3,312E-08	8,9424E-10	2,5E-07	0,36%
ВОС6_с_л	0,01	0,05	0,035	0,00000851	2,9785E-07	0,000002	14,89%
ВОС6_б_л	0,01	0,05	0,0366	0,001054	3,85764E-05	0,0002	19,29%
ВОС7_корп	0,3	1	0,546	0,0000001	5,46E-08	0,0000003	18,20%
ВОС7_с_л	0,3	1	0,546	0,0001	0,0000546	0,0003	18,20%
ВОС7_б_л	0,3	1	0,546	0,0001	0,0000546	0,0003	18,20%

Также в последнем столбце таблицы приведены соотношения $R_{ср.}/ R_{доп.}$, эти данные для ВОС*i*, *i* =1,6 приведены на рис. 2.6 в виде графиков. Видно, что расчетные значения относительного среднего риска для различных ВОС дают примерно одинаковые величины с одной и той же тенденцией: значения относительного среднего риска в корпоративных сетях находятся в пределах 3%, для открытых информационных систем с личной явкой находятся в пределах 12%-20%, а для открытых ИС с регистрацией новых пользователей без личной явки в среднем еще выше на 1%-5%, но не превышают 25%. При этом сами значения как допустимого, так и среднего риска для новых пользователей на

два порядка выше, чем при личной явке.

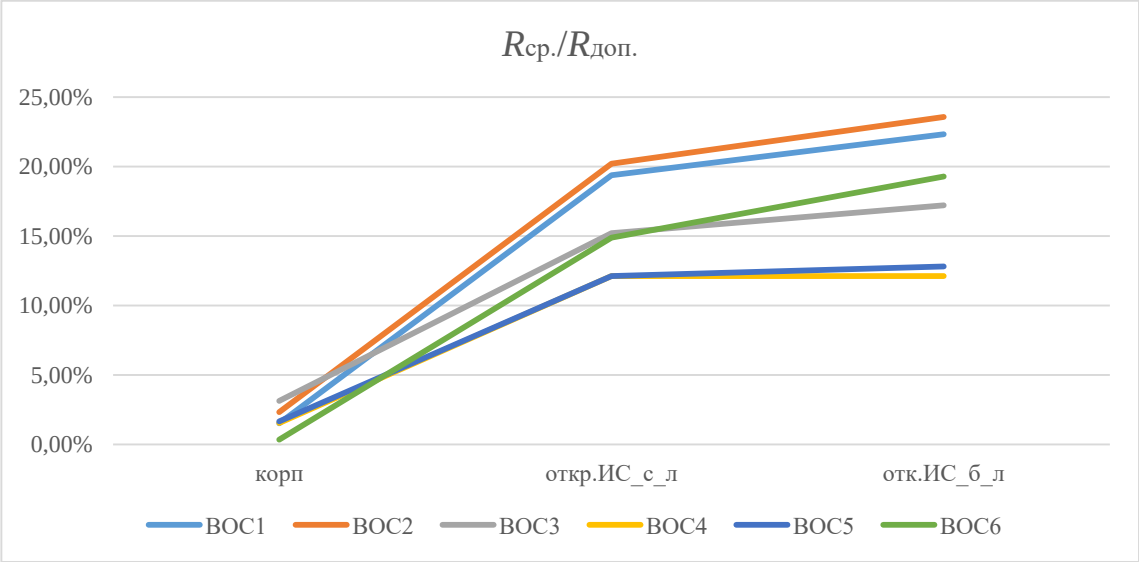

Рисунок 2.6 – Результаты расчета отношения среднего риска к допустимому для различных ВОС

Результаты расчетов относительного среднего риска для рассматриваемых ВОС в наглядной форме представлены на рис. 2.7. С этой целью диаграмма построена при $R_{доп.}$=0,3.

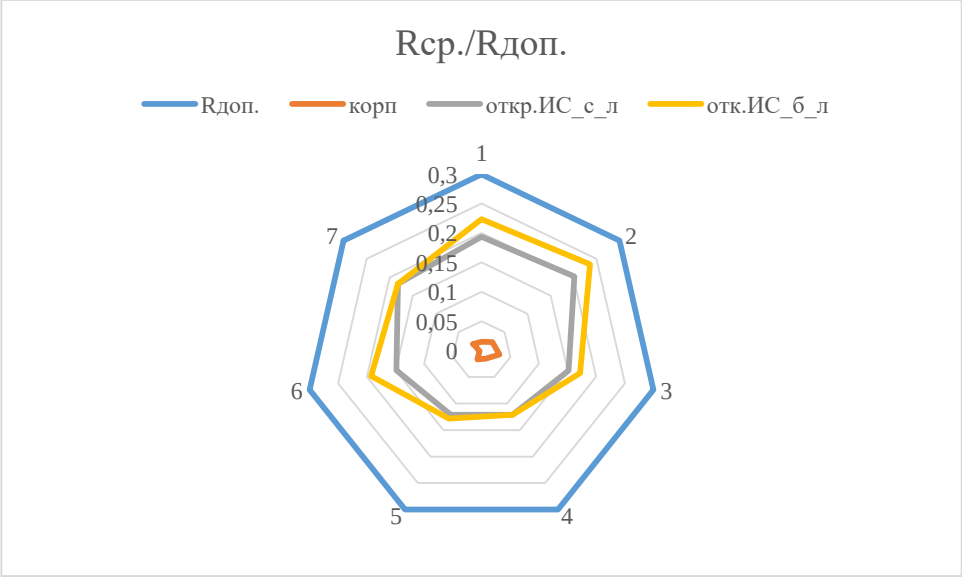

Рисунок 2.7 – Результаты расчета отношения $R_{ср.}$/ $R_{доп.}$ в виде лепесткового графика

Как видно из представленных результатов, относительная величина среднего риска $R_{ср.}$/ $R_{доп.}$ нежелательных событий в процессе первичной идентификации нового пользователя ИС для всех рассмотренных ВОС повторяет

одну и ту же тенденцию: для открытых информационных систем средние риски на порядок выше, чем для закрытых (корпоративных) систем. Насколько корректно выполнены предложенные оценки, покажет дальнейший научный анализ и статистика фиксации нежелательных событий. Итак, в данном разделе предлагаемой работы впервые представлены следующие результаты:

- выполнен расчет матриц рисков типовых вероятных опасных событий процесса первичной идентификации;
- определены уровни допустимого риска реализации типовых вероятных опасных событий для информационных систем закрытого типа (корпоративных систем) и открытого типа с обязательным требованием личной явки и без личной явки субъекта для регистрации его в качестве нового пользователя информационной системы;
- получены оценки средних значений рисков по отношению к допустимому уровню рисков для всех рассмотренных комбинаций;
- установлено, что риски первичной идентификации для открытых систем на порядок превышают риски для информационных систем закрытого типа, при этом сами средние значения рисков и величины допустимого риска – на два и более порядка выше, чем для корпоративных систем.

В целях получения наиболее общих результатов финальные характеристики приведены в безразмерном виде.

Приведенные материалы позволяют выполнять оценки рисков первичной идентификации субъектов в процессе регистрации новых пользователей для конкретных современных информационных систем.

2.5 Постановка задачи оценки доверия к результатам идентификации субъектов доступа

Как указано во введении, в связи с интенсивным развитием информатизации общества число ИС различного назначения неуклонно растет. Количество зарегистрированных субъектов и объектов доступа в ИС также может ис-

числяться сотнями тысяч, миллионами, а иногда и десятками миллионов (пример – ИС Федеральной налоговой службы России). Такие системы называют большими информационными системами (БИС). По прогнозам количество БИС будет увеличиваться. При удаленном электронном взаимодействии (УЭВ) очень важно знать, является ли другая сторона действительно той, с кем вы планировали взаимодействие (тот ли это субъект, за кого он себя выдает). Наиболее остро задача идентификации пользователей ИС стоит в системах управления доступом пользователей [143]. В условиях лавинообразного роста кибератак и разного рода мошенничеств задача идентификации сторон взаимодействия становится особенно актуальной [181].

Как было показано в разделе 1.3.1, в качестве основных критериев доверия к результатам идентификации могут быть приняты достоверность результатов идентификации $\varphi_Д$, надежность работы системы идентификации $\varphi_Н$ и безопасность $\varphi_Б$, в том числе безопасность личных персональных данных, содержащихся в идентификационной информации. При этом указанные характеристики определим в виде безразмерных параметров, т.е. все перечисленные характеристики могут изменяться только в пределах $0 \le X \le 1$, где X – безразмерная характеристика надежности $\varphi_Н$, безопасности $\varphi_Б$ или достоверности $\varphi_Д$.

Таким образом, для оценки доверия к результатам идентификации субъекта доступа можно ввести функцию доверия Ψ, которая в общем случает будет зависеть от времени и характеристик $\varphi_Н$, $\varphi_Б$ и $\varphi_Д$. Тогда текущая оценка доверия к результатам цифровой идентификации субъекта доступа сводится к поиску решений $\Psi(t, \varphi_Б, \varphi_Д, \varphi_Н)$ в безразмерном пространстве, ограниченном единичным кубом, поскольку сама функция доверия Ψ также может изменяться лишь в пределах от нуля до единицы:

$$0 \le \Psi(t, \varphi_Б, \varphi_Д, \varphi_Н) \le 1 \qquad (2.4)$$

Итак, постановка задачи оценки доверия к результатам идентификации в формализованном виде может сводиться к поиску решений $\psi(t, \varphi_Б, \varphi_Д, \varphi_Н)$ в безразмерном ортопространстве.

Альтернативным способом оценки доверия к полученным результатам

первичной идентификации субъекта доступа, как показано в работе [**Ошибка! Закладка не определена.**], могут быть приняты характеристики качества ПИ, степени связанности цифровых ИД с личностью субъекта доступа и безопасности используемых ПДн субъекта. Однако в силу того, что характеристики качества ПИ в настоящее время являются трудноизмеримыми параметрами, а степень связанности зависит в значительной степени от субъективного решения конкретного регистратора, проводящего процесс ПИ на основании своих регламентов, что тоже практически невозможно объективно выражать в цифровом виде, предложенный выше подход выглядит предпочтительнее. Все три предложенные в формуле (2.4.1) характеристики в конкретной информационной системе могут быть доведены до вполне определенных числовых значений.

2.6 Методика оценки доверия к результатам идентификации субъектов доступа

Анализ стандартов по идентификации [57 - 63] и пятнадцатилетний опыт исследования процессов идентификации и аутентификации автора позволил сформулировать **критерии доверия** к результатам первичной идентификации [154]:

- надежность работы системы идентификации;
- достоверность (актуальность, полнота, точность и аутентичность) результатов идентификации;
- выполнение в процессе первичной идентификации требований информационной безопасности, в том числе в отношении персональных идентификационных данных субъектов доступа.

Проведение оценок представленной субъектом идентификационной информации по предложенным критериям позволит сделать вывод о качестве представленной информации и степени связанности идентификационной информации с конкретной личностью.

Под надежностью в данной формулировке подразумевается функциональная надежность, определяемая как способность системы идентификации выполнять предусмотренные функциональные задачи с приемлемым уровнем безошибочности в реальных условиях эксплуатации, в том числе, минимальный уровень сбоев и ошибок в работе системы идентификации.

Степень связанности идентификационной и аутентификационной информации с конкретной личностью в текущей ситуации на отечественном рынке является не регламентированным процессом, за который отвечает регистрирующая сторона. Известны не единичные случаи регистрации субъектов доступа в качестве пользователей ИС и/или владельцев УКЭП по копии паспорта, которые в ряде случаев привели к материальным потерям. Во всех известных случаях представленная субъектом при регистрации идентификационная информация была недостоверна.

Поскольку задача определения степени связанности ИД с субъектом плохо формализуется, на данном этапе исследований предлагается включить ее в понятие достоверности (актуальность, полнота, точность и аутентичность) идентификационной информации.

Уровней доверия к результатам первичной идентификации может быть не менее трех (низкий, средний, высокий). Их количество определяется уровнями рисков ошибок идентификации субъекта при получении (или отказа в доступе) доступа к информации того или иного уровня конфиденциальности и требованиями к защите идентификационной информации, относящейся к персональным данным.

В отличие от зарубежной развитой практики оценки рисков каждой организацией во многих областях, в том числе и в части ИА и ПДн, в нашей стране утвержденных методик оценки рисков в области идентификации и аутентификации пока не разработано.

В связи с этим предлагаемая методика оценки доверия к результатам идентификации основывается на использовании сформулированных критериев доверия к результатам идентификации, базирующихся на выполненном

анализе рисков. Методика включает в себя модели процесса идентификации, позволяющие выполнить оценки надежности работы системы идентификации и достоверности получаемых результатов. Оценка безопасности персональных данных, имеющихся в составе идентификационной информации и обрабатываемых в процессе идентификации, достаточно хорошо описана в приказе № 21, методических материалах ФСТЭК России [182, 183] и 8 Центра ФСБ России [184]. Результирующая оценка доверия к результатам идентификации строится на анализе проведенных исследований достоверности ИД, надежности работы системы идентификации и безопасности личных данных пользователей ИС.

Таким образом, методика оценки доверия к результатам первичной идентификации может быть сформулирована в виде следующего алгоритма действий:

1) оценка надежности работы системы идентификации и аутентификации во время регистрации нового пользователя (проверка полноты, точности и аутентичности полученных от заявителя данных - отправление запросов в официальные органы, получение официальных и неофициальных подтверждений достоверности значений идентификационных атрибутов, привязка цифровых данных идентификационных атрибутов к личности заявителя и т.д.);
2) оценка достоверности и актуальности предоставленной заявителем идентификационной информации, в частности, подлинности представленных бумажных документов;
3) оценка безопасности ПДн субъектов доступа;
4) анализ полученных в результате 1-3 данных с целью вынесения решения.

2.7 Модели для оценки доверия к результатам идентификации

В простейшем случае использования одного идентификатора в закрытой корпоративной ИС задача идентификации сводится к вычислению некоторой функции

$$y = f(a, x_1) \quad (2.5)$$

где x_1 – предоставленная претендентом на доступ буквенно-цифровая последовательность;

a – индивидуальный параметр пользователя, с последующим сравнением значения y с заранее занесённой (эталонной) величиной $Y_0 = F(A, X_0)$ в базу данных учётных записей пользователей. В случае $Y = Y_0$ идентификация считается успешно пройденной.

Для территориально-разнесённых ИС с большим количеством пользователей, и особенно для ИС общего пользования, одного идентификатора для выполнения однозначной автоматической идентификации пользователя может быть недостаточно. Для таких ИС уравнение (2.6) усложнится:

$$Y = f(a, x_1, x_2, \dots x_k) = f(a, X), \quad (2.6)$$

где k – число идентификаторов.

Тогда функция проверки соответствия введённых значений идентификаторов $X = \{x_i\}$, $i = 1, 2., \dots k$ эталонными значениями $X_0 = \{x_{0i}\}$, $i = 1, 2, \dots k$ в базе данных учетных записей распадается на k пар. По сути, ищется пересечение конечных множеств

$$Y \bigcap Y_0 \quad (2.7)$$

Для малых k требование полной идентичности в формальном виде можно записать как $Y \bigcap Y_0$. Как показано в работе [144], если число N зарегистрированных субъектов и объектов в закрытых корпоративных информационных системах $N_{\text{зкис}} \geq 10^4$, или в информационных системах общего пользования $N_{\text{исоп}} \geq 10^3$, необходимо применять дополнительные меры по повышению надёжности и безопасности автоматической идентификации, что проиллюстрировано на примерах идентификации по данным паспорта и по сертификату ключа проверки электронной подписи владельца. В частности, поскольку

точность автоматической идентификации объекта с помощью одного идентификатора в СКПЭП, как правило, не превышает 10^{-3}, организационных мер может быть недостаточно и зачастую требуется введение в процедуру идентификации некоторого числа дополнительных идентификаторов, зависящего от количества зарегистрированных в базе данных учетных записей объектов и класса ГИС. В этом случае задача сводится к поиску минимального значения числа идентификаторов k, необходимого для однозначной идентификации одного конкретного субъекта или объекта из общего числа зарегистрированных объектов N.

Значительная часть функционирующих ИС требует предъявления одного, максимум, двух значений идентификаторов. Однако для БИС, как показано в работе [144], для повышения надежности идентификации необходимо увеличивать число идентификаторов.

Для общего решения задачи о достоверности идентификации субъекта (объекта) примем необходимость достижения заданного значения достоверности D в интервале значений $0 < D \leq 1$ при использовании неограниченного набора идентификаторов $ID_i, i = 1, 2, \ldots N$. В качестве основной цели данной работы определим поиск необходимого, но достаточного количества идентификаторов N для достижения заданного значения достоверности в зависимости от масштаба информационной системы.

Упрощенную архитектуру системы идентификации представим в виде схемы, состоящей из последовательных элементов проверки предъявляемых идентификаторов ID_i при $i = 1, \ldots N$ (рис. 2.8).

Рисунок 2.8 – Модель последовательного предъявления идентификаторов

Для последовательной схемы надёжность работы системы H_c определяется произведением надёжности ее элементов:

$$H_c = \prod_{i=1}^{N} H_i \tag{2.8}$$

где i – элемент системы;

N – число элементов.

Из (2.8) следует, что вероятность безотказной работы системы, состоящей из последовательного соединения элементов, будет ниже, чем вероятность безотказной работы самого надёжного элемента системы.

Рассмотрим схему параллельного (независимого) предъявления идентификаторов приведенную ниже (Рисунок 2.9).

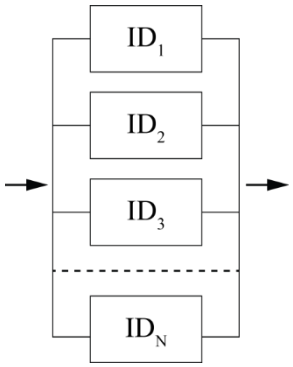

Рисунок 2.9 – Модель процесса идентификации при параллельной проверке идентификационной информации

Для повышения надёжности идентификации схема в виде последовательного предъявления ряда идентификаторов, должна быть заменена схемой параллельного сравнения предъявленных претендентом идентификаторов с эталонными [163]. Только в этом случае удастся достичь необходимого уровня надёжности первичной идентификации пользователя при доступе к информационным ресурсам, оценить которую сверху можно по формуле [154]:

$$P_1 \cdot P_2 \cdot \ldots \cdot P_N \leq \frac{1}{K+1} \tag{2.9}$$

где P_i – вероятность безошибочной идентификации с применением i-го идентификатора;

N – минимально-необходимое, но достаточное число идентификаторов;

K количество зарегистрированных в ИС объектов доступа и субъектов доступа.

Для более точных оценок надежности идентификации субъекта при доступе к информационным ресурсам воспользуемся результатами работ [35, 36, 15]. В качестве начального приближения примем модель структурной надежности на основе метода конечных автоматов, заключающуюся в том, что проверку каждого предъявленного идентификатора будем считать независимо (по надежности) работающим прибором.

Надёжность работы системы H_i определяется соотношением

$$H_c = 1 - \prod_{i=1}^{N}(1 - H_i) \tag{2.10}$$

где H_i – надёжность каждого элемента системы.

Достоверность идентификации D для схемы последовательно предъявляемых идентификаторов с номером i определяется соотношением

$$D = \prod_{i=1}^{N}(1 - q_i) \tag{2.11}$$

где q_i – вероятность ошибки работы i-го элемента [204, **Ошибка! Закладка не определена.**];

Достоверность идентификации при параллельной схеме определяется как

$$D = 1 - \prod_{i=1}^{N} q_i \tag{2.12}$$

где q_i – вероятность ошибки работы подсистемы при сравнении i -го идентификатора.

Утверждение. В больших системах с числом пользователей К (современные ИС имеют количество пользователей порядка $К = 10^6 - 10^8$). Для выполнения основной функции идентификации - уникальности и различимости каждого субъекта из общего количества пользователей необходимо достигать значение достоверности идентификации не ниже:

$$D = 1 + \frac{1}{(K+1)} \tag{2.13}$$

где K – число пользователей.

Анализ значений достоверности идентификации в двух рассмотренных схемах приводит к выводу о том, что наиболее предпочтительной архитектурной схемой математической модели подсистемы идентификации для больших систем является схема параллельного предъявления идентификаторов. Это утверждение согласуется с постулатом надежности.

Аналитическое решение. Воспользуемся классическим подходом, изложенным в [35]. Из определения системы, состоящей из параллельно соединённых элементов, условием безотказной работы системы P_c является безотказная работа хотя бы одного элемента $P_i,\ i = 1, n.$

Если считать отказы элементов независимыми, то на основании теоремы умножения вероятностей вероятность безотказной работы системы определяется следующим выражением:

$$P_c(t) = 1 - q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_n(t) = 1 - \prod_{i=1}^{n} \big(1 - p_i(t)\big), \tag{2.1}$$

где $P_c(t)$ – вероятность безотказности работы системы;

$q_i(t)$ – вероятность отказа работы i-го элемента;

$p_i(t)$ вероятность безотказной работы i-го элемента.

Принимая, что вероятность безотказной работы каждого элемента $p_i(\mathrm{t})$

на отрезке времени (t_1, t_2) подчиняется зависимости [35]:

$$p_i(t_1, t_2) = e^{-\int_{t_1}^{t_2} \lambda(t)dt}, \tag{2.2}$$

где $\lambda(t)$ – интенсивность отказа элемента.

С учетом (2.2) выражение (2.1) примет вид:

$$P_c(t) = 1 - \prod_{i=1}^{n} \left(1 - e^{\int_0^t \lambda_i(t)dt}\right) \tag{2.3}$$

для случая элементов с одинаковой надежностью работы:

$$P_c(t) = 1 - \prod_{i=1}^{n} \left(1 - e^{-\lambda(t)dt}\right), \tag{2.4}$$

при $\lambda = \text{const}$ выражение (2.4) примет известный вид:

$$P_c(t) = 1 - \prod_{i=1}^{n} \left(1 - e^{-\lambda t}\right), \tag{2.5}$$

Для случая (2.4) легко вычисляется средняя наработка до отказа систем

$$t_{\text{ср.с}} = \int_0^{\infty} P_c\,(t)dt = \int_0^{\infty} \left[1 - (1 - e^{-\lambda t})^n\right] dt, \tag{2.6}$$

При замене переменных

$$1 - e^{-\lambda t} = x;$$

$$t = \frac{1}{\lambda} ln \frac{1}{1 - x};$$

$$dt = \frac{dx}{\lambda(1 - x)};$$

$$t = 0; x = 0;$$

$$t = \infty; x = 1,$$

получим

$$t_{\text{ср.с}} = \frac{1}{\lambda} \int_0^{\infty} \frac{1 - x^n}{1 - x} dx = \frac{1}{\lambda} \int_0^{1} (1 + x + \cdots + x^{n-1}) dx = \frac{1}{\lambda} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right), \tag{2.7}$$

Для одного, двух и трех идентификаторов значения $t_{\text{ср.с}}$ будут равны,

соответственно $\frac{1}{\lambda}$, $\frac{3}{2\lambda}$ и $\frac{11}{6\lambda}$.

При большом n

$$t_{\text{ср.с}} \approx \frac{1}{\lambda}(ln\, n + C), \tag{2.8}$$

где C = 0,577.

Поскольку на практике для небольших информационных систем зачастую применяется схема последовательной проверки идентификаторов (Рисунок 2.), рассмотрим ее подробнее.

При анализе надёжности системы обычно принимают расчётную схему, согласно которой допускают, что на элемент системы действует простейший поток отказов с интенсивностью λ. Элемент системы отказывает в момент, когда приходит первое событие этого потока.

Примем, что последовательность случайных моментов времени, в которые происходят отказы идентификации, представляют собой простейший поток событий, а интервалы между событиями – независимые случайные величины, распределённые по показательному закону:

$$f\,(x) = \lambda e^{-\lambda t}\,, (t > 0) \tag{2.9}$$

Обозначим $P_i\,(t)$ – вероятность того, что в любой момент t система S будет находиться в состоянии $S_i\,(i = 1, \ldots n)$. Эти вероятности необходимо найти. По определению для любого t $\sum_{i=1}^{n} P_i(t) = 1$, т.к. события образуют полную группу несовместных событий. Направленный граф состояний системы идентификации представлен ниже (Рисунок 2.10).

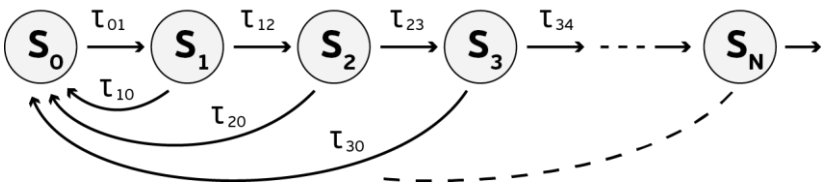

Рисунок 2.10 – Размеченный граф состояний системы идентификации

Обозначим:

S_0 – состояние системы: система готова.

S_1 – первый идентификатор предъявлен, система провела его проверку;

S_2 – второй идентификатор предъявлен, система провела его проверку;

S_3 – идентификация успешно пройдена, система передала управление системе аутентификации;

S_4 – подсистема аутентификации приняла идентификационные данные пользователя.

τ_{01} – переход из состояния S_0 в состояние S_1;

τ_{12} – переход из состояния S_1 в состояние S_2;

τ_{23} – переход из состояния S_2 в состояние S_3;

τ_{10} – переход из состояния S_1в состояние S_0 - подсистема идентификации возвращает процесс в начало (состояние S_0) из-за несовпадения первого идентификатора;

τ_{20} – переход из состояния S_2 в состояние S_0 - подсистема идентификации возвращает процесс в начало из-за несовпадения второго идентификатора;

τ_{30} – переход из состояния S_3 в состояние S_0 - подсистема идентификации возвращает процесс в начало из-за несовпадения третьего идентификатора;

τ_{34} – переход из состояния S_3 в состояние S_4 - подсистема идентификации передаёт данные претендента в подсистему аутентификации;

$P_0(t)$ – вероятность того, что в момент времени t система находится в состоянии S_0;

$P_i(t)$ – вероятность пребывания системы в состояниях S_i.

Тогда уравнения Колмогорова для рассматриваемой системы могут быть представлены в виде:

$$\begin{gathered}\frac{dP_0(t)}{dt} = -\tau_{01}P_0(t) + \tau_{10}P_1(t) + \tau_{20}P_2(t) + \tau_{30}P_3(t);\\ \frac{dP_1(t)}{dt} = -\tau_{12}P_1(t) - \tau_{10}P_1(t) + \tau_{01}P_0(t) + \tau_{30}P_3(t) = -P_1(t)(\tau_{10} + \tau_{12}) + \tau_{01}P_0(t);\\ \frac{dP_2(t)}{dt} = -\tau_{23}P_2(t) - \tau_{20}P_2(t) + \tau_{12}P_1(t) = -P_2(t)(\tau_{20} + \tau_{23}) + \tau_{12}P_1(t);\\ \frac{dP_3(t)}{dt} = -\tau_{34}P_3(t) - \tau_{30}P_3(t) + \tau_{23}P_2(t) = -P_3(t)(\tau_{30} + \tau_{34}) + \tau_{23}P_2(t);\end{gathered} \tag{2.10}$$

$$P_0(t) + P_1(t) + P_2(t) + P_3(t) = 1,$$

так как при любых t должно выполняться равенство $\sum_{i=1}^{3} P_i(t) = 1$.

Примем начальные условия в виде

$$P_0(0) = 1;$$
$$P_1(0) = P_2(0) = P_3(0) = 0.$$

Для проведения приближенных оценок надёжности идентификации личности найдём предельные стационарные состояния системы при $t \to \infty$.

Получим систему уравнений для трёх идентификаторов при обнулении левых частей системы (2.5), поскольку в стационарном устоявшемся потоке заявок претендентов на идентификацию производные равны нулю. Тогда:

$$\begin{gathered}
\tau_{01}P_0 = \tau_{10}P_1 + \tau_{20}P_2 + \tau_{30}P_3; \\
\tau_{01}P_0 = \tau_{12}P_1 + \tau_{10}P_1 = (\tau_{12} + \tau_{10})P_1; \\
\tau_{12}P_1 = \tau_{23}P_2 + \tau_{20}P_2 = (\tau_{23} + \tau_{20})P_2; \\
\tau_{23}P_2 = \tau_{34}P_3 + \tau_{30}P_3 = (\tau_{34} + \tau_{30})P_3; \\
P_0 + P_1 + P_2 + P_3 = 1
\end{gathered} \tag{2.11}$$

Отсюда получим:

$$\begin{gathered}
P_1 = \frac{\tau_{01}}{\tau_{10} + \tau_{12}} P_0; \\
P_2 = \frac{\tau_{12}}{\tau_{20} + \tau_{23}} P_1; \\
P_3 = \frac{\tau_{23}}{\tau_{30} + \tau_{34}} P_2; \\
P_0 = 1 - P_1 - P_2 - P_3
\end{gathered} \tag{2.12}$$

Рассмотрим возможные переходы из одного состояния системы в другое при предъявлении первого идентификатора. Для начала предположим, что в системе может быть всего 1 ошибочный идентификатор. Это равносильно тому, что претенденту предоставляется возможность всего один раз ввести идентификатор ошибочно, или при условии, что претендент не ошибся, система имеет ошибку при проверке правильно введённого идентификатора (это может происходить, например, когда ошибку внёс оператор, набивавший базу

данных идентификаторов). Тогда из состояния системы S_0 в состояние системы S_2 возможно всего два пути: «короткий» путь $\{0,1,2\}$ и "длинный" путь $\{0,1,0,1,2\}$; цифрами обозначены состояния системы.

При предъявлении второго идентификатора система возможных переходов может быть представлена векторами $\{0,1,2,3\}$, $\{0,1,0,1,2,3\}$, $\{0,1,2,0,1,2,3\}$, т.е. в первом случае отказов нет, во втором случае отказ происходит при предъявлении первого идентификатора, затем – второго.

Для системы с тремя предъявляемыми идентификаторами добавится ещё 4 вектора возможных переходов: $\{0,1,2,3,4\}$, $\{0,1,0,1,2,3,4\}$, $\{0,1,2,0,1,2,3,4\}$, $\{0,1,2,3,0,1,2,3,4\}$.

Таким образом, если принять число предъявляемых идентификаторов в системе за N, то общее число возможных векторов переходов будет равно $N + 1$. Если в системе допускается не один, а два разных ошибочных идентификатора, то число векторов перехода будет равно $2* N$. Исключением является случай $N = 1$, где мы считаем, что ошибочным может быть только один (единственный) идентификатор.

Заметим, что выражения для P_i как функции $P_i - 1$ в формуле (2.1) схожи при замене вероятностей переходов, что позволяет обобщить рассматриваемую систему на N идентификаторов. Рекуррентные соотношения будут иметь вид:

$$P_j = \frac{\tau_{ij}}{\tau_{ji} + \tau_{jk}} P_i \qquad (2.13)$$

где $j = i + 1, k = j + 1, i = 1,2, \dots, N.$

Для проведения дальнейшего решения необходимо оценить соотношение значений $\frac{\tau_{ij}}{\tau_{ji}+\tau_{jk}}$ из формулы (2.12). В рассматриваемой дроби значения τ_{ij} и τ_{jk} имеют одинаковый порядок величин, при этом $\tau_{ij} \in (0{,}5;\ 1]$, $\tau_{jk} \in (0{,}5;\ 1]$, а значение τ_{ji}, как правило, на два и более порядков меньше. Попробуем оценить верхнюю и нижнюю границы τ_{ji} из следующих соображений. Физический смысл τ_{ji} заключается в величине вероятности отказа идентификации при

предъявлении системе i-го идентификатора ID_i .

В общем случае для каждого идентификатора это соотношение может быть различным. Для поиска приближенных оценок τ_{ji} упростим задачу, определив нижнюю и верхнюю границу этой величины из подходов работы [35], считая главной составляющей τ_{ji} ошибки так называемого человеческого фактора.

Влияние человеческого фактора

При исследовании доверия к результатам идентификации необходимо учитывать влияние человеческого фактора на появление ошибок разного рода. Источниками ошибок разного рода (случайных, непреднамеренных, злонамеренных) в данном случае будут претендент (чаще всего это пользователь, пытающийся войти в систему), операторы, вводившие ИИ в момент регистрации пользователя в базе данных учетных записей ИС и в государственные реестры, а также сотрудники, осуществляющие в настройке подсистемы идентификации. Для упрощения задачи ошибками последней из указанных групп пренебрежём. Попробуем найти подход к оценке границ ошибок первых двух групп - претендента и операторов.

Вероятность появления ошибок операторов можно оценивать с помощью разных методов. Каждый из методов ориентирован на определённые виды деятельности операторов. Как правило, все разработанные методы основаны на вероятностном прогнозе оценки рисков (PRA – probabilistic risk assessment) и теории управления. В частности, некоторые из наиболее используемых методов рассматривались рабочими группами Международной федерацией информационных процессов (IFIP - International Federation for Information Processing). Наиболее известны методы корреляции надёжности человека в познавательной деятельности (HCRP – Human Cognitive Reliability Prediction), метод прогнозирования интенсивности ошибок человека (THERP – Technique for Human Error Rate Prediction), метод анализа надёжности работы человека и появления ошибок (SPAR – Standardized Plant Analysis Risk), разработанный

Эриком Холнагелом метод познавательной надёжности и анализа ошибок (CREAM – Cognitive Reability and Error Analysis Method). Для проведения оценок в рассматриваемом случае достаточно, согласно [35], удобно применять эмпирический метод оценки ошибок операторов (TESEO – Empirical Technique to Estimate Operators Errors) и способ оценки и снижения ошибок человека (HEART – Human Error Assessment and Reduction Technique [185]). Применим два этих метода к рассматриваемой в данной статье задаче.

В работе [35] показано, что при известных значениях вероятности $q_i, i = 1,2,..z$ ошибок операторов при выполнении ими предусмотренных z действий в рамках конкретного информационного взаимодействия вероятность безошибочного выполнения оператором процесса равна $P_1 = \prod_{i=1}^{z}(1 - q_i)$.

Если нет достаточных данных для определения вероятности P_1, то производится оптимистический прогноз надёжности оператора в виде $P_{БП} \leq P_2 = 1 - Q$, где Q- вероятность ошибки оператора, определённая по методу TESEO. Для оператора, вводящего 11-символьный СНИЛС, получим следующие оценки, пользуясь таблицей II.5.3 работы [35]: $P_{БП} \leq P_2 = 1 - Q = 1 - 0{,}01 * 0{,}5 * 1 * 1 * 1 = 0{,}95$.

Достоинство метода TESEO состоит в простоте, однако его применение не гарантирует приемлемый уровень точности прогноза.

В качестве второго дополнительного метода используем методику оценки вероятности ошибок операторов на основе статистических данных (Таблица 2.9) [35]:.

Таблица 2.9 – Вероятности ошибок человека-оператора

Вид ошибки	Вероятность ошибки
Ошибки считывания информации:	
– одинарного алфавитно-цифрового знака	$2 \cdot 10^{-4}$
– пятибуквенного слова при хорошем различении	$3 \cdot 10^{-4}$
– проверочного списка или цифрового показания	$1 \cdot 10^{-3}$

– десятизначного числа	$6 \cdot 10^{-3}$
Неисполнение отдельного требования при наличии памятки (инструкции) на рабочем месте	$1 \cdot 10^{-3}$
То же при отсутствии памятки и содержании в инструкции: – до 10 требований – более 10 требований	 $3 \cdot 10^{-3}$ $1 \cdot 10^{-2}$
Записи числовой информации (более 3 цифр)	10^{-3} на одну цифру

Также в работе [35] приведена информация, что ошибки операторов наиболее часто встречаются в ИС и наличествуют в 15% ÷ 30% от функционирующих информационных систем. Источниками ошибок могут быть:

– претендент на идентификацию (вводит идентификационную информацию самостоятельно);

– оператор, вводящий ИИ в БДУЗ ИС;

– оператор федеральной службы (ФНС, ПФР, ФМС), который вводил идентификационную информацию в поле с именем претендента в базу данных.

Ошибки претендента в системах идентификации зависят от длины вводимой информации и общего состояния его памяти. Для процесса первичной идентификации (но не для повторяющейся ежедневной идентификации при доступе к ИС) этой ошибкой можно пренебречь. Исключение составляет случай намеренного искажения ИИ (случай злоумышленника, который выдаёт себя за легального пользователя), который будет рассмотрен при исследовании надёжности процессов аутентификации.

Вероятность ошибки оператора, вводящего информацию в систему идентификации, оценим, исходя из анализа элементарных операций процедуры регистрации (ввод ФИО и СНИЛС). Представим, что в сертификат ключа проверки электронной подписи (СКПЭП) в нарушение Федерального закона «О персональных данных» №152-ФЗ [69] разрешили бы вводить данные паспорта владельца СКПЭП. В таком случае ошибка считывания информации

паспортных данных может быть оценена следующим образом. Серия и номер паспорта состоит из 10 числовых символов. Вероятность ошибки считывания при этом может составить величину $P_{сч.ц.} = 6 \cdot 10^{-3}$ (Таблица 2.9). Вероятность ошибки считывания места выдачи паспорта оценим как $P_{сч.м.} = 3 \cdot 10^{-4}$. Следовательно, суммарная ошибка считывания $P_{сч.}$ информации паспорта в предположении, что эти события независимы, может быть оценена как $P_{сч.} = 6{,}3 \cdot 10^{-3}$.

Вероятность ошибки записи информации о паспорте в систему для формирования запроса о достоверности паспортных данных может быть оценена «снизу» как вероятность ошибки введения 10-значного числа $Р\text{введ.запроса} = 10 \cdot 10^{-3} = 10^{-2}$. Такая оценка «снизу» согласуется с приведённым в таблице значением вероятности ошибочного ввода 10-тизначного числа как 0,06. Введя дополнительное предположение о том, что система проверки не даёт сбоев и ошибок, получаем оценку вероятности однократной ошибки проверки паспорта как перемножение вероятностей ошибок последовательных независимых операций: $P_{п.п.} = 6{,}3 \cdot 10^{-3}\ 6{,}0 \cdot 10^{-2} = 3{,}78 \cdot 10^{-4}$.

Оценкой вероятности ошибки «сверху», например, может служить база недействительных паспортов, которую можно найти на сайте МВД России. Число недействительных паспортов на 5 апреля 2020 г. составляло 1 048 576, население – 145 181 900, число выданных паспортов оценивается в 115 млн. штук [**Ошибка! Закладка не определена.**]. Следовательно, оценка вероятности однократной ошибки проверки паспорта – $0{,}9 \cdot 10^{-2}$.

На основании вышеизложенного оценим вероятность появления ошибки в паспортных данных для идентификации в пределах $10^{-4} – 10^{-2}$. Другими словами, если бы можно было вводить в СКПЭП паспортные данные, это не изменило бы кардинальным образом положение с достоверностью идентификации.

Повторно рассмотрим СНИЛС, используемый в качестве идентификатора для доступа к государственным услугам. СНИЛС застрахованного лица

не должен меняться со временем и состоит из следующих компонент: ххх-ххх-ххх уу, где ххх-ххх-ххх - порядковый номер застрахованного лица (9 цифр), уу - контрольное число (2 цифры). Страховой номер содержит все 9 цифр, включая ведущие нули. Страховые номера СНИЛС, содержащие три или более одинаковых цифр, идущих подряд, не присваиваются. Вероятность ошибки ввода значения СНИЛС можно оценить как ошибку ввода десятизначного числа $6{,}0 \cdot 10^{-3}$ и ошибку ввода ещё одной цифры $0{,}2 \cdot 10^{-3}$, в итоге получим $6{,}2 \cdot 10^{-3}$. С учётом проверки введенных значений условно можно принять вероятность ошибки порядка 10^{-3}. Для СНИЛС (также, как и для ИНН) проведенные рядом известных экспертов (например, приведенных в работе [144]) оценки дают среднее значение вероятности ошибки ввода оператором, близкое к 10^{-3}.

В качестве третьего метода используем метод HEART, как более точный, поскольку он предусматривает выбор значения вероятности человеческой ошибки из таблицы вероятностей ошибок операторов с перемножением на поправочные коэффициенты, также заданные таблично.

Применение метода HEART (табл.II.5.4 в работе [35]) в рассматриваемом случае даёт следующие оценки. Вероятность ошибки ввода СНИЛС оператором (Таблица 2.9) определим как ошибку: $Q_1 = 6{,}2 \cdot 10^{-3}$. Поправочные коэффициенты для рассматриваемой задачи могут только повысить это значение в полтора-два раза. В итоге оценки вероятности ошибки «сверху» (максимальной вероятной ошибки) может быть представлены как $Q_1 \sim 10^{-2}$.

Оценка ошибок при передаче информации

Проведем анализ ошибок при передаче сообщения. Пусть, например, типовое сообщение в системе идентификации и аутентификации, полученное от претендента на идентификацию представляет собой n последовательно передаваемых бит информации. Для проведения оценок ошибок воспользуемся подходом, приведенном в работе [35].

Предполагается, что канал биномиальный, т.е. вероятность k ошибок на длине сообщения n определяется как

$$P(k,n) = C_n^k p^k (1-p)^{n-k} \quad (2.14)$$

где p – вероятность ошибки на бит;

k – длина блока информационных бит;

$n = 112 + 8N,$ где N– количество байт данных сообщения; количество контрольных бит – 16 (код CRC)

При приеме сообщения должен быть реализован информационный процесс, включающий следующие составные части:

– проверка правильности типа пакета;

– определение адреса отправителя;

– определение адреса получателя;

– проверка длины сообщения;

– проверка правильности контрольных бит (проверка контрольной суммы).

Данные процессы в соответствии с уровнями иерархии упорядочиваются таким образом: 1-5; 2-4; 3-3; 4-2; 5-1.

При приеме сообщения процессы выполняются в обратном порядке: вначале выполняется процесс 5, затем 4, затем 3, затем 2, затем 1.

Вероятность ошибки (трансформации) всего сообщения в предположении, что вероятность $1 - (1 - \mathrm{p})^{16} \approx 1$, согласно [35], можно оценить:

$$G_N = \prod_{i=1}^{4} G_i \approx [1 - \frac{1}{2^{16}} \sum_{i=r+1}^{n} C_n^i p^i (1-p)^{n-i}] \cdot \prod_{j=1}^{4} \frac{2^{16} + 1 - K_j}{2^{16}} \quad (2.15)$$

Таким образом, в разделе выполнена оценка надежности идентификации пользователей при их доступе к информационным ресурсам в информационных системах класса БИС. Показана необходимость учета соотношения количества зарегистрированных пользователей и объектов в системе к числу ис-

пользуемых при доступе пользователей идентификаторов. Например, для системы ФНС России с числом зарегистрированных пользователей порядка 10^7 двух идентификаторов недостаточно и необходимо использовать не два, а, как минимум, три идентификатора длиной 10-12 символов с оценочным значением вероятности ошибки 10^{-3} для обеспечения надежности идентификации.

Альтернативным способом решения задачи могло быть применение международной системы идентификации объектов [186] – система OID (Object Identification). К числу достоинств данной системы относится уникальность объектов, обусловленная строгой иерархической структурой. К числу недостатков относится, в первую очередь, существенный рост числа индексов объектов при учёте большого числа объектов в крупных распределённых ИС, что сказывается на необходимости расширения места в соответствующем поле СКПЭП и времени его обработки. Из-за перечисленных недостатков применение системы OID ограничено.

Другим способом решения данной задачи является выпуск сертификатов доступа, рассмотренных в стандартах [54-56]. Введение дополнительных полей сертификата, содержащих три идентификатора, или, что возможно в ряде случаев, дополнительного «доверенного» идентификатора для конкретной ИС, также может позволить достичь более высокого уровня надёжности идентификации объектов и субъектов.

Моделирование процесса первичной идентификации

Моделирование процесса первичной идентификации для схем, представленных на рис.2.11 и рис.2.12, с помощью программного комплекса AnyLogic позволило провести параметрическое исследование влияния вероятностей появления ошибок идентификации при верификации каждого идентификатора для рассматриваемой схемы при общем количестве предъявляемых субъектом идентификаторов $n = 5$. В частности, выполнена оценка сверху и снизу потенциального влияния ошибок в двух из пяти идентификаторов на значение функции достоверности D для различных схем верификации [187].

Поскольку моделирование потоков заявок на идентификацию и их обработка в системе идентификации имеет протяженность во времени, по оси абсцисс о*x* отложено время обработки.

В работе [67] показано, что значения ошибок использования в качестве предъявляемой идентификационной информации идентификатора СНИЛС может иметь диапазон [0; 10^{-4}]. Значения ИНН – также диапазон [0; 10^{-4}].

В качестве варьируемых параметров принимались значения q_i вероятностей появления ошибок. Были заданы значения q_i =10^{-4} для i=1,2,3. Согласно рекомендациям работы [67] величина q_i варьировалась в пределах [0; 0,01]. Подразумевалось, что это мог быть как традиционный идентификационный атрибут, так и биометрическая характеристика с высокой надежностью идентификации. В качестве q_5 оценивалось влияние ошибок биометрии с невысокой надежностью результатов, вероятности ошибки варьировались в диапазоне [0; 0,3], поскольку значения ошибок при снятии биометрические характеристики голоса и лица согласно [146, 147] могут достигать величины 0,3.

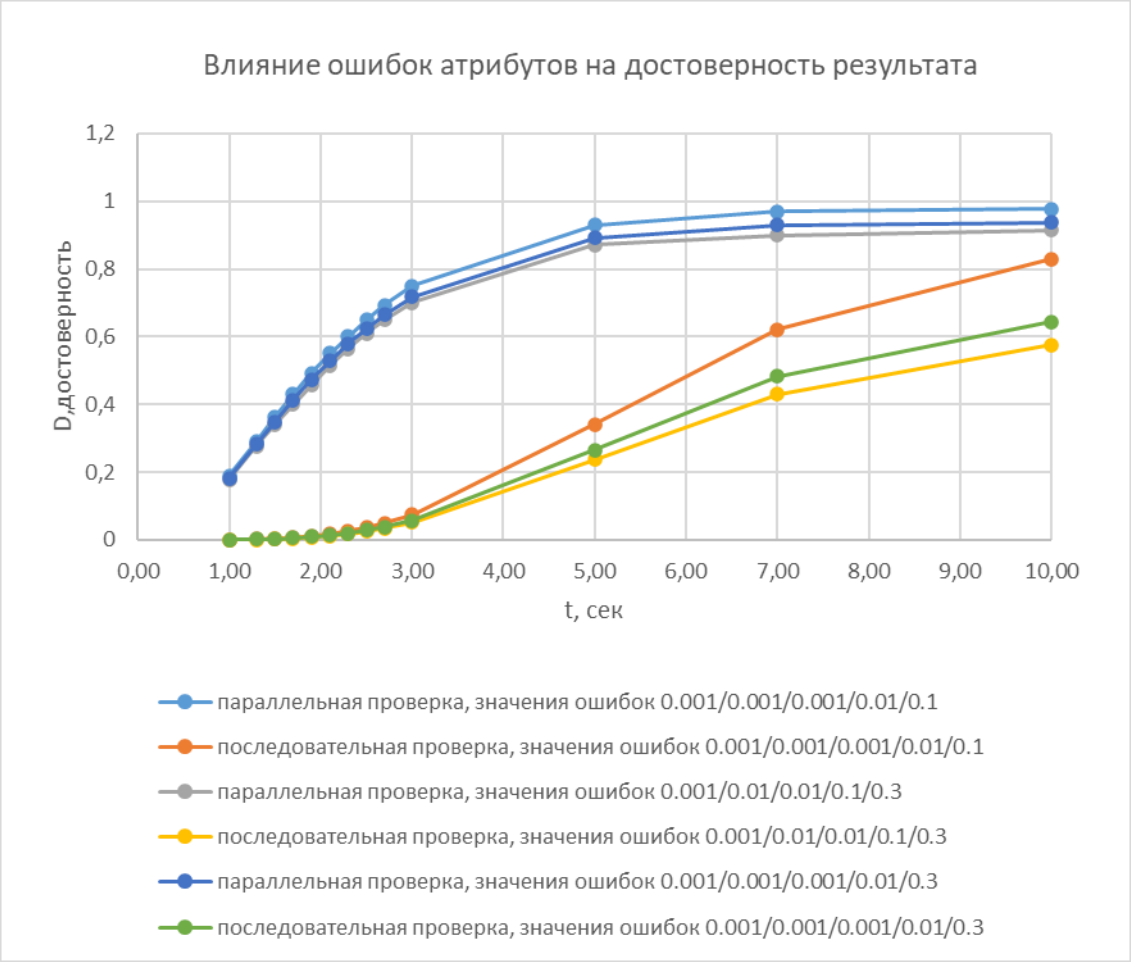

Рисунок 2.11. Параметрическое исследование влияния вероятностей появления ошибок при верификации идентификаторов (общее число идентификаторов=5) на функцию достоверности идентификации *D*.

Из представленных на рис.2.11 графиков видно, что при последовательной верификации пяти предъявленных идентификаторов величина ошибки достоверности первичной идентификации может достигать 40%, при параллельной – не более 10%. При этом величина вероятности появления ошибки одного из идентификаторов в 30% может привести к падению достоверности идентификации субъекта на 23% при последовательной верификации идентификаторов, и всего 6% при параллельной проверке идентификаторов. Анализ представленных графиков показывает, что уже к десятой секунде моделирования кривые приближаются к асимптотам, которые определяются соотношениями (2.11) и (2.12). Расчет асимптот для последовательной схемы верификации идентификационных атрибутов по формуле (2.11) приведен в таблице 2.10.

Таблица 2.10 – Расчет достоверности первичной идентификации для последовательной схемы верификации идентификационных атрибутов

q1	q2	q3	q4	q5	*D*
0,001	0,001	0,001	0,01	0,1	0,888
0,001	0,01	0,01	0,1	0,3	0,617
0,001	0,001	0,001	0,01	0,3	0,691

Для параллельной схемы проверки расчет значений достоверности по формуле (2.12) дали результаты, близкие к единице. В постановке данного исследования можно считать $D = 0{,}999$ для всех представленных на графике соотношений параметров.

Таким образом, моделирование процесса первичной идентификации с помощью программного комплекса AnyLogic в наглядной форме показало преимущество одновременной верификации представленных идентификационных атрибутов перед последовательной, а также дало результаты параметрического анализа влияния вероятностей появления ошибок на величину достоверности результатов идентификации субъекта. Приведенный пример расчета показал удовлетворительное совпадение (при $t \geq 10$) результатов расчетов с известными аналитическими решениями (2.11) и (2.12).

2.8 Оценка уровней доверия к результатам идентификации субъектов доступа

Согласно международным стандартам [61, 63] система идентификации должна быть защищена. Для обоснования и выбора средств защиты информации рекомендуется проводить классический анализ: на основе оценки рисков и анализа потенциальных угроз разрабатывается модель нарушителя, на основе которой производится выбор средств защиты. Главный вектор – защита самой СИА и ее данных, содержащих идентификационные атрибуты пользователей, от НСД. Особое внимание согласно положениям 152-ФЗ [69] следует обратить на защиту личных данных, содержащихся в идентификационных атрибутах. Кроме этого, необходимо строго периодически проводить анализ

рисков. Международные стандарты, разрабатываемые после 2018 г., рекомендуют применять шифрование перед тем, как ПДн отправляются в хранилище, а сами системы, обрабатывающие персональные данные, рекомендуют проектировать согласно принципам Security by design и Privacy by design. Безопасность не бывает абсолютной. Для ГИС и объектов КИИ введены уровни защищенности.

Согласно критериям доверия к результатам идентификации, разработанным в п.2.5, проведем оценку уровней доверия, достигнутым в результате идентификации.

Уровень безопасности системы идентификации и персональных данных, обрабатываемых в системе, предлагается измерять в безразмерных единицах. Введем функцию безопасности $\varphi_Б(t)$, значения которой могут изменяться от 0 до 1.

Достоверность результатов идентификации также оценивается в безразмерных величинах. Достоверность информации обычно оценивается как

D (t) = D± ΔD, где ΔD – доверительный интервал.*

Для грубых оценок достоверности рассмотрим модель на основе МКА, заключающуюся в том, что проверку каждого предъявленного идентификационного атрибута будем считать независимо (по надежности) работающим прибором.

Надёжность работы системы определяется соотношением (2.10), следовательно, достоверность идентификации $\varphi_д$ может быть оценена:

$$\varphi_д = 1 - q_1(t) * q_2(t) * \dots * q_n = 1 - \prod_{i=1}^{n}(1 - p_i(t)) \qquad (2.29)$$

где q_i - вероятность ошибки работы подсистемы при сравнении *i*-го идентификационного атрибута, $p_i\ (t)$ – вероятность отсутствия ошибки.

Утверждение. В больших системах с числом пользователей *K* (современные ИС уже имеют количество пользователей до значения $K=10^6$-10^8) для выполнения основной функции идентификации - уникальности и различимости

каждого субъекта из общего количества пользователей необходимо достигать значение достоверности идентификации не ниже

$$\varphi_д = 1 - 1/(K+1) \quad (2.30)$$

Таким образом, пространство решений функции доверия к результатам идентификации $\Theta(t) = \Theta(\varphi_Б(t)\varphi_д(t), \varphi_н(t))$ (2.29) может быть представлено в виде некой объемной фигуры, ограниченной единичным кубом (рис.2.9)

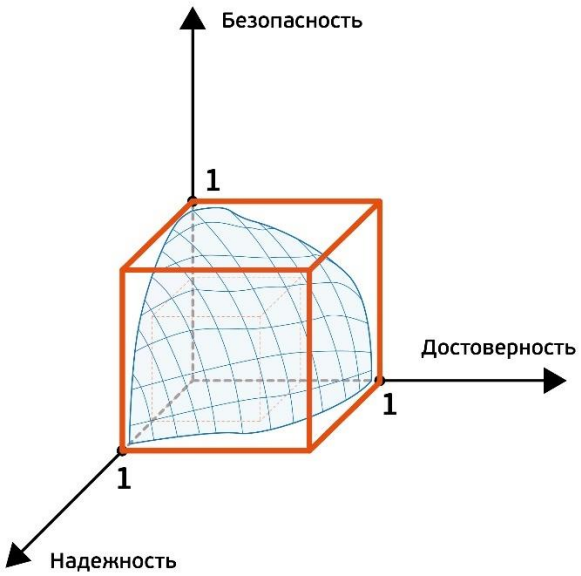

Рисунок 2.9. Пространство решений ψ [$\varphi_Б(t)$, $\varphi_д(t)$, $\varphi_н(t)$]

Форма и вид указанной объемной фигуры будет определяться параметрами конкретной ИС. Тем не менее, можно говорить о степени связанности функций безопасности, надежности и достоверности.

От степени связанности будет зависеть и представление уровней доверия. Если не связаны – вложенные кубы в единичном пространстве, если связаны – эллипсы, близкие к окружностям. Форма полученного безразмерного пространства доверия к идентификации ψ [$\varphi_Б(t)$, $\varphi_д(t)$, $\varphi_н(t)$], которое может в ряде случаев быть вычислено, зависит от степени связи, которую предстоит исследовать.

ВЫВОДЫ ПО ГЛАВЕ 2

По результатам проведенных исследований можно сделать следующие выводы:

1. На основе анализа материалов по теме диссертации, рассмотренных в первой главе, предложена методология формирования иерархии доверия к результатам идентификации и аутентификации, основанная на международных и национальных стандартах системы ГОСТ Р, а также результатах научных исследований. Представлены онтология и состав методологии, позволяющей формировать уровни доверия, а также проводить оценки доверия к результатам идентификации и аутентификации.

2. Сформулирована задача идентификации субъектов доступа в современных информационных системах. Идентификация в условиях роста количества субъектов и объектов в ИС становится нетривиальной задачей и выдвигает новые требования к длине идентификаторов или их количеству. Установлена зависимость необходимого количества идентификаторов с известными оценками безошибочности идентификации от числа зарегистрированных в ИС субъектов и объектов доступа.

3. Выполнен структурно-функциональный анализ процессов идентификации. Предложены модели и разработана методика оценки надежности идентификации. Приведены оценки надежности первичной идентификации, а также оценки ошибок идентификационной информации и ошибок при верификации, а также при передаче идентификационной информации;

4. Впервые введены понятия первичной и вторичной идентификации. Сформулированы цели, задачи и требования к первичной и вторичной идентификации. Установлено, что доверие к результатам идентификации определяется главным образом результатами первичной идентификации. Доверие к результатам первичной идентификации в свою очередь, зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем идентификационных атрибутов, доверия к результатам верификации этих иденти-

фикационных атрибутов и доверия к привязке идентификационной информации к конкретной личности заявителя. Указанные положения вошли в первый национальный стандарт ГОСТ Р ХХХ-2019 «Идентификация и аутентификация. Общие положения» и в проект ГОСТ Р ХХХ-2019 «Идентификация и аутентификация. Уровни доверия к результатам идентификации», куда также введены основные понятия и основные положения организации процессов идентификации с целью достижения определенных уровней доверия к полученным результатам.

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

6. Проведен параметрический анализ влияния ошибок верификации двух из пяти предъявленных идентификационных атрибутов для двух моделей процесса первичной идентификации – последовательной и параллельной верификации предъявленных заявителем идентификационных атрибутов. Анализ проведен с помощью имитационного моделирования. Показано, что для достижения заданного уровня доверия к результатам более эффективной является параллельная организация процедуры верификации.

7. Рассмотрены наиболее распространенные методы биометрической идентификации. Показаны пределы изменения достоверности результатов идентификации, полученных с помощью биометрических характеристик, для двух моделей процесса первичной идентификации – последовательной и параллельной верификации предъявленных заявителем идентификационных атрибутов. Установлено, что при применении для идентификации исключительно биометрических методов идентификации без использования традиционных методов, использующих государственные базы идентификаторов населения, уровень доверия к результатам идентификации будет низким. Тем не менее, биометрическую идентификацию рекомендуется использовать в качестве дополнительного фактора идентификации и привязки цифровых данных к личности субъекта доступа и для обеспечения неотказуемости от процесса регистрации

нового пользователя информационной системы. При этом особенно эффективно использовать видеозапись снятия биометрических характеристик.

8. Впервые проведена оценка рисков первичной идентификации. Рассмотрены типовые угрозы и возможные атаки, идентифицированы основные риски первичной идентификации, которые согласно ГОСТ Р 31010 рассмотрены в виде набора вероятных опасных событий (ВОС). Для этого набора ВОС построены матрицы рисков, анализ которых позволил определить уровни допустимых рисков для трех наиболее распространенных типов информационных систем (ИС): закрытых (корпоративных), открытых ИС с личной явкой нового пользователя к регистратору и открытых ИС без личной явки субъекта к регистратору.

9. Установлено, что уровень рисков первичной идентификации для открытых систем на порядок выше, чем для корпоративных, при этом наибольший риск представляет регистрация нового пользователя в удаленном режиме без личного присутствия. Получены оценки средних значений рисков по отношению к допустимому уровню рисков для всех рассмотренных комбинаций.

10. На основе проведенных исследований сформулированы критерии доверия и приведен способ оценки доверия к результатам идентификации в соответствии с предложенными критериями для ИС различного назначения.

8. Проведена оценка надежности первичной идентификации субъектов доступа для больших информационных систем. Показана необходимость учета соотношения количества зарегистрированных пользователей и объектов в системе к числу используемых при доступе пользователей идентификаторов. Например, для систем с числом зарегистрированных пользователей порядка 10^7 двух идентификаторов недостаточно и необходимо использовать не два, а, как минимум, три идентификатора длиной 10-12 символов с оценочным значением вероятности ошибки 10^{-3} для обеспечения надежности идентификации.

3 Методология формирования иерархии уровней доверия к результатам аутентификации субъектов доступа

Анализ многолетней практики создания и эксплуатации систем аутентификации показывает, что системы ИА относятся к классу интеллектуальных систем [8, 10] описание которых в силу разнообразия применяемых технологий, механизмов и средств требует системного подхода.

В работе [188] при описании сложных систем предлагается использование принципов:

- цели;
- многоуровневого описания;
- классификации.

Рассмотрим, как можно применить эти принципы для систематизации и классификации процессов ИА. Введем следующие обозначения:

- цели ИА обозначим в виде $G = G\{ST, SO, NA, OK\}$;
- структурное описание системы – множество $SS\{ST, SO\}$;
- состояния системы – множество $S = S\{ST, SO, NA\}$;
- входящий поток заявок на ИА – λ;
- поток выполнения заявок системой ИА - μ;
- множество угроз $V = V\{ST, UA, CA\}$;
- множество атак $A = A\{ST, UA, CA\}$;
- множество уязвимостей: $U = U\{ST, SO, NA\}$.

Заметим, что корректное решение задач ИА участников удаленного электронного взаимодействия не является тривиальным процессом, поэтому при выборе и внедрении тех или иных решений необходимо понимать возможности, ограничения и уровень доверия к используемым механизмам и средствам аутентификации.

3.1 Основные характеристики процесса аутентификации субъектов доступа

В процессах аутентификации участвуют практически все пользователи компьютеров, ИС и прикладных программ. Взаимодействие субъекта доступа с системой идентификации и аутентификации начинается с включения компьютера. После успешного прохождения процедуры идентификации, критерием которой является совпадение введенного субъектом идентификатора с имеющимся в системе, аутентификацию проходят, чтобы получить доступ к компьютеру, локальной сети, Интернету, распределенной сети, к системам защиты от НСД, к виртуальным частным сетям [189], приложениям [**Ошибка! Закладка не определена.**, 27, 190]. Особое место занимает аутентификация при беспроводном [191], удаленном сетевом доступе к корпоративным сетям и ресурсам [192, 193], в том числе при переходе к облачным вычислениям [194].

Примерами взаимодействующих сторон, которые могут быть идентифицированы и аутентифицированы, кроме пользователей, могут быть процессы, открытые ИС, логические объекты и т.д. Классическая задача ИА решается для взаимодействия пользователь – сервер ИА с распространением этого решения на другие объекты взаимодействия.

В процессе аутентификации взаимодействующие объекты и субъекты обмениваются АИ. Используются следующие типы аутентификационной информации [53]:

- предъявляемая АИ;
- данные, необходимые для аутентификации (Рисунок 3.1).

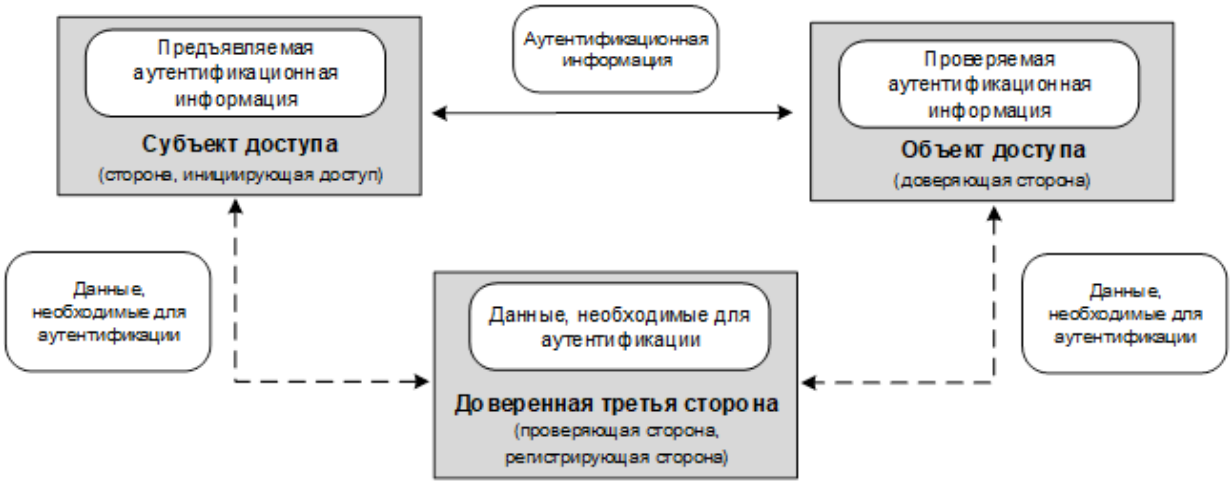

Рисунок 3.1 – Обмен аутентификационной информацией между претендентом на доступ, проверяющей стороной и ДТС при аутентификации

При некоторых схемах аутентификации претенденту может понадобиться обращение к доверенной третьей стороне (ДТС). Аналогично, и проверяющая сторона может обратиться в ДТС с целью проведения обмена АИ. В таких случаях ДТС может хранить проверочную АИ, относящуюся в соответствующей взаимодействующей стороне. Существуют схемы аутентификации, в которых ДТС используется для доставки АИ, предназначенной для обмена в процедуре аутентификации. Большинство реальных схем аутентификации построены без участия ДТС. Однако существуют бизнес-задачи, в которых аутентификация подразумевает наличие ДТС в системе аутентификации. Типичным примером является трансграничный обмен подписанными электронными документами, где ДТС с каждой стороны отвечает за проверку валидности цифровых сертификатов доступа и сертификатов ключей проверки электронной подписи, а также за хранение АИ при обмене. Вторым и наиболее распространённым примером является ДТС в виде корпоративного удостоверяющего центра, отвечающего за выпуск цифровых сертификатов доступа и сертификатов ключа проверки электронной подписи (СКПЭП). В случае корпоративной сети с поддержкой ИОК одним из распространённых случаев является схема с ДТС для локальной сети и протоколом аутентификации Kerberos.

Проверяющая сторона в корпоративной сети чаще всего представляет

собой сервер аутентификации. В зависимости от числа пользователей и задач ИА в системе аутентификации может быть несколько серверов, связанных между собой доверенным (trust) образом – сервер аутентификации, сервер управления учётными записями пользователей (IdM – сервер, сервер управления идентификацией и доступом пользователей), сервера управления удалённым сетевым доступом (типичные примеры – сервера RADIUS– RFC 2865 и RFC 2866 или DIAMETER – RFC 3588 и RFC 6733).

В упрощённом виде классическая процедура ИА со стороны пользователя (клиентская часть) достаточна для рассмотрения процесса ИА в закрытой (локальной) корпоративной системе, где многие процедуры (например, процедура регистрации пользователей) строго регулируются внутренними регламентами (Рисунок 3.2). С учётом развития информационных технологий, в том числе, технологий предоставления доступа, и появления нового класса ИС – систем ИСОП (см. Введение) при изучении процессов ИА необходимо рассматривать весь цикл необходимых процедур, составляющих процесс аутентификации. Прежде чем рассматривать процесс ИА, определим участников процессов аутентификации:

– субъект доступа (называемый также до аутентификации аппликант, претендент);

– центр регистрации – его основной задачей является установление и фиксация (закрепление) связи субъекта и его уникального секретного признака – аутентификатора. Таким центром может выступать, например, удалённый центр регистрации удостоверяющего центра, связанный доверительными отношениями с данным УЦ;

– доверяющая сторона – владелец того ресурса, к которому претендует получить доступ субъект доступа. Он проверяет по протоколу аутентификации факт владения субъектом доступа соответствующим аутентификатором – секретом, который выдан субъекту ЦР-ом;

– проверяющая сторона (центр валидации, ЦВ), входит в состав инфра-

структуры открытых ключей (ИОК), - выполняет проверку наличия фиксированной ЦР-ом связи «субъект доступа – аутентификатор» и проверяет, является ли ЭУ действительным (валидным) на момент проверки.

Может иметь место объединение отдельных сущностей в одном лице. Например, ЦР, ЦВ и доверяющая сторона могут быть объединены в одну единую структуру.

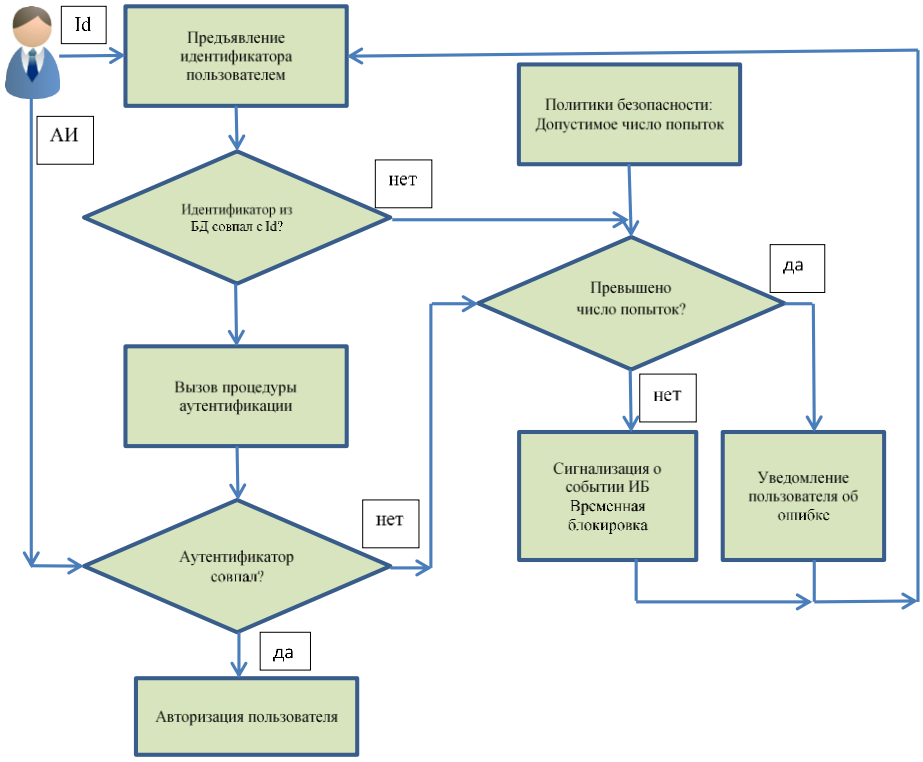

Рисунок 3.2 – Упрощённый вид процесса «Идентификация и аутентификация»

Рассмотрим составные части ИА и участников взаимодействия более подробно, основываясь на результатах работы [128].

Этапы аутентификации

Идентификация и аутентификация включают три основных этапа. Первый этап является регистрацией, которая распадается на цепочки последовательно выполняемых взаимосвязанных действий:

– Субъект (претендент или аппликант) обращается в ЦР с целью стать

пользователем ИС. Заявитель предъявляет в ЦР свои Credentials (ЭУ или бумажные действующие удостоверения личности, содержащие присвоенные ему идентификационные атрибуты и их значения. Примерами значений идентификационного атрибута являются: номер паспорта, номер удостоверения, СНИЛС, ИНН).

– ЦР проверяет предъявленные бумажные документы на подлинность и действительность (валидация). Предъявленное электронное удостоверение (ЭУ) также проверяется на предмет достоверности содержания и его действительности (валидация). Также проверяется уникальность совокупности предъявленных идентификационных атрибутов, проводится их верификация (проверка с помощью запросов, как правило, в государственные реестры) и определяется степень связи проверенных идентификационных данных с конкретной личностью заявителя. Если хоть одно из перечисленных условий (уникальность, подтверждение из официальных источников, степень привязки цифровых данных к субъекту) не соответствует требованиям и уровням доверия к полученным результатам, принятым в конкретной ИС, то аппликант получает отказ в регистрации.

– На основании выполненной проверки ЦР создаёт учётную запись для данного субъекта в базе данных ЦР для доступа к информационным ресурсам (ресурсу), содержащую уникальный идентификатор, присвоенный новому субъекту доступа, и всю проверочную информацию, связанную с данным субъектом.

– На основе полученной учетной записи для субъекта ЦР издаёт/регистрирует секрет (аутентификатор), ассоциированный с конкретным субъектом. Простейшим секретом может быть сформированный по тому или иному установленному алгоритму пароль, усиленным секретом - одноразовый пароль (OTP) или комбинация OTP + многоразовый пароль. Самым строгим секретом является секретный ключ, который согласно нормативно-правовой базе может быть сформирован либо самим субъектом, либо ЦР-ом. Для данного

секретного ключа на основе соответствующего открытого ключа в ЦР формируется сертификат ключа подписи (ЭУ - электронное удостоверение, в западных документах аналогом является Credentials – часть учетной записи), связывающий секретный ключ (аутентификатор) с его владельцем. В простейшем случае процесс издания ЭУ сводится к регистрации пары логин-пароль. В самых сложных случаях для одного субъекта может быть издано несколько ЭУ (например, сертификаты ключа подписи, ключа шифрования, ключа логического доступа). Фактически ЭУ является своего рода «электронным паспортом», имеющим реквизиты издателя, время, место издания, срок действия, алгоритм формирования (издания), процедуру проверки (например, цепочки доверия) и т.д.

– Далее следует необязательная процедура делегирования прав доступа (фактически делегирование доверия к изданным аутентификатору и ЭУ) другой (или другим) ИС на основе доверительных отношений. При переходе к облачным вычислениям эта процедура становится весьма актуальной.

- Последней процедурой регистрации является выдача изданных ЦР-ом аутентификатора и ЭУ на руки субъекту. Подробно этап регистрации рассмотрен в главе 2 в разделе «первичная идентификация».

Второй этап аутентификации называется обмен аутентификационной информацией с целью подтверждения подлинности предъявленного идентификатора. Данный этап включает:

– Хранение секрета (аутентификатора) и ЭУ. Как уже было показано выше, самым строгим секретом является закрытый ключ. Если в виде аутентификатора используется ключ электронной подписи (это достаточно частый случай на практике), то за его хранение, согласно ст.10 Федерального закона [72], при использовании усиленных электронных подписей участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия, а также не использо-

вать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена». Как показано в работах [194, 195], лучшим средством хранения секретного ключа (ключа проверки подписи) является применение для генерации, хранения и использования устройств класса SSCD (Secure Signature Creation Device – устройство безопасной генерации подписи). Это согласуется с рекомендациями [196] и требованиями стандартов [197, 198, 199]. Если в виде аутентификатора используется другой секрет (пароль, одноразовый пароль и др.), то в зависимости от типа организации, где работает пользователь, управление секретом подчиняется определённым политикам безопасности. Например, в ряде государственных органов для аутентификации в некоторых приложениях строго через определённый период генерируются N-символьные пароли по закону случайных чисел и сразу автоматически записываются в защищённую память электронных ключей таким образом, что пользователь даже не знает своего пароля.

– Инициирование обмена путем предъявления претендентом идентификатора доверяющей стороне. Простейшими примерами предъявления идентификатора является ввод логина после включения компьютера или при входе в электронную почту (в данном примере логин совпадает с названием персонального почтового ящика). После ввода претендентом логина СИА сравнивает предъявленный идентификатор с зарегистрированным в базе пользователей, и в случае совпадения просит предъявить аутентификатор для подтверждения подлинности идентификатора.

– Процедура обмена аутентификационной информацией. Простейшим аутентификатором является пароль. В современных протоколах сетевой аутентификации обычно многоразовый пароль не передается по сети в открытом виде [28]. Одноразовые пароли передаются по сети в открытом виде, однако для их генерации используется вектор начальной инициализации. К тому же перехваченный OTP-пароль достаточно проблематично использовать - для каждой следующей сессии используется новый OTP. Тем не менее, практиче-

ские реализации OTP-аутентификации зависят от квалификации специалистов, проектирующих и настраивающих данное решение, и такую возможность (и связанную с ней уязвимости) не стоит сбрасывать со счетов. При применении протоколов на основе PKI сообщения перед отправкой подписываются сторонами и обмен (challenge-response) производится уже зашифрованными сообщениями. При положительном результате обмена аутентификационной информацией доверяющая сторона самостоятельно или с помощью проверяющей стороны инициирует этап валидации.

Третий этап называется валидацией. Проверка валидности ЭУ (сертификата ключа подписи) – это действия, производимые над проверяемым сертификатом ключа подписи для того, чтобы убедиться в возможности его использования. Проверка подписи распадается на 3 этапа:

з) собственно криптография, вычисление формулы подписи (с этим достаточно просто, имеются СКЗИ, произведенные согласно требованиям ФСБ России);

– построение цепочки сертификации (полное отсутствие в РФ методик, единственное, что есть созвучное, так это методики, разработанные NIST [98, 120, 200], но они используют алгоритмы RSA);

– определение полномочий осуществляется на уровне приложения, когда имеется решение о достаточном уровне полномочий в конкретной транзакции). Валидация состоит из следующих процедур: проверки валидности ЭУ и пути сертификации (цепочки сертификатов) ЭУ. Путь считается валидным, если первый сертификат издан пунктом доверия, последний сертификат издан для конечного данного объекта и содержит данный открытый ключ, имена издателей и субъектов сертификатов (кроме первого и последнего) образуют непрерывную последовательность – имя издателя текущего сертификата совпадает с именем субъекта предыдущего сертификата. При этом важно, чтобы период действия сертификатов цепочки не истёк на момент проверки. Таким образом, проверяется срок действия ЭУ – проверяется в поле Validity по датам начала действия и конца действия, действенность ЭУ – текущий статус, т.е.

отсутствие ЭУ (сертификата ключа подписи) в актуальном списке отозванных сертификатов ключей подписей. Эта проверка производится либо с помощью доверенного сервиса OCSP, либо проверяется, нет ли данного сертификата в списке отозванных Delta CRL, либо с помощью сервиса XKMS [201]; проверяется область действия, а при необходимости, и другие поля ЭУ (например, для атрибутных сертификатов).

Перечисленные процедуры по валидации ЭУ должны выполняться средствами квалифицированных доверенных сервисов УЦ. Актуальной задачей является разработка регламентов к процедурам регистрации и процедуре хранения секрета, особенно сотрудниками государственных органов, а также к процедурам валидации. Такие требования и регламенты пока не сформулированы. Чтобы перейти к перечисленным задачам, необходимо четко описать функциональные требования к исследуемым системам и рассмотреть условия их работы. Сначала рассмотрим место системы ИА в общей системе управления доступом.

В целом корпоративные СИА хорошо изучены, их подробное описание, архитектуру и типовой состав можно найти в литературе [10, 13, 28, 30, 40]. Как было показано в первой главе, подавляющая часть нормативной базы разработана для закрытых систем.

На функционально-структурной схеме клиентской части типовой СИА (Рисунок 3.3) видно, что основные функции управления, такие, как разграничение доступа механизмы ИА, а также политики и правила безопасности, сосредоточены в руках администратора безопасности. Такие же принципы управления безопасностью и механизмами разграничения прав доступа, а также способами ИА должны быть распространены на ИСОП. тем более, что для открытых систем общего пользования добавляется, а зачастую является одним из основных видов Web-доступ.

Рисунок 3.3 – Типовая функциональная схема клиентской части СИА

На рисунке, отображающем архитектуру ЕСИА (Рисунок 3.4), которая являющаяся ярким примером современных СИА для ИСОП, видно, что для организации защищённого Web- доступа модуль аутентификации содержит блоки, предназначенные для ИА пользователей с использованием универсальной электронной карты, карты электронного правительства, OTP и паролей (кодов доступа).

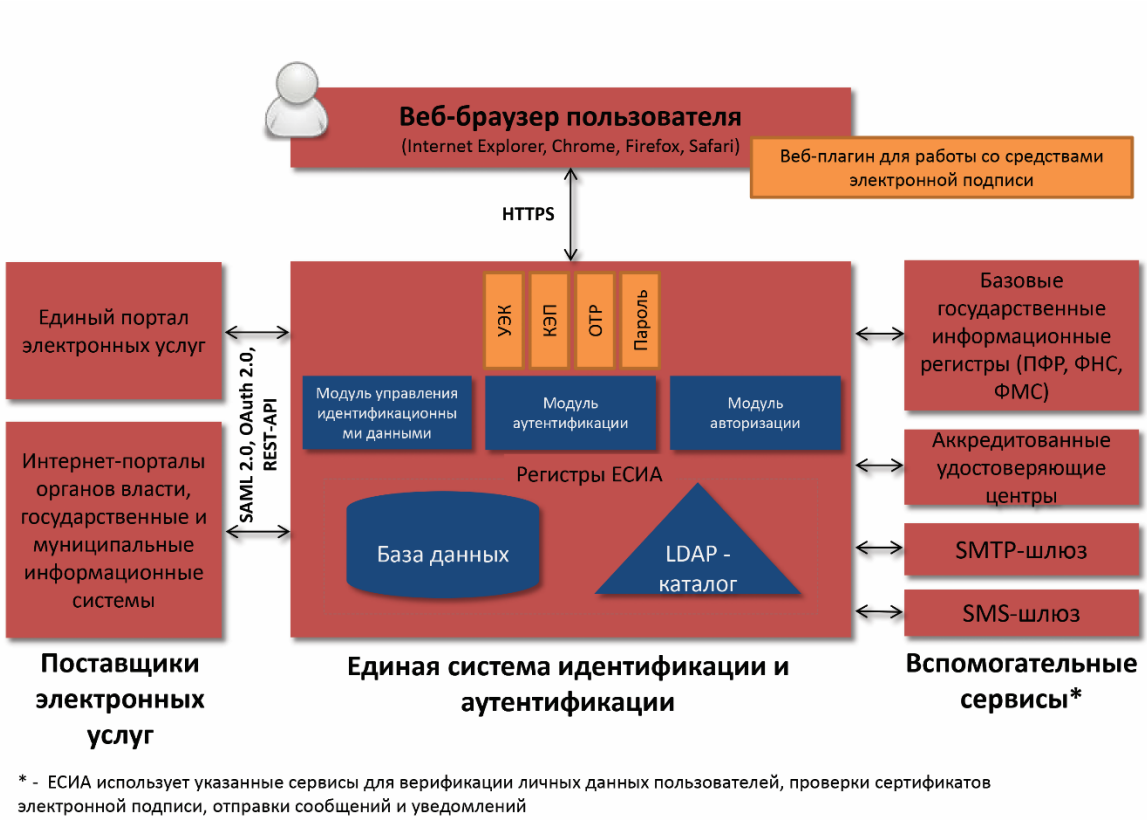

Рисунок 3.4 – Архитектура ЕСИА

Схема доступа, основные функции и механизмы аутентификации при Web-доступе к информационным ресурсам портала государственных услуг подробно описаны в работе [141].

При всей широчайшей распространённости СИА вопросы организации таких сложных систем, использования в них тех или иных технологий и механизмов ИА, проблемы надёжности и безопасности СИА недостаточно изучены, и, следовательно, далеко не в полной мере формализованы. Для изучения многообразия существующих и проектируемых СИА с учетом разной степени сложности их реализации необходимо предварительно классифицировать данный тип ИС с целью выработки адекватных подходов к исследованию характеристик надёжности и безопасности в зависимости от назначения, состава, применяемых технологий ИА.

3.2 Классификация процесса и систем аутентификации субъектов доступа

Возможно, из-за сложности данной темы, вопросам классификации СИА в открытых источниках автором данной статьи найдено всего две работы [41,202]. Разработанная более 15 лет назад Р. Смитом классификация СИА касается, главным образом, вопросов ИА при предоставлении сетевого доступа пользователей корпоративных ИС. Основным механизмом аутентификации является пароль. За прошедшие годы технологии далеко шагнули вперед, предложенная Р. Смитом классификация представляется неполной и устаревшей, а терминология, возможно, из-за неудачного перевода, не представляется общепринятой. К сожалению, эта классификация была повторена в [41].

Рассмотрим, как можно применить принципы системного подхода, рассмотренные в начале этой главы, к систематизации и классификации процессов ИА.

Принцип цели. Попробуем выделить основные цели создания СИА. Согласно [4] и результатам работы [131], двумя основными целями процесса аутентификации являются:

– аутентификация сторон при УЭВ;

– аутентификация источника данных.

Аутентификация сторон, как правило, является он-лайн сервисом безопасности, основными задачами которого являются:

– подтверждение предъявленного идентификатора в целях дальнейшего предоставления доступа к информационному ресурсу или сети;

– идентификация владельца электронной подписи и обеспечение неотказуемости при применении ЭП;

– установление доверительных отношений при УЭВ.

Первая задача в полной мере применима к СИА, поскольку системы управления доступом пользователей ИС или отдельных информационных ресурсов включают в себя СИА как одной из подсистем. Задачи идентификация

владельца ЭП и обеспечение неотказуемости при подписи электронного документа входят в задачу предоставления доступа к модулям прикладного программного обеспечения, использующим подпись как одного из сервисов безопасности. Другими словами, задачи идентификации и обеспечения неотказуемости также сводятся к задаче управления доступом. Задача установления доверительных отношений является более сложной, т.к. участниками взаимодействия могут являться пары «устройство – устройство» (класс задач M2M), «пользователь-устройство» (например, широко применяемая клиент-серверная схема) и «пользователь-пользователь». Задачи класса M2M могут решаться как службами СИА, так и в рамках сетевых инфраструктурных настроек (например, IPsec). Задачи аутентификации пользователь-устройство также могут решаться как СИА, так и вне ее (пример: SSL – Secure Socket Layer). Задача установления доверительных отношений пользователь-пользователь может входить в функционал СИА, а может решаться с помощью других механизмов, примером в данном случае может являться почта PGP- Pretty Good Privacy.

Аутентификация источника данных является офф-лайн сервисом, основным механизмом которого является проверка электронной подписи источника данных. Как правило, эта задача пока не входит в функционал СИА.

Классификация систем идентификации и аутентификации

Таким образом, основной целью СИА является подтверждение идентификации зарегистрированного в ИС пользователя для управления его доступом.

Принцип многоуровневого описания. Подробное описание процессов аутентификации выполнено в работе [128]. Показано, что процесс аутентификации состоит из взаимосвязанной цепочки последовательно выполняемых процедур, разделяющихся на два класса по отношению к времени их выполнения. К первому (подготовительному) классу относятся процедуры регистрации нового пользователя ИС (однократно выполняемая процедура) и хранения

аутентификационной информации (как правило, процесс, длящийся во времени), ко второму классу относятся процедуры предъявления АИ, протоколы обмена «претендент – проверяющая сторона», валидации и принятия решения о результате прохождения претендентом процесса аутентификации. Процедуры второго класса проводятся быстро (ка правило, не более 1-2 секунд) при каждой попытке доступа к информационным ресурсам ИС.

Принципы многоуровневого моделирования каждой процедуры представлен в работах [161, 203]. Детализированное рассмотрение процессов и механизмов установления доверительных отношений при УЭВ приводится в работе [204].

На основе рассмотренных в указанных работах детализированных описаний можно выполнить классификацию СИА. При проведении классификации очень важным является выбор признаков и критериев, по которым производится классификация. Покажем, что предлагаемый подход позволяет выбрать признаки и определить критерии для классификации современных СИА.

Для определения признаков классификации СИА вспомним, что аутентификация является одним из важнейших сервисов информационной безопасности [137]. Следовательно, предлагаемый сервис безопасности должен обладать такими свойствами защищённости, как доступность, целостность, конфиденциальность.

Основными целями обеспечения доступности при этом будут являться: обеспечение гарантий обработки запросов пользователей на аутентификацию, разделение доступа пользователей, управление доступом, а также персонификация доступа, то есть жёсткая привязка идентификационной и аутентификационной информации пользователя к конкретной личности. В соответствии с указанными целями можно выделить задачи:

– обеспечения необходимой производительности обработки всех запросов легальных пользователей на аутентификацию при условии обеспечения доступности и отказоустойчивости сервера аутентификации,

– организации механизмов надёжной идентификации и аутентификации пользователей,

– обеспечения автоматизированных и подконтрольных (подлежащих записи и хранения записей, а также мониторингу) процедур заведения новых учётных записей, приостановки доступа пользователя (например, на период отпуска или болезни), изменения прав доступа и удаления УЗ,

– обеспечения персонификации доступа с помощью жёсткой привязки ИД и АИ к конкретному пользователю, желательно на основе предоставления доступа с применением цифровых сертификатов доступа пользователя при использовании механизма электронной подписи для аутентификации.

Свойство обеспечения целостности информации в СИА условно может быть разбито на цели защиты целостности программного обеспечения системы, УЗ и АИ пользователей в базе данных учётных записей, а также при генерации, хранении, предъявлении и передаче. При переходе к облачным вычислениям обеспечение целостности АИ в силу сложности решения может рассматриваться в виде отдельной цели. Задачи, связанные с достижением указанных целей обеспечения целостности, в целом совпадают с целями.

Согласно требованиям №152-ФЗ «О персональных данных» [69] в СИА должна обеспечиваться конфиденциальность УЗ и АИ пользователей. Для достижения указанных целей можно сформулировать следующие задачи:

– для обеспечения конфиденциальности УЗ пользователей необходимо разработать комплекс мер по защите сервера базы данных учётных записей (БДУЗ) пользователей, строго ограничить и контролировать доступ к указанной базе данных, организовать хранение в БДУЗ паролей только в хешированном виде, обеспечить конфиденциальность векторов инициализации при генерации одноразовых паролей, а также обеспечить надёжную защиту персональных данных пользователей при хранении и передаче в БДУЗ;

– в целях обеспечения конфиденциальности АИ пользователей при генерации, выдаче, хранении, предъявлении и протоколах обмена необходимо

применять комплекс мер по обеспечению ИБ на основе оценки рисков применительно к конкретной ИС, при этом особое внимание рекомендуется обратить на использование безопасных технологий, механизмов и средств идентификации и аутентификации.

Как показано в работе [164], АИ пользователей лучше всего защищена при использовании в виде механизма аутентификации электронной подписи, при этом согласно Директиве о применении электронной подписи [205] наиболее безопасно применять персональные пользовательские устройства класса SSCD, специально спроектированных по требованиям ИБ для генерации ключевого материала и проведения криптографических операций внутри чипа, и гарантирующих неизвлекаемость закрытого ключа. В принятом в июле 2014 г. Советом Европы документе eIDAS (Положение 910/2014 об электронной идентификации, аутентификации и электронной подписи) [206] требование SSCD усилено и заменено на QSCD (Qualified Signature Creation Device – квалифицированные устройства аппаратной генерации ключевой информации).

Классификация СИА осуществляется по признакам выполнения основных целей и вытекающих из них задач ИБ, а также методов их решения (Рисунок 3.5).

Цели	Задачи	I уровень доверия	II уровень доверия	III уровень доверия	
Доступность	Гарантии обработки запросов на аутентификацию	Отказоустойчивость СИА, обеспечение необходимой производительности	Допустима очередь заявок	Ограничение длины очереди	Гарантированное обслуживание с ограничением длины очереди	Треб. ФН
	Разделение доступа	Идентификация пользователя Аутентификация пользователя	Вероятность ошибки идентификации 10^{-4}-10^{-2}	Вероятность ошибки идентификации 10^{-6}-10^{-4}	Вероятность ошибки идентификации 10^{-8}-10^{-6}	
	Управление доступом	Заведение новой учетной записи (УЗ), приостановка доступа, отзыв, изменение прав доступа, удаление УЗ	Соблюдение регламента	Неквалифицированный сертификат доступа	Квалифицированный сертификат доступа	
	Персонификация доступа	Жесткая привязка ИД и АИ к конкретному пользователю	Уникальный профиль доступа	Неквалифицированный сертификат доступа или OTP	Квалифицированный сертификат доступа	
Конфиденциальность	Конфиденциальность учетных записей	Защита БДУЗ от НСД	Защита от НСД орг. мерами, хэширование учетных записей	Усиленная защита от НСД	Qualified Signature Creation Device	Требования ИБ к системе идентификации и аутентификации
	Конфиденциальность АИ пользователя	Запрет экспорта ключей, орг. и тех. меры защиты АИ от НСД	Пользователь несет ответственность за сохранение пароля в тайне	Security Signature Creation Device или SSO+Смарт-карта	Шифрование учетных записей, хэширование ИД и АИ	
	Конфиденциальность ПДн пользователя	Обеспечение защиты ПДн пользователя	Защита БДУЗ от НСД	Выполнение регламента по защите БДУЗ от НСД	Шифрование ПДн в БДУЗ	
Целостность	Целостность системного и прикладного ПО ПсИА	Обеспечение целостности ПО ПсИА и клиенского ПО	Программные средства контроля целостности	Комбинированные средства контроля целостности	Аппаратные средства хранения контрольных сумм и ключей	
	Целостность учетных записей в БДУЗ	Обеспечение целостности учетных записей пользователей в БД сервера аутентификации	Хэширование учетных записей	Хэширование учетных записей	Хэширование учетных записей, электронная подпись	
	Целостность АИ пользователя в БДУЗ и у владельца АИ	Обеспечение целостности АИ пользователя при генерации, хранении, предъявлении и передаче	Хранение АИ в БДУЗ только в хэшированном виде	Хранение АИ в БДУЗ только в хэшированном виде и/или открытые ключи пользователей	БДУЗ содержит только открытые ключи пользователей	

Рисунок 3.5 – Классификация СИА по целям и задачам информационной безопасности

Каждую задачу, изображённую на рисунке, можно рассмотреть более подробно. Остановимся на некоторых наиболее существенных задачах СИА.

Так, для обеспечения доступа всех зарегистрированных в ИС пользователей необходимо проектировать СИА с учётом её отказоустойчивости по отношению к запросам на аутентификацию. Производительность СИА, как правило, является избыточной, т.к. пиковые нагрузки по аутентификации пользователей обычно приходятся на получасовые периоды времени начала и окончания рабочего дня, в остальное время вычислительные мощности серверов аутентификации могут использоваться для других задач. Тем не менее, в техническом задании на проектирование СИА необходимо задавать максимальное время обработки запросов на аутентификацию в зависимости от интенсивности входящего потока заявок λ. Как показано в работах [15, 22, 23] основным условием гарантированной обработки заявок в заданное время является соотношение $\frac{\lambda}{\mu} < 1$, где μ - интенсивность обработки СИА заявок. Кроме выполнения такого условия для производительности, СИА должна обладать уровнем отказоустойчивости не ниже уровня отказоустойчивости самой ИС, к ресурсам которой предоставляется доступ пользователей.

В отличие от систем идентификации, СИА являются на порядок более сложными интеллектуальными системами. Напомним, что аутентификация (А) – процесс, состоящий из связанных подпроцессов подтверждения подлинности предъявленных идентификаторов с помощью аутентификатора и подтверждения принадлежности этого аутентификатора конкретному владельцу.

На основе развития классификации [132] с использованием результатов работы [164] выделим следующие типы СИА:

– **локальная**. Этот тип полностью совпадает с представленным в работе [41]. Службы аутентификации расположены на каждом устройстве, там же производится процесс А с помощью одного валидатора (механизма А, которому доверяет владелец ресурса) и принимается решение о доступе. Приме-

рами локальной А является персональный компьютер, ноутбук, сотовый телефон.

– **прямая**. Также совпадает с [41]. Владелец ресурса в процессе А доверяет одному валидатору, расположенному внутри защищенного периметра локальной вычислительной сети. Прямой А называется потому, что все пользователи, желающие получить доступ к ресурсу, напрямую проходят процесс А, предъявляя аутентификатор валидатору. Примером СИА прямого типа являются небольшие организации численностью до 20 рабочих мест.

– **доменная**. Отличается от прямой тем, что одному валидатору, расположенному внутри защищённого периметра локальной вычислительной сети, доверяют владельцы многих ресурсов, расположенные в ЛВС. В количественном отношении СИА доменного типа преобладают в сегментах малого и среднего бизнеса.

– **иерархическая**. Отличается от доменной наличием подчиненных доменов. В иерархической схеме СИА доступ пользователям может предоставлять подчинённый домен, однако в центре имеется БДУЗ пользователей и право управления доступом. Типичным примером таких СИА является организация, имеющая широкую филиальную сеть.

– **распределённая сетевая**. Отличается от доменной наличием множества доменов, связанных между собой трастовыми (доверенными) отношениями. В каждом домене независимо производится процесс А и принимается решение о доступе. Такие СИА характерны для крупных корпораций и холдингов.

– **мостовая**. Отличается от распределённой сетевой наличием ДТС. СИА мостового типа характерны для ведомственного взаимодействия с развитым электронным документооборотом.

– **браузерная**. Отличается от мостовой механизмом А, основанном на организации защищённого канала связи клиент-сервер на сессионном уровне. ДТС может находиться на этом же сервере. Одним из ярких примеров СИА браузерного типа является портал государственных услуг.

– **браузерная с трансляцией доверия**. Этот тип СИА пока мало известен в Российской Федерации в связи с неразвитостью публичных облачных сервисов. Предназначен для обеспечения доступа к облачным сервисам и ИС, в которых не имеется учётной записи данного пользователя. Отличается от браузерной наличием задачи транслирования доверия к аутентификации, которую пользователь успешно прошёл в первичной ИС, в другие ИС, к которым данному пользователю необходимо предоставить доступ. Эта задача, как правило, решается с применением федеративной системы трансляции доверия, представленной во многих публикациях, в частности, в работе [207].

Заметим, что классифицировать СИА можно также по следующим признакам:

– по методу аутентификации (предопределенному сочетанию факторов, способа организации обмена аутентификационной информацией и соответствующему данному сочетанию протокола аутентификации), пример такой классификации приведен в работе [**Ошибка! Закладка не определена.**];

– по основному механизму аутентификации (используемому виду аутентификационной информации): пароль, OTP, закрытый ключ; пример такой классификации рассмотрен в работе [204];

– по видам доступа (дискреционный, мандатный, ролевой) и используемым при этом методам аутентификации; такая классификация наиболее актуальна для корпоративных систем, пример приводится в работе [**Ошибка! Закладка не определена.**].

Классификация процессов аутентификации

По основным видам аутентификацию, как средство защиты от активных атак, представляется целесообразным разделить на аутентификацию сторон (партнёров) и аутентификацию источника данных или сообщений.

Во многих информационных системах процесс аутентификации ассоциируют со следующими задачами, которые можно классифицировать по их целевому назначению (Рисунок 3.6):

– **для предоставления санкционированного доступа**. Используется в

системах управления логическим доступом к компьютеру, корпоративной сети, информационным ресурсам и сервисам. Также используется как фильтр «свой-чужой»;

– **для установления доверительных отношений при удалённом доступе.** Такая аутентификация может быть взаимной (двухсторонней) и односторонней. Типичный пример – сетевые протоколы обмена с предварительным установлением доверительных отношений и выработки сеансовых ключей (с помощью симметричных криптографических протоколов) на основе многоходового защищённого обмена подписанной сторонами информации на базе PKI (протокол АН – первая часть протокола SSL -- может быть как односторонним, так и двухсторонним). Участниками (взаимодействующими сторонами) могут быть «субъект – объект» или «объект – объект» (например, IPSec, M2M);

– **для установления (идентификации) личности обладателя электронной подписи, проверки наличия полномочий на право подписи и фиксации неотказуемости выполнения процедуры подписи электронного документа владельцем электронной подписи.** Используется в системах электронного документооборота для придания юридической силы электронному документу, имеет ряд особенностей. В частности, как правило, применение электронной подписи встраивается в систему электронного документооборота (ЭДО) и вызывается средствами ЭДО. При этом аутентификация используется при доступе пользователя к системе ЭДО. Из целей (подтверждение личности обладателя подписи и неотказуемость) следует дополнительное требование - доказательство принадлежности ключа подписи конкретному владельцу. Эта задача решается как с помощью применения строгой аутентификации, так и с применением дополнительного фактора идентификации владельца ключевого носителя по его биометрическим характеристикам.

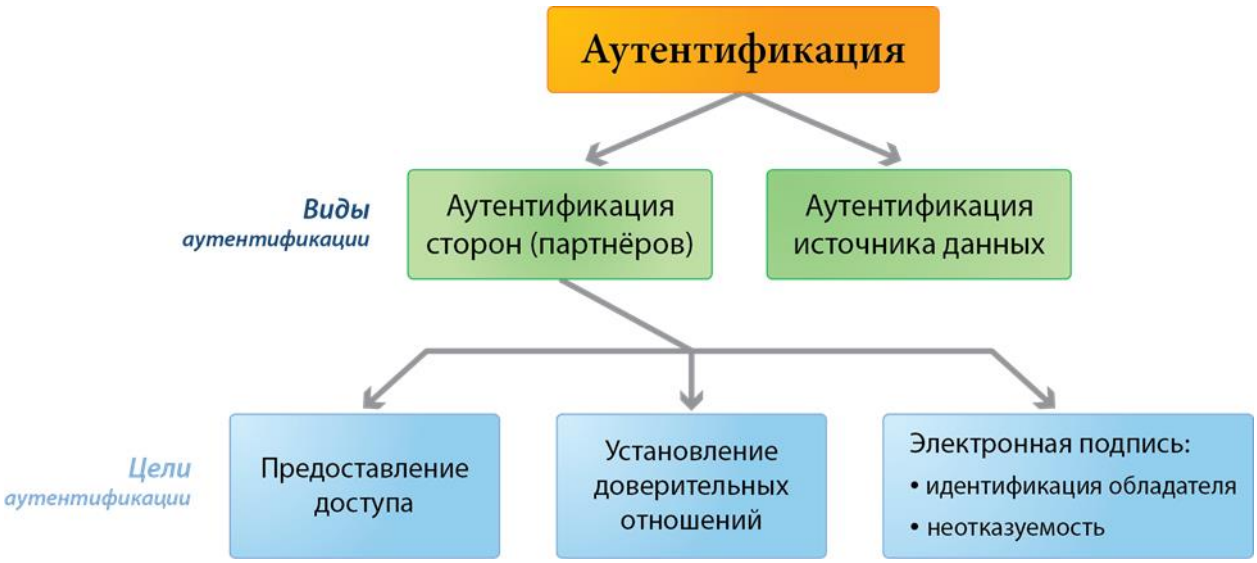

Рисунок 3.6 – Классификация процесса аутентификации по видам и целям

Установим приоритетность (последовательность и взаимосвязь) решения задач аутентификации при рассмотрении задачи применения ЭП.

Как правило, применение ЭП производится из прикладной программы, т.е. подразумевает использование подписи после авторизации пользователя. Значит, задача предоставления доступа более первична для сетевого взаимодействия.

Иное дело при УЭВ. Для решения задачи предоставления доступа при УЭВ сначала необходимо решить задачу установления доверительных отношений. После установления доверительных отношений решается задача предоставления доступа. Затем – задача применения ЭП уже из прикладного программного обеспечения, куда встроена функция применения подписи. Следовательно, очерёдность, а, следовательно, и приоритетность решения задач выглядит следующим образом:

Таблица 3.1 – Последовательность решения задач идентификации и аутентификации при применении ЭП

Сетевое взаимодействие	Удалённое сетевое взаимодействие
	установление доверительных отношений
предоставление доступа	предоставление доступа
применение ЭП	применение ЭП

В любом случае применение ЭП следует «за» предоставлением доступа.

Следовательно, решение задачи аутентификации с целью предоставления доступа следует решать первой.

Подсистемы аутентификации можно различать по типу информационной системы и по месту применения: в локальной вычислительной сети; в распределённой корпоративной вычислительной сети; для удалённого доступа легальных пользователей к корпоративной сети; для доступа к облачным сервисам из корпоративной сети; для доступа к облачным сервисам из «недоверенной» среды.

Кроме этого, системы идентификации и аутентификации можно классифицировать по категории информации, хранящейся и обрабатываемой на ресурсах, к которым надо организовать доступ: общедоступная (открытая) информация; информация ограниченного доступа (ДСП, персональные данные, «секретно» и т.д., ещё более 30 видов служебных тайн). Для того, чтобы соотнести виды разрешённой аутентификации применительно к организации доступа к ИС, содержащих разные категории информации, необходимо провести анализ на основе оценки рисков разглашения не только данных категорий информации, но и аутентификационной (персональной) информации пользователей. Например, критичными параметрами могут быть такие свойства, как целостность и конфиденциальность информации, используемой в процессе аутентификации пользователя.

По количеству используемых факторов аутентификацию можно классифицировать как: однофакторную (простую), например, с помощью пароля; двухфакторную, как правило, с помощью носителя, в котором хранится цифровой сертификат и соответствующий ему закрытый ключ, вторым фактором является знание PIN-кода, позволяющего воспользоваться закрытым ключом для заверения сообщений при обмене; многофакторную.

При организации системы строгой аутентификации необходимо использовать, как минимум, двухфакторную схему, поскольку закрытый ключ и сертификат доступа необходимо безопасно хранить в смарт-карте или ее аналоге.

Понятие «многофакторная» аутентификация, несмотря на частое употребление, часто воспринимается не совсем корректно. Единственный дополнительный фактор (под которым в подавляющем числе случаев понимается исключительно биометрия) может использоваться, строго говоря, только как дополнительное доказательство принадлежности данного устройства (и записанной в него аутентификационной информации) его владельцу.

Понятия: аутентификатор, протокол и фактор аутентификации

Метод аутентификации, включающий в себя реализуемое при аутентификации предопределенное сочетание факторов аутентификации, организации обмена и обработки аутентификационной информации (односторонний или взаимный), а также соответствующих данному сочетанию протоколов аутентификации, в западных национальных стандартах часто называют аутентификатором. Уточним понятия протокола и фактора аутентификации. Протокол должен позволять участникам процесса аутентификации осуществить аутентификацию. Протокол реализует алгоритм (правила), в рамках которого субъект доступа и объект доступа последовательно выполняют определенные действия и обмениваются сообщениями. В зависимости от применения тех или иных факторов аутентификации, видов аутентификационной информации, количества взаимодействующих сторон (кроме претендента и доверяющей стороны для некоторых протоколов в обмен сообщениями может включаться третья доверенная сторона в роли проверяющей стороны) и способов обмена различают группы протоколов, позволяющие организовать простую, усиленную и строгую аутентификацию [**Ошибка! Закладка не определена.**]. В простой и усиленной аутентификации применяют сетевые аутентификационные протоколы обмена с применением хэш-функций для обмена парольной информацией, в строгой аутентификации применяются только стойкие криптографические протоколы с использованием секретных ключей, полученных как правило с помощью алгоритмов ассиметричной криптографии [44,28].

Фактором аутентификации называется вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа при

аутентификации. В процессе аутентификации применяются следующие факторы:

фактор знания - субъект доступа должен знать определенную информацию, например, пароль, графический пароль, одноразовый пароль или PIN-код;

фактор владения - субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию, например, устройство аутентификации или механизм, приспособление, вещь, которые содержат аутентификационную информацию;

биометрический фактор - субъекту доступа должен быть свойственен определенный признак, например, биометрические данные физического лица или шаблон поведения.

В 2019 году представители американской делегации на ноябрьском заседании 27 подкомитета ISO в г. Париж предложили в качестве одного из основных факторов аутентификации считать географические координаты чипа, содержащего закрытый ключ, применяющийся в качестве аутентифицирующей информации наряду с традиционными факторами знания и владения. Однако все остальные эксперты, собравшиеся на данном заседании, не поддержали этой инициативы в виду неготовности повсеместной технологии определения координат. Количество одновременно применяемых факторов аутентификации и протоколы аутентификации вкупе с организацией обмена аутентификационной информацией (односторонняя или взаимная) существенно сказываются на достоверность результатов аутентификации.

Предлагаемая в данной работе трёхуровневая модель достоверности аутентификации согласовывается с текущим состоянием нормативной базы РФ по оценке состояния защищённости ИС, обрабатывающих информацию ограниченного доступа, не содержащую государственную тайну [208, 209], а также законодательства по защите персональных данных [69, 183], и введения трех видов электронной подписи [72] Этот подход не противоречит [68], где

сказано, что участниками электронного взаимодействия и обладателями информации могут быть три уровня пользователей: граждане (физические лица), организации (юридические лица), государство (государственные органы и органы местного самоуправления).

Деление на такие группы приемлемо с точки зрения как грубой оценки рисков (низкий, средний, высокий уровень), так и оценки надёжности и последствий от ошибок ИА и атак (низкий, средний, высокий уровень). В сложившейся за период с 2002 г. практике применения аутентификаторов (токенов) массово используется тоже всего три типа: многоразовый пароль, технология одноразовых паролей OTP (One Time Password), а также технология аутентификации на основе PKI и цифровых сертификатов, в частности строгой двухфакторной аутентификации посредством смарт-карт, содержащих неизвлекаемый ключ электронной подписи, применение которого невозможно без ввода PIN-кода (когда по сути используется технология электронной подписи). Таким образом, основываясь на приведенных рассуждениях и исследованиях [163,142], можно предложить три типа аутентификации (простая, усиленная, строгая).

При организации всех упомянутых видов доступа возможна классификация по используемым технологиям: пара «имя пользователя – пароль», пара «имя пользователя – одноразовый пароль», а также пара «заданные поля цифрового сертификата доступа – закрытый ключ» (Таблица 3.2).

Таблица 3.2 – Аутентификационная информация в различных технологиях

Идентификационная информация	Аутентификационная информация	Вид аутентификации
Имя пользователя	Пароль	Простая
Имя пользователя /заданные поля сертификата X.509, сформированного удостоверяющим центром с неопределенным уровнем доверия для доступа пользователя	Одноразовый пароль (технология OTP) / закрытый ключ (ключ подписи)	Усиленная

Заданные поля сертификата X.509, сформированного доверенным (аккредитованным) удостоверяющим центром для доступа пользователя	Ключ подписи или закрытый ключ доступа	Строгая

Преимущество применения закрытого ключа как аутентифицирующей информации очевидно - для такой схемы аутентификации не требуется знание значения ключа подписи на серверной стороне, а достаточно лишь владеть открытым ключом и уведомлением о способе подтверждения подлинности. Это существенно повышает уровень защищённости процесса аутентификации, однако организация доступа с применением цифровых сертификатов доступа и закрытого ключа электронной подписи может иметь свои подуровни доверия, зависящие от способов формирования и хранения закрытого ключа. Так, закрытый ключ (ключевая пара) может быть сформирован по технологии усиленной неквалифицированной подписи или с помощью технологии усиленной квалифицированной подписи. Также надо учитывать способы формирования и хранения ключевой пары. Дело в том, что закрытый ключ может быть интегрирован в ключевой носитель (смарт-карту, USB-ключ и др.) после того, как ключевая пара сгенерирована программным крипто-сервис-провайдером в оперативной памяти компьютера. При другом, более безопасном способе, ключевой материал формируется в защищённой памяти чипа смарт-карты или USB-ключа. Однако чипы могут быть разные, например, есть чипы, специально спроектированные, произведенные и сертифицированные по различным требованиям безопасности. Самым безопасным вариантом является применение чипов класса Secure by Design (безопасные по условиям проектирования), сертифицированных по различным уровням требований CAST и Common Criteria (например, самым распространённым требованием на западе является наличие у устройства генерации ключевого материала сертификата EAL4+).

По участию количества сторон в обмене строгая аутентификация может быть (Рисунок 3.7):

– односторонняя. Типичным примером которой является однонаправленный протокол SSL, в котором требуется проверка сертификата только на стороне клиента;

– двухсторонняя. Например, вариант SSL, когда проверяются сертификаты серверной и клиентских сторон;

– трёхсторонняя. К двум сторонам при аутентификации добавляется доверенная третья сторона (например, широко применяемый в корпоративных системах протокол Kerberos).

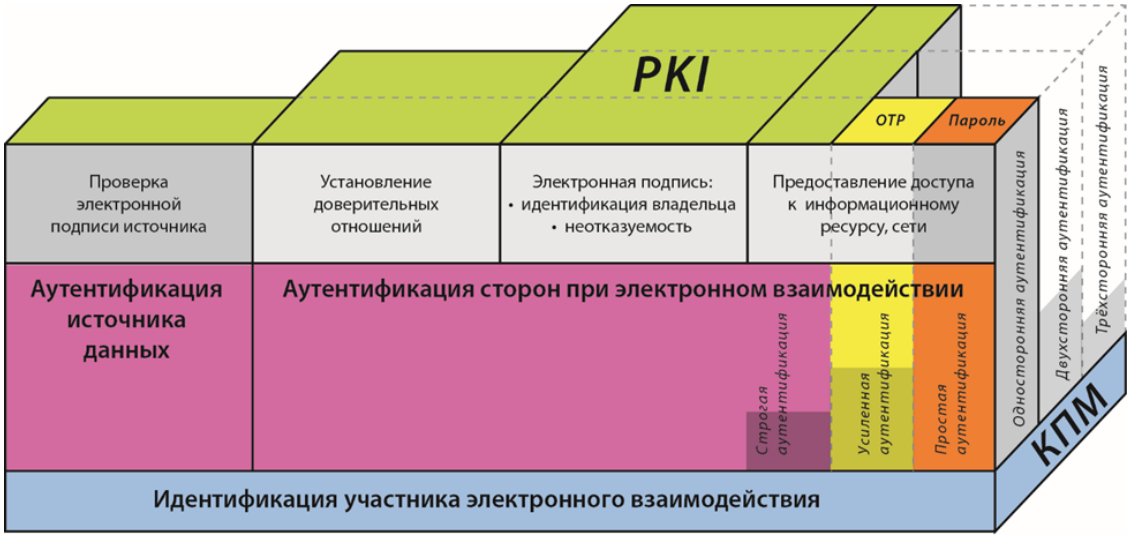

Рисунок 3.7 – Классификация идентификации и аутентификации в разрезе «цели и задачи – уровни участия сторон в процессе аутентификации»

На рисунке показано, что многоразовые пароли, одноразовые пароли и аутентификация источника данных производятся посредством односторонней аутентификации. При этом отличие двух первых от процесса аутентификации источника данных состоит в том, что это процесс производится на основе инфраструктуры открытых ключей. Наиболее полно возможности ИОК могут использоваться при применении электронной подписи и установлении доверительных отношений (двухсторонняя аутентификация сторон электронного взаимодействия). Для идентификации пользователей при использовании инфраструктуры открытых ключей следует применять идентификаторы класса

«Корпоративный персональный многоразовый» согласно классификации.

Классификация средств идентификации и аутентификации

По уровням доверия средства аутентификации могут быть разделены на следующие градации, расположенные по мере возрастания уровня защищённости аутентификационной и идентификационной информации.

Низкий уровень – простая аутентификация:

– парольная аутентификация. Пароль не передаётся по сети в открытом виде. Сравниваются хеши паролей.

Средний уровень – усиленная аутентификация:

– одноразовый пароль;

– многоразовый пароль (пароль учётной записи пользователя) совместно с одноразовым паролем (OTP);

– неквалифицированный сертификат доступа.

Высокий уровень – строгая аутентификация:

– квалифицированный сертификат доступа, секрет (ключ подписи) хранится в реестре;

– квалифицированный сертификат доступа, секрет (ключ подписи) хранится на незащищённом носителе (дискета, флешь-память);

– квалифицированный сертификат доступа, секрет (ключ подписи) хранится в защищённом хранилище (после генерации установленным на средствах вычислительной техники криптопровайдером импортируется из оперативной памяти в смарт-карту, USB-ключ), доступ к секрету защищён PIN-кодом;

– квалифицированный сертификат доступа, секрет (ключ подписи) генерируется средствами смарт-карты (USB-ключа) и никогда не покидает защищённой памяти чипа, доступ к секрету защищён PIN-кодом;

– квалифицированный сертификат доступа, секрет (ключ подписи) генерируется средствами смарт-карты (USB-ключа) и никогда не покидает защищённой памяти чипа; доступ к секрету защищён PIN-кодом, принадлеж-

ность ключевого носителя конкретному пользователю дополнительно доказывается биометрическими способами.

Классификация средств идентификации и аутентификации

На рис. 3.8 представлена классификация средств ИА по критерию применяемых в процессах идентификации и аутентификации технологий, разработанная автором в 2006 году [130].

Рисунок 3.8 – Классификация средств идентификации и аутентификации с точки зрения применяемых технологий

Как видно из рисунка, многие используемые сегодня устройства не могут обеспечить высокий уровень защищённости аутентификационной информации в силу ограничений технологий, на которых они основаны. Например, если аутентифицирующая информация записана в электронный ключ Touch Memory, то она может быть скопирована злоумышленником и перенесена в такое же устройство и использована для доступа вместо владельца. Сами же ключи Touch Memory предназначены только для идентификации их обладателя. Заметим, что биометрические технологии, даже самые сложные, явля-

ются технологиями идентификации, например, одна из самых передовых технологий Match on Card предназначена строго для подтверждения факта обладания смарт-картой. Это дополнительный идентификационный фактор, который позволяет повысить общий уровень защищённости в корпоративной сети и повысить уровень персональной ответственности. Прежде всего, это защита от такого распространённого явления, как передача устройства, содержащего криптографический ключ, товарищу по работе (например, с целью сокрытия факта отсутствия на рабочем месте).

Классификация процессов аутентификации по уровням достоверности результатов

Классификацию аутентификации по уровням достоверности результатов лучше всего вести на основе простой шкалы по аналогии с установленными №63-ФЗ видами электронной подписи: простая, усиленная и строгая. По аналогии с результатами второй главы можно говорить о достоверности аутентификации (наряду с надежностью и безопасностью) как об одной из составляющих доверия к результатам аутентификации. Принцип классификации аутентификации по уровням доверия также должен базироваться на анализе рисков от атак на взаимодействующие стороны и сам процесс взаимодействия. Данная классификация должна учитывать применяемые технологии аутентификации, а также обеспечение целостности и конфиденциальности аутентификационной информации. Приведём краткое описание трёх уровней доверия аутентификации, предложенные в работе [167].

Простая аутентификация основана на традиционных многоразовых паролях и применяется с обязательным согласованием средств использования пароля и способов его обработки (например, хеширование, шифрование при передаче и хранении). Системы простой аутентификации на основе многоразовых паролей обычно обладают низкой стойкостью к атакам, поскольку, как правило, выбор аутентификационной информации основывается на относительно небольшом выборе слов. Существуют системы типизации общеупотребитель-

ных подходов к образованию паролей, которые легко запоминать (дата рождения, имена близких, название местности и т.д.). Кроме того, пароли можно перехватить, разгадать, подсмотреть или украсть.

Усиленная аутентификация базируется на более стойкой к атакам технологии OTP (One-Time-Password, одноразовый пароль), при которой для каждого запроса на доступ используется новый пароль, действительный только для одного входа в систему. В зависимости от конкретной реализации применение OTP может существенно повысить безопасность аутентификации. Одними из самых распространённых схем с OTP являются системы аутентификации, в которых для доступа пользователя одноразовый пароль одновременно используется вместе с многоразовым паролем. Технологии генерации OTP могут быть различными, наиболее часто употребляются схемы выработки одноразовых паролей «по событию» и «по времени». Стойкость OTP определяется вектором инициализации аутентификатора [42]. К усиленной аутентификации также может быть отнесён механизм, основанный на технологии электронной подписи с использованием цифрового сертификата доступа, выпущенного УЦ с неопределенным уровнем доверия.

Понятие «строгая» аутентификация в силу частого, но не всегда правильного употребления, нуждается в более полном рассмотрении. Основой идеей строгой аутентификации является то, что проверяемая сторона в процессе защищённого обмена последовательно подписываемой сторонами информации доказывает проверяющей стороне обладание предварительно распределённым безопасным способом секретом (как правило, речь идёт о закрытом ключе). Строгая аутентификация согласно [4] должна быть обязательно взаимной, производится с применением инфраструктуры открытых ключей и соответствующих криптографических протоколов.

Рассмотрим выполнение задач обеспечения доступности, целостности и конфиденциальности данных пользователя для предложенных уровней доверия аутентификации (Таблица 3.3).

Таблица 3.3 – Связь типов аутентификации с безопасностью пользовательских данных на стороне клиента

Типы аутентификации	доступность	целостность	конфиденциальность
Простая (пароль)	+	-	-
Усиленная (OTP)	+	-	-
Усиленная (X.509, выдан УЦ с неопределенным уровнем доверия)	+	+	-
Строгая (X.509, выдан доверенным УЦ)	+	+	+

3.3 Разработка и совершенствование существующих моделей и методов оценки рисков применительно к процессу аутентификации

В отличие от традиционных методов риск - менеджмента, осуществляющих привязку рисков к стоимости конкретного актива, разработаем методику и модели анализа рисков в «безразмерном» виде с учётом особенностей идентификации и аутентификации, применение которой к конкретному активу не представит для специалиста трудностей.

Применим многоуровневую модель оценки рисков ИА при ЭУВ:

MRA (первый уровень) - предварительный анализ на основе качественных оценок уровня рисков СИА для владельцев ГИС на основе анализа общих последствий для конкретной организации или ведомства; на этом же уровне можно проводить качественный и, при необходимости, количественный анализ на основе рассмотрения опасных событий (например, дерево опасных событий) и их последствий для СИА как элемента ИС;

MRB (второй уровень) - качественный и количественный анализ рисков СИА на основе детализированной модели дерева отказов и исследования последствий на уровне процессов ИА;

MRC (третий уровень) – количественный анализ рисков на уровне процедур, происходящих в компонентах СИА (серверный компонент, канал, рабочая станция и т.д.);

MRD (четвертый уровень) – уточняющий количественный анализ рисков на уровне элементов компонент СИА (например, в устройствах генерации аутентификационной информации). Соотношение уровней анализа рисков и уровней детализации СИА, как иллюстрация принципов построения многоуровневой модели для анализа рисков, приведено ниже (Рис. 3.9).

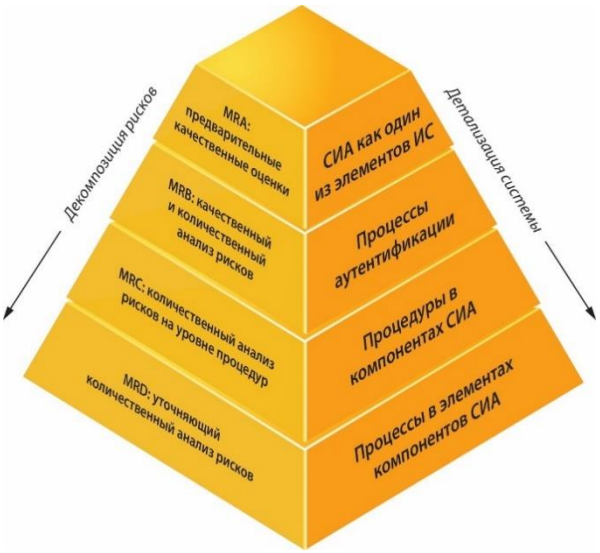

Рисунок 3.9 – Соотношение уровней анализа рисков с уровнями детализации

Ключевым элементом оценки рисков согласно [106, 119, 124] является итерационный процесс их анализа. С учётом результатов анализа, проведенного в первой и второй главах, существующие алгоритмы оценки рисков доработаны применительно к задаче идентификации и аутентификации.

Алгоритм анализа рисков согласно [105,124] для многоуровневой модели включает:

- идентификацию рисков;
- анализ рисков;
- декомпозицию рисков;
- снижение (или принятие) рисков.

Предложенный алгоритм применительно к анализу рисков идентификации и аутентификации представлен на рис. 3.10.

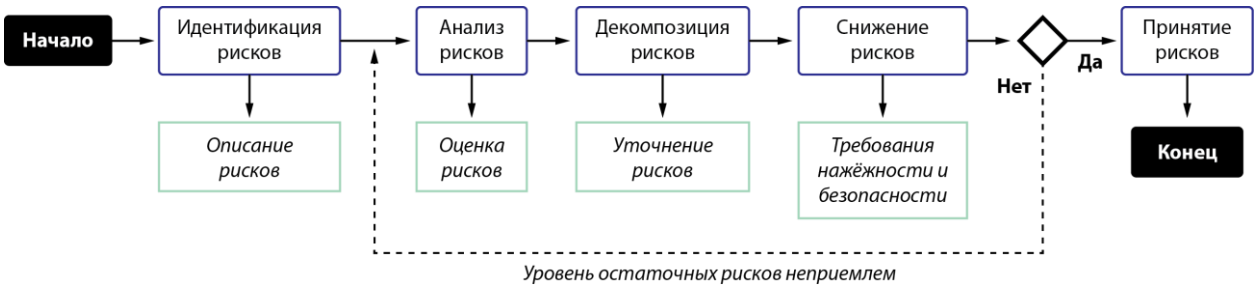

Рисунок 3.10 – Алгоритм анализа рисков идентификации и аутентификации

При необходимости уточнения значений рисков ИА для анализа на более низких уровнях модели могут быть детализированы. Например, уточнение значений риска такой критической процедуры как регистрация пользователей портала государственных и муниципальных услуг будет рассмотрена ниже.

Уровень детализации и набор инструментов анализа рисков предлагается выбирать, исходя из индивидуальных особенностей системы, её предназначения и определенного уровня рисков.

Общая схема оценки рисков ИА, представленная на рис. 3.11, включает как процессы, рассмотренные в первых двух главах (анализ процесса идентификации, анализ процессов и систем аутентификации, классификация, анализ нормативной базы) так и собственно процессы аутентификации, которые будут исследованные в настоящей главе.

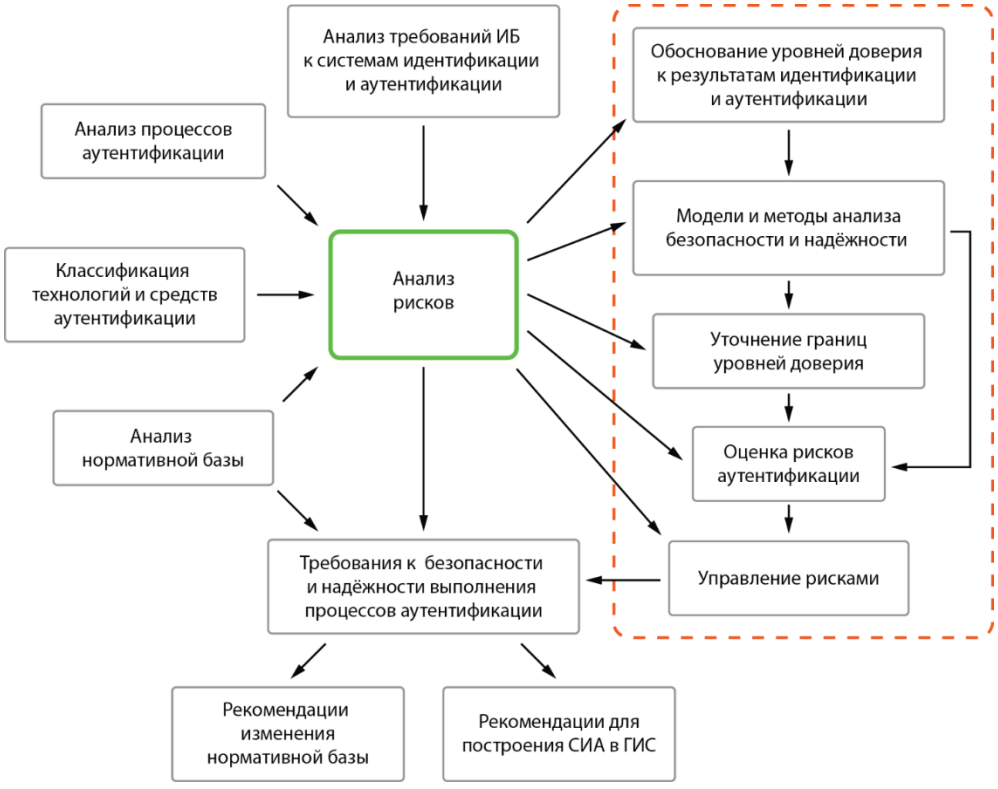

Рисунок 3.11. Общая схема исследования рисков аутентификации

Суть предложенного метода состоит в многоуровневом анализе рисков процессов аутентификации. Его отличительная особенность состоит в том, что метод позволяет детализировать влияние на величину остаточных рисков компонентов системы идентификации и аутентификации по принципу от «общего к частному» (Рис. 3.12).

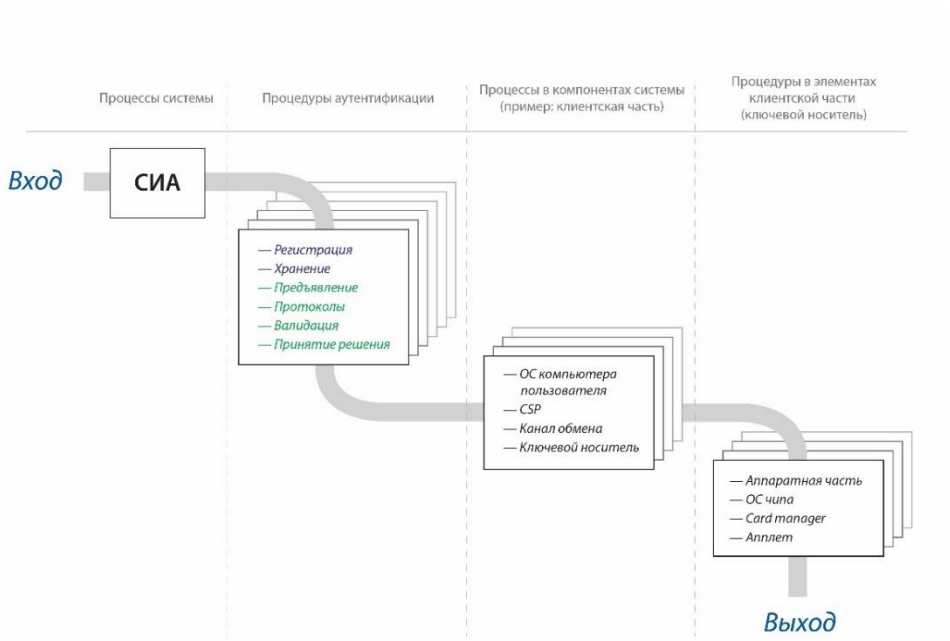

Рисунок 3.12 – Принцип построения многоуровневой модели

Описание области применения, идентификацию рисков, анализ последствий, определение критериев рисков и их обработку будем выполнять в целом соответствии с действующими стандартами [105, 122-124].

Методика оценки высокоуровневых рисков аутентификации

Сначала введём основные определения, рассмотрим актуальные угрозы, уязвимости, атаки и методы их нейтрализации, затем определим опасные события и вероятности их наступления.

В силу сложности оценки рисков для систем идентификации и аутентификации оценивание рисков предлагается проводить в несколько этапов, от-

личающихся уровнем детализации (многоуровневая оценка рисков). В стандартах, описывающих методики анализа рисков, показано, что процесс их оценки всегда является итерационным.

Покажем, как можно выполнить данную оценку на примере рассмотренных во второй главе трёх уровней идентификации. Как прототип для оценки возьмём руководство [210], разработанное для переходного периода от бумажного документооборота к безбумажному с акцентом на электронные транзакции.

В виде исходных данных, кроме трёхуровневой модели аутентификации, возьмём качественную трёхуровневую модель рисков (Н - низкий, С-средний, В - высокий), предложенную в стандарте [211] и поддержанную в российских стандартах, например, в серии стандартов [105-110].

Для проведения высокоуровневой оценки (в терминах стандарта [211]) предлагается следующий набор категорий: репутационные риски, финансовые риски, риски ущерба для программ и проектов организации, риски НСД к чувствительной конфиденциальной информации и безопасность персональных данных сотрудников и контрагентов.

Результаты заносятся в таблицу. Пример заполнения таблицы для различных уровней используемых (или планируемых к применению) технологий аутентификации приводится ниже (таблица 3.4)

Таблица 3.4 – Максимальные оценки рисков выбранных категорий при условии использования средств аутентификации, принадлежащих определенному технологическому уровню

	Технологические уровни аутентификации		
Потенциальный ущерб	простая	усиленная	строгая
репутации	В	С	Н
финансам	С	С	Н
проектам и программам	В	С	Н
НСД к КИ	В	С	С

ПДн данные сотрудников и контрагентов	B	C	C

Заполнение таких таблиц, как правило, не составляет трудностей для экспертов по ИБ. В то же время, такие оценки полезны для руководства и могут служить отправной точкой для планирования следующих итераций по оценке рисков. Подобные таблицы имеют и самостоятельное значение. В частности, на основании такого ранжирования рисков можно сделать следующие шаги.

Первым шагом применительно к выбранным категориям может явиться процесс проведения детализированной оценки рисков для государственных информационных систем. В частности, одной из целей исследования может являться определение диапазона изменений ущерба по категориям в зависимости от ошибок идентификации и аутентификации для выявленных высоких уровней потенциального ущерба.

На втором шаге можно определить связь уровней идентифицированных рисков с технологическими уровнями аутентификации. При этом следует пользоваться следующим правилом. Если среди занятых в транзакции несколько категорий потенциального ущерба соответствуют уровню простой аутентификации, а хотя бы одна – усиленной, то для данного типа транзакций следует использовать усиленную аутентификацию.

На третьем шаге следует выбрать технологии идентификации и аутентификации и закрепить их в соответствующих технических регламентах.

На четвёртом шаге после выбора и внедрения технологий идентификации и аутентификации следует проверить, может ли реально достигаться требуемый уровень достоверности аутентификации как составной части обеспечения безопасности.

Наконец, на пятом шаге необходима организация проверок (аудита) корректности выполнения идентификации и аутентификации для поддержания заданного уровня рисков на всех этапах жизненного цикла аутентификационной информации пользователя (инициализация, получение, верификация, транзакции, записи, смена, отзыв, аудит, списание, архивирование).

Следующая итерация (более детализированный уровень) оценки рисков связана с более детальным изучением как системы идентификации и аутентификации и участников процессов, так и самых актуальных уязвимостей, угроз и вероятных опасных событий.

Анализ рисков системы идентификации и аутентификации как отдельной системы

Для уровней MRB и MRC необходимо провести предварительный анализ угроз и уязвимостей СИА.

Пространство угроз безопасности выполнения процессов идентификации и аутентификации для различных систем идентификации и аутентификации согласно требованиям стандарта [211] является N-мерным. Рассмотрим угрозы, наиболее часто встречающиеся в разных системах идентификации и аутентификации, и покажем, что модель пространства угроз аутентификации является не только многомерной, но и многоуровневой. Также покажем, что противодействие угрозам требует дифференциации требований безопасности, то есть введения уровней достоверности аутентификации.

Основываясь на методическом документе [183], рассмотрим угрозы нарушения безопасности процессов аутентификации по следующей схеме:

- оценим угрозы всей системе идентификации и аутентификации как компоненту информационной системы,
- рассмотрим угрозы типовому процессу аутентификации, состоящему из ряда последовательно выполняемых процедур.

При этом покажем, что наиболее актуальные угрозы можно рассматривать и на более детальном уровне – детализировать угрозы на различных уровнях абстракции процесса аутентификации, например, на уровне процесса аутентификации в целом, на уровне системы идентификации и аутентификации информационной системы, на уровне устройств, на которых хранятся аутентификационные данные пользователей.

Первый уровень детализации – угрозы аутентификации в системе управления

доступом информационной системы. Согласно [182] в процессе информационного взаимодействия следует обеспечить следующие характеристики безопасности: конфиденциальность, доступность, целостность. Для системы идентификации и аутентификации можно выделить три основных типа источника угроз: антропогенные, техногенные и стихийные источники.

К **антропогенным** источникам относятся субъекты, имеющие доступ к системе идентификации и аутентификации, и действия которых могут привести к нарушению безопасности информации. По отношению к системе идентификации и аутентификации антропогенные источники могут быть внутренними и внешними. Внешними источниками угроз могут являться лица, осуществляющие доступ под видом легального пользователя или с использованием алгоритмических или программных закладок. Внутренними источниками угроз могут являться легальные пользователи с различными правами доступа. К таким источникам может относиться технический персонал, обеспечивающий эксплуатацию системы идентификации и аутентификации и информационной системы в целом. Угрозы от внутренних источников разделяются на ошибки, нарушения требований регламентов и инструкций, а также преднамеренные действия (сговор) с внешними злоумышленниками.

Угрозы от антропогенных источников могут быть случайными и преднамеренными. Источники случайных угроз используют уязвимости в архитектуре системы идентификации и аутентификации, системном и прикладном программном обеспечении, сбои аппаратной и программной частей системы, ее отказы и повреждения. Случайные угрозы, как правило, реализуются по невнимательности, халатности, из любопытства, но без злого умысла.

В отличие от них источники преднамеренных угроз (злоумышленники) отличаются целенаправленным действием по дезорганизации работы системы идентификации и аутентификации: выявлению и использованию уязвимостей программного обеспечения и ее архитектурных компонентов, использованию специально размещённых закладок или вредоносных программных средств.

Наибольшую опасность, как правило, представляют преднамеренные угрозы,

исходящие от внешних и внутренних антропогенных источников.

Техногенные источники угроз напрямую зависят от используемой техники и также разделяются на внешние и внутренние. К внешним источникам можно отнести такие инфраструктурные элементы системы идентификации и аутентификации, как средства связи, инженерные коммуникации и т.д. К внутренним источникам можно отнести некачественные средства вычислительной техники, вспомогательные средства (телефонии, сигнализации, охраны) и т.д. Угрозами техногенного характера являются аварии (отключение электропитания, водоснабжения и канализации), сбои и неисправности (выход из строя серверов, коммуникационного и сетевого оборудования, АРМов администраторов и пр.), помехи, наводки и т.д.

Стихийные источники угроз, как правило, внешние: наводнения, землетрясения, пожары, ураганы, магнитные бури и т.п. Возникновение этих источников трудно спрогнозировать, а противодействие им затруднительно. Обычно учитывают, что в целях ликвидации последствий стихийных бедствий на территорию ИС и СИА могут проникнуть спасатели, среди которых могут оказаться нарушители.

Стандарт [119] рекомендует ранжирование уровня угроз в зависимости от результата её воздействия по простой шкале: высокий, средний и низкий. Для каждого сочетания ИС и СИА необходимо проводить такой анализ угроз на качественном уровне. Пример анализа приводится в таблице 3.5.

Таблица 3.5 – Пример анализа угроз на качественном уровне

Источник угроз	Вид угрозы	Уровень угрозы
внешний нарушитель	без злого умысла	низкий
внешний нарушитель	злонамеренная	высокий
внутренний нарушитель	ошибки	средний
внутренний нарушитель	Злонамеренная - инсайдер	высокий

Источник угроз	Вид угрозы	Уровень угрозы
техногенные угрозы	аварии	низкий
техногенные угрозы	отказы	средний
техногенные угрозы	сбои	средний
стихийные угрозы	пожары	низкий
стихийные угрозы	наводнения	низкий
стихийные угрозы	землетрясения	низкий
стихийные угрозы	др. форс-мажорные	низкий

Таким образом, из рассмотренных источников наиболее опасными угрозами для системы идентификации и аутентификации являются внешние и внутренние антропогенные источники, затем следуют техногенные угрозы – отказы и сбои аппаратных и программных компонентов системы.

Рассмотрим данные угрозы более подробно на следующем уровне детализации.

Второй уровень детализации – угрозы аутентификации, отражающие ее последовательное выполнение. Согласно [86] процессы идентификации и аутентификации могут быть представлены в виде выполнения ряда последовательных процедур. Воспользуемся результатами работы [**Ошибка! Закладка не определена.**], в которой имеется полное описание процессов аутентификации при удалённом электронном взаимодействии. Примем, что процесс аутентификации состоит из следующей последовательности выполняемых действий:

регистрация нового пользователя информационной системы, включая назначение ему идентификатора доступа;

хранение идентификационной и аутентификационной информации;

предъявление идентификатора доступа и аутентификационной информации при доступе пользователя.

подтверждение подлинности пользователя с применением протоколов аутентификации;

подтверждение принадлежности аутентификационной информации данному пользователю (валидация аутентификационной информации);

принятие решения о результате аутентификации пользователя;

авторизация пользователя в информационной системе при положительном результате аутентификации.

Угрозы регистрации подробно рассмотрены в главе 2. Угрозы безопасности хранения идентификационной и аутентификационной информации также могут быть разделены на уровни.

Как правило, угрозы рассматриваются в сочетании с уязвимостями, которые могут предоставлять возможности реализации угроз. При рассмотрении хранения такой подход наиболее четко иллюстрирует обоснование введения уровней безопасности.

Согласно статье 10 Федерального закона №63-ФЗ [72] участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей ЭП. На примере применения усиленной квалифицированной ЭП, зачастую используемой не только для подписи, но и как механизм аутентификации при доступе к информационной системе, покажем, что в зависимости от технологий формирования ключевого материала, СКП и передачи их во владение пользователю угрозы компрометации ключей ЭП можно разделить на уровни безопасности их хранения.

Как известно, для формирования ключевого материала (открытого и закрытого ключей), согласно действующему законодательству, можно воспользоваться внешним CSP (крипто сервис провайдером) или внутренним СКЗИ (средство криптографической защиты информации), встроенным в защищённый чип смарт-карты. Понятие «внешний» в данном контексте означает использование СКЗИ в виде сертифицированного по требованиям безопасности

ФСБ России CSP в оперативной памяти компьютера. Полученный любым из указанных способов открытый ключ посылается вместе с запросом в УЦ, который формирует на основе полученного открытого ключа пользователя СКПП, заверяя правильность его заполнения и проверку принадлежности владельцу своей ЭП. Уязвимость закрытого ключа к возможности его кражи или копирования определяет список угроз компрометации связанного с ним СКПП или сертификата доступа. Согласно рекомендациям [107], выделим три уровня угроз (низкий, средний, высокий) и соответствующих им уровней уязвимости в зависимости от способа формирования закрытого ключа. Рассмотрим следующие способы формирования ключевого материала:

– для выработки открытого и закрытого ключей применяется внешний CSP с последующим импортом закрытого ключа в память оптического носителя или флэш-память;

– lля выработки открытого и закрытого ключей применяется внешний CSP с последующим импортом закрытого ключа в память устройства (ключевого носителя), в котором доступ к закрытому ключу защищён PIN-кодом;

– формирование ключевого материала производится с помощью программного обеспечения внутри памяти устройства (флэш-память, USB-ключ), защищённой PIN-кодом;

– формирование ключевого материала производится аппаратно внутри специально спроектированного чипа устройства SSCD (Secure Signature Creation Device), устройства безопасной генерации подписи.

Результаты такого анализа представлены ниже (таблица 3.6).

Таблица 3.6 – Уровни угроз компрометации закрытого ключа

Способ формирования ключевого материала	Носитель ключевой информации	Уровень уязвимости	Уязвимость	Уровень угрозы
Внешний CSP с последующим импортированием закрытого ключа на дискету	Дискета	Высокий	Дискету легко скопировать	Высокий

Внешний CSP с последующим импортированием закрытого ключа на носитель с памятью, защищенной PIN-кодом	Смарт-карта, USB-ключ	Средний	Для копирования надо знать или подобрать PIN-код	Средний
Формирование ключевого материала производится программно внутри памяти устройства, защищённого PIN-кодом	USB-ключ на основе бытового микроконтроллера	Средний	Закрытый ключ защищён только PIN –кодом и нуждается в дополнительных средствах защиты	Низкий
Формирование ключевого материала производится аппаратно внутри специально спроектированного чипа устройства SSCD	SSCD (Secure Signature Creation Device)	Низкий	Неизвлекаемость закрытого ключа гарантирована международными и российскими сертификатами	Низкий

Рассмотрим основные угрозы и уязвимости, возникающие при предъявлении пользователем идентификационной и аутентификационной информации. Рассмотрение проведем в упрощённой клиент-серверной схеме аутентификации применительно к трём наиболее часто применяемым видам аутентификаторов: пароль, одноразовый пароль, закрытый ключ.

При взаимодействии клиент предъявляет ИД и АИ серверу аутентификации, который проверяет подлинность предъявленной ИД с помощью протоколов аутентификации и использования АИ претендента (таблица 3.7)

Таблица 3.7 - Уровни угроз и уязвимостей в процедуре предъявления аутентификатора

Вид аутентификатора	Уровень уязвимости	Уязвимость предъявления	Уровень угрозы
Пароль	Высокий	Предъявляется в открытом виде	Высокий
Одноразовый пароль	Высокий	Предъявляется и передается по сети в открытом виде	Средний
Закрытый ключ используется в	Средний	Закрытый ключ нуждается	Низкий

Вид аутентификатора	Уровень уязвимости	Уязвимость предъявления	Уровень угрозы
оперативной памяти средств вычислительной техники		в средствах защиты, например, средствами ОС	
Процедура подписи производится внутри специально спроектированного чипа устройства SSCD	Низкий	Неизвлекаемость закрытого ключа гарантирована	Низкий

Некоторые результаты, представленные в таблице, нуждаются в пояснениях. Например, при применении одноразового пароля в виде аутентификатора, его уязвимость велика, однако воспользоваться этим практически невозможно, так как при правильной организации механизма аутентификации, данный OTP-пароль действует исключительно в рамках текущей сессии. Поэтому уровень угроз может быть оценён как средний.

Также требуют объяснения и содержание предпоследней строки таблицы. При соблюдении условий безопасного применения данного типа аутентификатора вероятность успешных атак на закрытый ключ может быть сведена практически к нулю за счёт согласованных организационных и технических мероприятий. Технические меры защиты в данном случае состоят из согласованной работы по противодействию атакам доверенной операционной системы и CSP.

Угрозы протоколам аутентификации, используемым при подтверждении подлинности пользователя, условно можно разделить на следующие группы:

угрозы, которые направлены на сам протокол аутентификации,

угрозы, которые направлены на раскрытие значений аутентификаторов или компрометацию конфиденциальной информации.

Атаки, направленные на раскрытие значения аутентификатора, в общем случае более опасны, чем атаки, просто компрометирующие АИ, поскольку с помощью аутентификатора злоумышленник может действовать от имени легального пользователя.

Центры регистрации, УЦ, проверяющие и доверяющие стороны обычно

считаются «доверенными», а заявители и их системы — «недоверенными» (доверенными могут быть признаны лишь их заявки на подтверждение личности). Доверенность ЦР, CSP и проверяющих сторон не означает их неуязвимости. Поэтому следует избегать по возможности использования протоколов, в которых задействуются секреты (АИ) с большим сроком действия.

В число угроз протоколам аутентификации входят:

угроза «подслушивание»;

угроза «имитация», в том числе:

- угроза «имитация заявителя»;
- угроза «имитация проверяющей стороны»;
- угроза «имитация доверяющей стороны»;

угроза перехвата сеанса аутентифицированного пользователя, в том числе:

- обращение от имени пользователя к доверяющей стороне с целью получения конфиденциальной информации либо ввода недействительной информации;
- обращение от имени доверяющей стороны к проверяющей стороне с целью получения конфиденциальной информации либо ввода недействительной информации.

Предполагается, что злоумышленники могут не только подслушивать выполнение протокола аутентификации, но и встраиваться в него. Но протокол может быть способен к распознанию перехваченных сообщений либо к тому, чтобы противостоять возможности анализа, в результате которого злоумышленник мог бы получить информацию, которая позволила бы ему представляться заявителем. Из-за большой распространённости парольных протоколов и из-за способов их реализации пользователи таких протоколов уязвимы по отношению к имитации проверяющей стороны. Большое распространение беспроводных сетей создаёт условия для перехвата сеансов аутентифицированных пользователей.

Перечислим основные механизмы атак на протоколы аутентификации:

- пассивное прослушивание;
- активные атаки: имитация заявителя (угадывание пароля, воспроизведение);

внесение изменений в канал аутентификации, в том числе перехват сеанса аутентифицированного пользователя; имитация проверяющей стороны; атака типа «человек посередине».

Перечислим основные методы противодействия некоторым угрозам безопасного выполнения протоколов аутентификации.

Противодействие подслушиванию. Злоумышленник, записавший выполнение протокола, устойчивого к прослушиванию, и имеющий возможность анализа этих записей, не сможет получить сведения, которые позволили бы ему узнать закрытый ключ, секретный ключ, пароль или иную информацию, которая позволила бы ему представиться заявителем. В данном случае отсутствие возможности означает, что попытки ведут к весьма маловероятному успеху, что количество криптографических операций, необходимых для успеха, как минимум, должно составлять 2^{80}, что количество возможных попыток пренебрежимо мало по сравнению с количеством возможных ключей или паролей.

Противодействие угадыванию паролей. Протокол аутентификации устойчив по отношению к атакам угадывания пароля, если злоумышленник, не имеющий априорного знания о пароле, не имеет возможности выявления пароля повторяющимися попытками аутентификации с предполагаемыми паролями. На это влияют и энтропия паролей, и сам протокол. Системы парольной аутентификации могут противостоять атакам угадывания путём требования применения только высокоэнтропийных паролей, обязательного применения ограничения количества неудачных попыток аутентификации либо частоты этих попыток. Для противостояния атакам на пароли, не направленных на конкретного пользователя, проверяющая сторона может также использовать средства обеспечения сетевой безопасности.

Противодействие воспроизведению. Протокол аутентификации противодействует атакам воспроизведения, если невозможно осуществить успешную аутентификацию путём записи и последующего воспроизведения сообщения аутентификации.

Противодействие перехвату. Протоколы аутентификации и передачи сообщений противостоят перехвату, если злоумышленник не может тайно вставлять, удалять или перенаправлять сообщения, а также вносить изменения в любую информацию, пересылаемую между заявителем и доверяющей стороной.

Противодействие имитации проверяющей стороны. Протокол аутентификации противостоит имитации проверяющей стороны, если злоумышленник не может узнать значение аутентификатора, выступая в роли проверяющей стороны.

Противодействие атаке «человек посередине». Протоколы аутентификации противодействуют атакам «человек посередине», если заявитель и проверяющая сторона взаимодействуют таким образом, который обеспечивает невозможность незаметного участия третьей стороны.

Как показано в работе [28, 29], основные применяемые в настоящее время протоколы аутентификации достаточно хорошо защищены от атак. Следовательно, уровень угроз и уязвимостей протоколов аутентификации будем считать низким.

При подтверждении принадлежности аутентификационной информации данному пользователю (валидации аутентификационной информации) также возможна реализация ряда угроз, направленных на нарушение функционирования участников проверки (угрозы валидации).

Валидация – это процедура подтверждения принадлежности АИ пользователю в момент проверки. Основным механизмом подтверждения является проверка действительности ЭУ, которое связывает данного пользователя с ИД и аутентификатором. Простейшим ЭУ является пароль, процедура проверки при этом сводится к сравнению хешей предъявленного пароля с хранимым в базе данных сервера аутентификации. В случае ЭУ в виде цифрового сертификата процедура валидации сводится к проверке действительности всей цепочки, начиная с сертификата пользователя и заканчивая корневым сертифи-

катом, заверяющим своей подписью цепочку доверенных сертификатов системы УЦ. Для такой проверки необходимо иметь развернутую систему сервисов проверки валидности сертификатов. Одним из таких сервисов является OCSP (Online Certificate Status Protocol) – протокол получения статуса сертификата в реальном времени, который применяется для предоставления пользователям УЦ актуальной информации о статусах сертификатов ключей подписи, описанный в RFC 2560. По протоколу OCSP можно получить информацию об изменении статуса цифрового сертификата в реальном времени.

Также для получения квитанции (подтверждения) необходимо использовать сервис DVCS, разработанный на базе RFC 3029 (Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols), в котором описан протокол создания квитанции – электронного документа с ЭП сервиса, фиксирующего во времени факт и результат проверки электронной подписи. Квитанция должна содержать штамп времени, получаемый с помощью сервиса TSP (Time-Stamp Protocol, RFC 3161). Штамп времени — это подписанный ЭП документ, которым Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции от документа. Само значение хэш-функции также указывается в штампе.

Проверяющие стороны должны быть уверены, что аутентификатор, предъявленный пользователем, действителен и создан не ранее, чем 24 часа назад.

В виде угроз валидации в настоящее время можно указать, в первую очередь, работоспособность сервисов OCSP, DVCS и TSP или их заменителей по всей цепочке выданных ЭУ. Гарантированно осуществить проверку валидности сертификата можно только в ограниченной области их применения. Заметим, что в принципе угрозы валидности также требуют введения уровней, поскольку процедуры опубликования, отзыва и приостановки действия сертификатов также должны нормироваться в зависимости от уровней информации, содержащейся в ИС, доступ к которой осуществляется с применением цифровых сертификатов. Градация уровней достоверности валидности сертификата

в данном случае должна исчисляться в часах на все критичные изменения его статуса, одним из примеров является электронная сделка по продаже электроэнергии, исчисляемая, в среднем, десятками или сотнями млн. руб. Обязательность соблюдения УЦ таких требований будет служить одним из критериев его «доверенности» и «квалифицированности». В статье 14 Федерального закона №63-ФЗ [72] требуется публикация изменения его статуса (например, аннулирования) сертификата «в течение одного рабочего дня». Будет ли считаться валидной транзакция, которая была совершена в первой половине этого дня? Этот вопрос останется открытым. В соответствии с принятым 27 декабря 2019 г. законом [212] проверка валидности сертификатов переносится на ДТС.

Учитывая вышеизложенное, оценим уровень угроз валидации как высокий.

Угрозы безопасности для принятия решения о результате аутентификации пользователя. Принятие решения, как правило, осуществляется на отказоустойчивом сервере, находящемся внутри контролируемого периметра. Процедура подобна хорошо изученной схеме принятия решения «свой-чужой». Примем, что уровень угроз и уязвимостей в данном случае является низкими.

Безусловно, процессный подход, основанный на представленном рассмотрении процессов аутентификации как последовательности определенных действий, не включает в себя весь комплекс возможных угроз. Так, к угрозам, которые не рассмотрены, можно отнести:

злонамеренное ПО, направленное на компрометацию аутентификаторов;

вторжение в системы пользователей, УЦ или проверяющих сторон с целью получения ЭУ или аутентификаторов;

угрозы компрометации аутентификаторов со стороны инсайдеров;

угроза реализации атак, при которых обманутый заявитель использует небезопасный протокол, думая, что использует безопасный, либо самостоятельно преодолевает средства защиты (например, принимая сертификаты серверов, не прошедшие проверку);

явный отказ пользователей, сознательно скомпрометировавших свой аутентификатор и другие угрозы.

Анализ перечисленных угроз и мер противодействия им не представляет трудностей. Например, для противодействия злонамеренному ПО, как правило, применяют многоуровневую антивирусную защиту и межсетевые экраны, а также обязательность обновления системного ПО. Одним из наилучших средств радикального противодействия является переход на технологии, исключающие применение аутентификатора в оперативной памяти компьютера, и перенаправление всех критичных операций по применению закрытого ключа внутри защищённого чипа устройства SSCD. Частично нерассмотренные угрозы будут исследованы ниже, на следующем уровне детализации.

На третьем уровне детализации рассмотрим угрозы аутентификации в устройствах и программном обеспечении.

В виде актуального объекта проведем анализ широко применяемых на практике устройств хранения аутентификационной информации (далее КН - ключевых носителей) JaCarta или eToken.

В зависимости от вариантов использования и выполнения рекомендаций производителей СКЗИ существует разный уровень угроз в зависимости от уязвимостей, используемых злоумышленником.

Одним из вариантов использования КН является хранение ключевого материала, сформированного СКЗИ в оперативной памяти компьютера. Если пользователь пренебрегает рекомендацией производителя КриптоПро о взведении флага «неизвлекаемость» для ключевого материала при импортировании его в КН, то уровень угроз можно оценить как «средний», а если компьютер использует несертифицированное системное ПО и не защищён должным образом от злонамеренного ПО, то «высокий». Если флаг «неизвлекаемость» взведён, то уровень угроз может считаться как «средний» или «низкий». Низким уровень угроз будет также при использовании КН для генерации ключевого материала.

Устройство генерации ключевого материала при необходимости также

можно детализировать. Современные представляют собой мини-ЭВМ, состоящую из процессора, сопроцессора, контроллера, как минимум, четырёх видов памяти, устройств ввода – вывода информации и т.д. Программное обеспечение состоит из ОС, платформы взаимодействия (например, Global Platform), менеджера команд, специального ПО, плагинов, драйверов и т.д. На уровне устройства также иногда необходимо проводить анализ угроз и уязвимостей. Особенно это актуально при сертификации устройства.

На четвертом уровне детализации рассмотрим угрозы аутентификации на уровне микросхем в составе КН класса SSCD.

Используемые для генерации ключевого материала и проведения критических операций (выработка криптографических ключей, электронная подпись) микросхемы должны производиться и проходить подготовку к эксплуатации также с учётом вероятных угроз. Идеальной мишенью для атак на них, организованных, как правило, на основе тщательно подготовленных сбоев, являются криптографические чипы смарт-карт, которые, фактически, находятся в полном распоряжении их владельца. Криптоаналитик может применить к смарт-карте все перечисленные ниже виды воздействий с целью определения прошитого в смарт-карте секретного ключа. Перечислим известные атаки на чип класса SSCD, основной целью которых является извлечение закрытого ключа (компрометация):

- физические атаки на чип (например, послойное снятие) с целью извлечения необходимой информации;
- изменение напряжения питания шифратора, существенно превосходящее допустимые пределы (spike attack);
- изменение тактовой частоты шифратора, выходящее за допустимые рамки (glitch attack);
- высокоточное облучение шифратора с помощью лазера, ультрафиолетовым, рентгеновским или каким-либо другим излучением (optical & radiation attacks);
- высокоточное наведение электромагнитного поля или локальный нагрев определенной области шифратора (electromagnetic & heating attacks);

- внесение изменений в конструкцию чипа, например, нарушение определенного порядка электрических контактов.

Основоположниками еще одного вида атак - на основе ошибок - являются три специалиста американской компании Bellcore: Дэн Боне (Dan Boneh), Ричард Де Милло (Richard DeMillo) и Ричард Липтон (Richard Lipton). В своей работе [213], вышедшей в 1996 г., они предложили данный вид атак и описали некоторые из возможных атак на основе ошибок на ряд асимметричных криптосистем. К сожалению, какого-либо универсального средства против известных методов воздействия на шифратор не существует. Однако можно существенно усложнить проведение атак против аппаратного шифратора, которые основаны на сбоях. В частности, могут быть использованы следующие способы защиты [214]:

- внедрение в шифратор детекторов различных видов воздействий (например, детекторов изменения напряжения, частоты питания и/или синхронизации, освещённости и т.д.), которые при обнаружении атаки выполняли бы его блокировку;
- использование встроенного датчика изменения геометрии чипа, который вызывает гарантированное уничтожение ключевого материала при послойном снятии;
- различного рода пассивное экранирование шифратора, устранение которого приводило бы к его выходу из строя;
- различные виды дублирования вычислений со сравнением результатов.

Указанные меры существенно повышают стоимость чипов или снижают их быстродействие, однако участившиеся атаки на закрытые ключи оправдывают эти затраты [215].

Таким образом, в данном разделе рассмотрены угрозы аутентификации на разных уровнях, при этом антропогенный источник угроз выделен как самый опасный. Из анализа угроз безопасности выполнения процедур аутентификации следует, что самыми опасными являются процедуры регистрации субъ-

екта доступа, хранения и применения аутентификационной информации. Основной причиной актуальности выявленных угроз является недостаточно развитая нормативная база в части отсутствия конкретных требований безопасности и технических регламентов выполнения указанных процедур. На примере рассмотрения процедур регистрации и хранения показано, что анализ угроз является обоснованием введения уровней доверия к результатам аутентификации с разными уровнями требований к безопасности их выполнения. Согласно [124] проведем идентификацию рисков аутентификации.

3.4 Управление рисками аутентификации

Управление рисками аутентификации можно проводить несколькими методами, исследованными автором в работах [**Ошибка! Закладка не определена.**, **Ошибка! Закладка не определена.**] на основе анализа применимости методов управления рисками аутентификации [149]. При этом после описания объекта и анализа угроз требуется идентифицировать риски, провести их анализ и выработать меры по снижению вероятности их реализации.

Метод 1. Анализ вероятных опасных событий, рассмотренный в главе 2 применительно к первичной идентификации субъекта доступа. На основе анализа многолетнего опыта построения и эксплуатации ряда промышленных СИА выделим ряд вероятных опасных событий $ВОС_i$, $i = 1, M.$ Перечислим эти события и приведём для примера некие оценки частоты их реализации, при этом размер потенциального ущерба положим равным 1, чтобы на безразмерном примере проще было рассмотреть подходы к управлению рисками аутентификации.

$ВОС_1$. Целенаправленные действия злоумышленника при регистрации. Регистрация – одна из самых ответственных операций процессов аутентификации, существенно влияющая на безопасность, надёжность и, в конечном счёте, на доверие к результатам работы СИА. Тем не менее, процедура регистрации является одной из самых не затронутых регулированием. Определим подобные действия при регистрации как «маскарад». Оценим частоту такого

события для существующих СИА в достаточно широких пределах: 10^{-7}-10^{-5} в год.

$ВОС_2$. Злоумышленник для доступа к интересующим его информационным ресурсам может воспользоваться уязвимостями СИА. Поскольку требования ИБ к СИА пока не сформированы, это опасное событие имеет вероятность осуществиться. Определим данное событие как «уязвимости СИА» и оценим частоту в пределах 10^{-5}-10^{-3}.

$ВОС_3$. Этот тип вероятного опасного события связан с действиями инсайдера, когда легальный пользователь (или администратор) помогает злоумышленнику пройти все рубежи безопасности СИА. Кратко назовём это событие «помощь инсайдера». Оценки частоты: 10^{-6}-10^{-4}.

$ВОС_4$. Завладение злоумышленником идентификатором доступа и аутентификационной информацией легального пользователя. Это может быть кража, клонирование ИД и АИ, подсмотренный пароль, перехваченный PIN-код. Определим этот тип «кража ИД и АИ» и оценим частоту: 10^{-5}-10^{-3}.

$ВОС_5$. «Вход по принуждению» встречается все реже и реже: 10^{-7}-10^{-5}.

$ВОС_6$. Ошибки и/или целенаправленные действия злоумышленника при смене пароля, замене цифрового сертификата доступа или вариант «забыл дома смарт-карту». Коротко назовём этот тип «смена АИ» и оценим частоту в пределах 10^{-5}-10^{-3}.

$ВОС_7$. Данный тип ВОС связан с ошибками валидации ЭУ. Определим его как «ошибки валидации». Оценки частоты: 10^{-6}-10^{-4}.

$ВОС_8$. Ошибки в принятии решения «свой–чужой» на серверах. Частота подобного события 10^{-7}-10^{-5}.

$ВОС_9$. Имитация доверяющей стороны. Особенно распространен данный тип событий при предоставлении Web – доступа. Фишинг (подмена сайта) оценим в пределах 10^{-4}-10^{-2}.

$ВОС_{10}$. Подмена доверенной стороны или объекта (spoofing) оценим как 10^{-6}-10^{-4}.

$ВОС_{11}$. Риск добровольной передачи персонального устройства аутентификации оценим в пределах 10^{-4}-10^{-2}. Средство борьбы – усиленная персонализация (совмещение смарт-карты, содержащей АИ, с зарплатной или введение карт с технологией Match on Card).

$ВОС_{12}$. Воздействие вредоносного программного обеспечения, с учетом политики безопасности организации, оценивается как 10^{-4}-10^{-2}.

Перечисленные оценки для абстрактной типовой ИС представлены в табл. 3.8.

Таблица 3.8 – Перечень событий и интервальная оценка частоты их реализации (шт./год).

$ВОС_1$	Регистрация злоумышленника под видом легального пользователя	$10^{-7} – 10^{-5}$
$ВОС_2$	Использование уязвимостей СИА	$10^{-5} – 10^{-3}$
$ВОС_3$	Помощь инсайдера	$10^{-6} – 10^{-4}$
$ВОС_4$	Завладение злоумышленником АИ легального пользователя	$10^{-5} – 10^{-3}$
$ВОС_5$	"Вход под принуждением"	$10^{-7} – 10^{-5}$
$ВОС_6$	Ошибки или целенаправленные действия при смене АИ	$10^{-5} – 10^{-3}$
$ВОС_7$	Ошибки валидации	$10^{-6} – 10^{-4}$
$ВОС_8$	Ошибки в принятии решения "свой-чужой"	$10^{-7} – 10^{-5}$
$ВОС_9$	Фишинг	$10^{-4} – 10^{-2}$
$ВОС_{10}$	Подмена доверенной стороны (spoofing)	$10^{-6} – 10^{-4}$
$ВОС_{11}$	Риск добровольной передачи устройства аутентификации и аутентификационной информации	$10^{-4} – 10^{-2}$
$ВОС_{12}$	Воздействие вредоносного ПО	$10^{-4} – 10^{-2}$

Для оценки рисков и надёжности работы системы согласно [105] для каждой конкретной ИС надо ранжировать перечисленные события на основе вероятности их появления в течение года f и относительной величины риска $\overline{R}$. Условием нормировки является

$$\bar{R} = \frac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} C_i} = 1 \qquad (3.2)$$

где $R_i = C_i \times f_i$ - величина риска $ВОС_i$, C_i – величина ущерба от $ВОС_i$,

M- количество $ВОС_i$.

В качестве примера приведем результаты ранжирования некоторых из

перечисленных выше ВОС для абстрактной ИС в виде таблицы 3.9

Таблица 3.9 - Пример ранжирования рисков аутентификации

ВОС	**Описание опасного события**	f_i	R_i
1	Воздействие вредоносного ПО	10^{-3}	0,122
2	Фишинг	10^{-4}	0,141
3	Риск добровольной передачи носителя (ключа и АУ)	10^{-4}	0,110
4	Ошибки или целенаправленные действия при смене АУ	10^{-4}	0,096
5	Использование уязвимостей системы АУ	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

Результаты ранжирования представлены на рисунке 3.13 в виде пронумерованных кружков, обозначающих номер события в таблице 3.9 в плоскости переменных $\{R_i,\ lgp_i\}$.

Из анализа рис. 3.13 следует, что, например, для снижения ВОС 2 (фишинг – подмена сайта, на который пользователю необходимо предоставить доступ) достаточно перейти с парольной аутентификации на технологию защищенного доступа с использованием TLS (Transport Secure Socket Layer) с двусторонней взаимной аутентификацией на основе применения цифровых SSL-сертификатов на стороне сервера и клиента.

Это приведет к снижению вероятности подмены сайта приблизительно на два порядка (с 10^{-4} до 10^{-6}). Еще примерно на два порядка можно снизить вероятность фишинговой атаки за счет применения технологии хранения закрытого ключа и клиентского сертификата в устройстве класса SSCD (Secure Signature Creation Design – устройство генерации ключей электронной подписи). Итоговое снижение ВОС в год за счет указанных мер может снизиться до 10^{-6} и даже ниже.

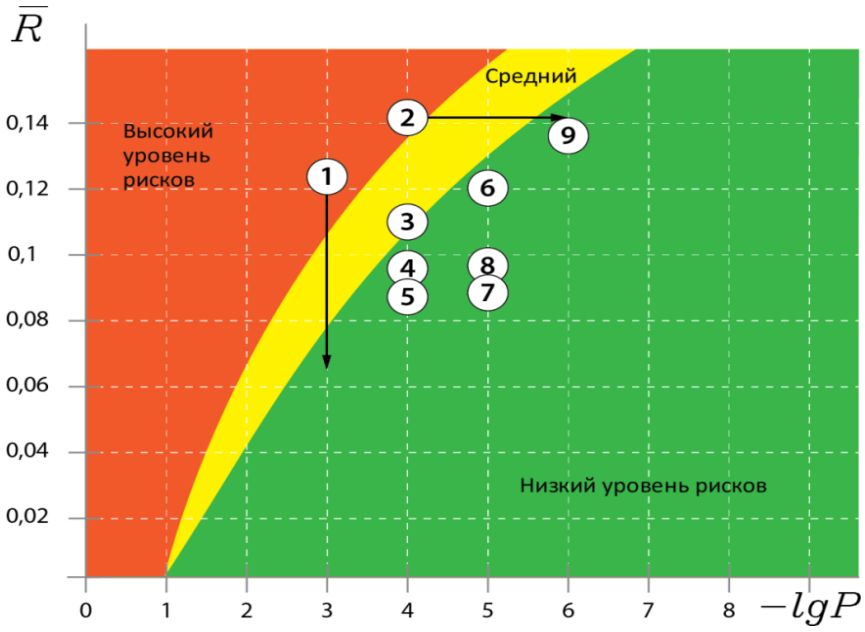

Рис. 3.13. Пример поля управления рисками аутентификации

В то же время снижение рисков в рассмотренных примерах может проводиться в отношении не только частоты реализации ВОС, но и размера риска, используя в качестве механизмов снижения рисков традиционные способы обеспечения доступности, целостности и конфиденциальности информации, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты. При этом риски будут снижаться в вертикальном направлении до определенного уровня.

Соответствующими способами можно снизить риски за счет внедрения СЗИ (ВОС 1 – установка антивирусного программного обеспечения; ВОС 3 – переход на смарт-карты с технологией Match-on-Card; ВОС 8 – внедрение СЗИ в систему АУ).

При достижении приемлемых уровней рисков по частоте (в горизонтальном направлении) и размеру (в вертикальном направлении) процесс управления рисками можно считать выполненным.

Если приемлемых уровней для остаточных рисков достичь не удается, необходимо подключать такие механизмы управления рисками, как уклонение от

риска (ликвидация причин и/или последствий риска), ограничение (нейтрализация) риска (например, путем реализации контрмер, уменьшающих воздействие угроз безопасности), перенос риска на стороннюю организацию (страхование рисков).

К достоинствам данного метода анализа рисков аутентификации можно отнести его наглядность. Недостатком же его является необходимость в большом объеме предварительной работы по выявлению ВОС, зачастую в условиях отсутствия фактического материала в виде статистических данных или результатов мониторинга за достаточно продолжительный период времени. В таких случаях, согласно ГОСТ Р ИСО/МЭК 13335-1-2006, рекомендуется воспользоваться методом экспертных оценок.

Метод 2. Анализ дерева уязвимостей, угроз и контрмер.

В данном методе риски представляются в виде дерева уязвимостей и угроз, на которые накладываются соответствующие планируемые или применяемые контрмеры. В качестве входного параметра используется инициирующее событие и среднегодовая вероятность его реализации, в качестве выходного параметра — результирующее событие и вероятность его реализации. Как правило, рассматриваемые параметры в таком анализе нормируются. Для вероятностей p_i реализации нежелательных событий условие нормировки можно записать в виде

$$\sum_{i=1}^{M} p_i = 1$$

где M — число возможных состояний системы при реализации одного события.

Пример такого анализа для события в виде авторизации злоумышленника в качестве легального пользователя ИС на основе результатов работы [**Ошибка! Закладка не определена.**] приводится на рис. 3.14.

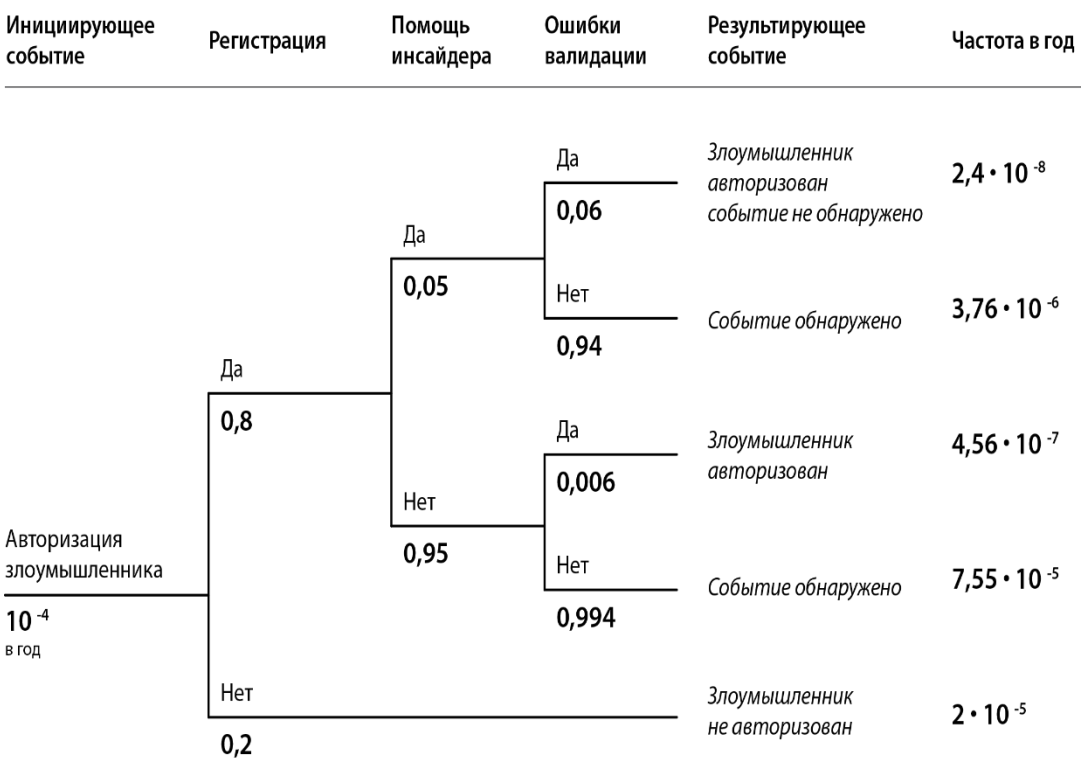

Рисунок 3.14. Пример построения дерева событий

В качестве достоинства данного метода можно выделить наглядность цепочки событий, которые могут реализовываться в рассматриваемой системы. Существенным недостатком данного метода применительно к задаче аутентификации является большой объем определения вероятностей событий. В целом метод не слишком удобен для управления рисками аутентификации при УЭВ.

Метод 3. Управление рисками попарного анализа "угроза — степень тяжести последствий от потери свойств ИБ". Метод применим для анализа при условии достаточно полного набора статистических данных выявленных угроз для рассматриваемой конкретной системы и условий ее функционирования. Этот метод достаточно развит для многих сфер экономики, в частности, в качестве основы применяется в методике оценки рисков, утвержденной Банком России [216].

Суть метода состоит в управлении рисками при рассмотрении пар «угроза - степень тяжести последствий от потери свойств ИБ», в формализованном виде это выглядит следующим образом:

$$R_p = \sum_{i=1}^{k} P_p * I_{pi}$$

где R_p – величина риска от реализации угрозы p,

P_p – вероятность реализации угрозы p,

I_{pi}- степень тяжести последствий от потери свойств ИБ, обусловленная реализацией угрозы p на свойство безопасности i, k- число свойств.

Риски R_p считаются допустимыми, если $R_p \leq R_a$, где R_a – допустимый уровень рисков. В основе метода лежит анализ избыточных рисков, просуммированных для всех случаев $R_p - R_a > 0$. Пусть число избыточных рисков равно N. Тогда можно определить «обезразмеренное» среднее значение избыточного риска по формуле:

$$R_{average} = \frac{\sum_{p=1}^{N}(R_p - R_a)}{N * (R_{max} - R_a)}$$

где R_{max} – максимальное значение риска.

Величина $R_{average}$ как средний избыточный риск позволяет оценить состояние ИБ в целом. Так, при близких к нулю значениях систему аутентификации можно оценить как защищенную с точки зрения ИБ, а при стремлении $R_{average}$ к единице СИА можно охарактеризовать как слабо защищенную. Одним из явных достоинств данного метода является возможность разбиения отрезка $[0,1]$ значений $R_{average}$ на интервалы, которые могут выполнять функции необходимого числа уровней ИБ. К недостаткам данного метода следует отнести необходимость тщательного анализа угроз и уязвимостей СИА. В целом данный метод может применяться для управления рисками аутентификации. Модификацией рассматриваемого метода является оценка не только среднего избыточного риска, но и нормализованного среднеквадратичного отклонения, анализ которого более чувствителен к аномально высоким рискам и более устойчив к добавлению пар с низким избыточным риском [216].

Метод 4. Графовый метод управления рисками по изменению времени, необходимого на реализацию атаки. Этот метод априори считается одним из самых эффективных при проектировании и построении информационных си-

стем и СИА как части ИС. Метод основан на базисных положениях классической теории надежности механизмов и машин. Рассмотрен в работе [**Ошибка! Закладка не определена.**] применительно к задаче моделирования СИА для оценки надежности ее функционирования. Для описания процессов используются Марковские и полумарковские методы анализа в предположении, что условия применимости этих методов соблюдаются [35]. Суть метода в формализованном виде применительно к анализу рисков можно представить следующим образом.

Количественные способы оценки рисков базируются на формуле:

$R = f*C$, где R- величина риска, f – вероятность наступления опасного события, C – степень тяжести последствий от его реализации.

Направленный граф состояний системы, вершины которого характеризуют вероятные состояния системы, а ребра соответствуют переходам из одного состояния в другое, позволяет оценить время перехода из i-го состояния в j-ое. Одним из результатов применения графового метода является то, что он позволяет оценивать время, необходимое для выполнения отдельных переходов из одного вероятного состояния системы в другое, в том числе, оценивается вероятность перехода в опасное состояние. В некоторых моделях время и достижимость конечной цели может быть достаточно быстро оценено методом Петри-Маркова [31,32]. При введении средств защиты возможный путь и, соответственно, время, изменяются. Оценки нормализованного снижения рисков может производиться по формуле: $dR = 1 - t_{old}/t_{new}$, где t_{old} - время без учета введения новых СЗИ, t_{new} – время функционирования СИА с учетом введенных СЗИ. Чем ближе к 1 значение dR, тем более защищенная система с введенной СЗИ. Достоинством данного метода является его наглядность и универсальность, к числу недостатков следует отнести необходимость понимания процессов и умение применять, а в ряде случаев и строить математические модели СИА, что не является простой задачей для неподготовленного специалиста.

Метод 5. Экономический метод управления рисками. Суть метода состоит в повышении стоимости реализации атаки при возможном снижении

стоимости установки дополнительных СЗИ для реализации контрмер. В формализованном виде ущерб *SAL* от однократной реализации угрозы можно оценить как *SAL= AV*EF*, где *AV* – стоимость объекта атаки, *EF* – относительный ущерб от успешной реализации одной атаки. Если принять в рассмотрение среднегодовую частоту реализации угрозы *AWO*, то ожидаемый годовой ущерб *SYL* может быть оценен по формуле *SYL=SAL*AWO*. При этом значение *AWO* может быть определено из статистических данных о нарушениях ИБ в СИА или определяться экспертными оценками. Экономический эффект от реализации мер по снижению вероятности данной угрозы можно оценить как *ROI=(AWO*RM-CZI)/CZI*, где *RM*- коэффициент снижения риска в результате внедрения мер по снижению вероятности реализации угрозы, *CZI* – стоимость указанных мер. При положительном значении *ROI* реализация мер является экономически оправданной. *ROI* является инструментом экономической оценки эффективности работы службы ИБ, целью которой является увеличение *ROI*.

Экономический эффект действий атакующего *ROA* может быть оценен по формуле *ROA=WI/(ERS+EAS)*, где *WI* – ожидаемая выгода от успешной атаки, *ERS*- затраты на атаку до внедрения СЗИ, снижающего вероятность реализации данной угрозы, *EAS*- дополнительные затраты на преодоление защитных функций СЗИ. Целью службы защиты информации является минимизация величины *ROA*, выражающаяся в снижении привлекательности ИС как объекта атак. Достоинством данного метода является простота и ясность организации противодействия реализациям угроз, при этом необходимо очень хорошо уметь моделировать пути реализации угроз и понимать методы противодействия.

Таким образом, в итоге рассмотрены все основные этапы исследования, составляющие метод анализа рисков аутентификации, включая один из ранее не изученных вопросов управления рисками аутентификации.

3.5 Моделирование процесса аутентификации для исследования надежности и безопасности результатов аутентификации

Исследования функциональной надёжности систем идентификации и аутентификации включают (рисунок 3.15):

– описание состава и содержания процессов и систем идентификации и аутентификации;

– определение целей анализа и распределение их по уровням моделирования;

– анализ надежности процессов и систем идентификации и аутентификации;

– оценка результатов и выработка рекомендаций по совершенствованию процессов и систем идентификации и аутентификации с точки зрения надежности.

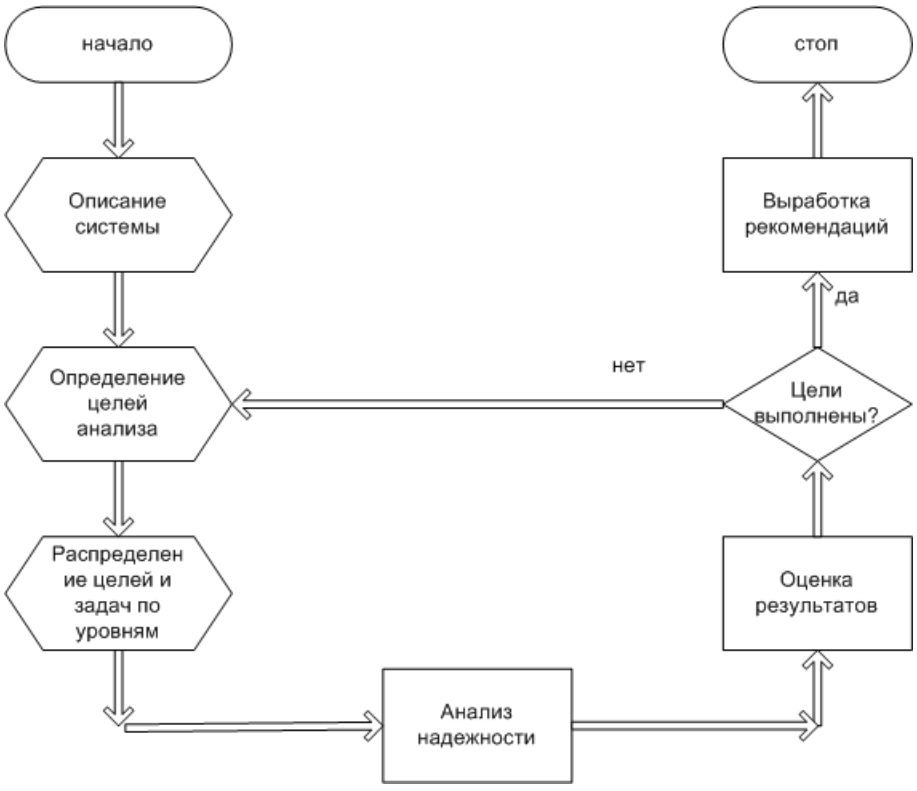

Рисунок 3.15 - Алгоритм исследования функциональной надежности СИА

3.5.1. Концепция моделирования СИА. Моделирование СИА условно можно разделить на три уровня. Концепция и принципы моделирования изложены в [**Ошибка! Закладка не определена.**].

Верхний (первый) уровень – модели поведения СИА как единого целого. При таком подходе СИА является отдельной системой, т.е. представляя собой подсистему рассматриваемой ИС. При этом из традиционной триады безопасности приоритеты для СИА должны быт выстроены в следующем порядке: доступность СИА для всех заявок на аутентификацию, целостность ПО системы, конфиденциальность идентификационной и аутентификационной информации субъектов доступа.

3.5.2. Моделирование на верхнем уровне

Ярким примером моделирования на верхнем уровне являются модели, основанные на применении хорошо развитого к настоящему времени математического аппарата систем массового обслуживания (СМО). С помощью моделей СМО можно определить необходимые интегральные характеристики СИА при их проектировании. При этом входными (заданными) параметрами обычно являются данные о входящем потоке заявок на обслуживание и процессе обслуживания. В качестве выходных параметров, как правило, определяется время обслуживания заявок и время ожидания (задержки). Используя модель верхнего уровня, можно выполнить грубые оценки надежности СИА. Обеспечение целостности и конфиденциальности в данном случае является стандартной задачей и не является предметом исследования. К первому уровню также можно отнести модели взаимодействия СИА с подсистемой управления доступом и другими подсистемами защиты информации. Главной целью моделей верхнего уровня является выбор оборудования, системного и прикладного ПО, а также способов и механизмов интеграции сетевого и серверного оборудования и программного обеспечения для проектирования СИА с заданными выходными параметрами.

При выборе технологий, способов и механизмов ИА, а также оценки рисков ИА и увязки проектируемой СИА с утвержденными политиками безопасности организации требуется моделирование второго уровня – моделирование процессов ИА. Процессы моделирования второго уровня ИА пока не

развиты. Данная работа является в этом смысле пионерской. Примеры построения моделей и некоторых методик расчета рассмотрим ниже в данной главе.

На третьем уровне производится моделирование процедур, составляющих процесс ИА. К настоящему времени достаточно полно исследованы уязвимости протоколов аутентификации. В виде примера подробного анализа можно привести работу [28]. Имеются модели поведения пользователя – например, при составлении модели нарушителя. Целями третьего уровня моделирования является оценка рисков отдельных процедур ИА, выработка требований безопасности к процедурам аутентификации, технических регламентов и т.д.

На четвертом уровне рассматриваются устройства, программное обеспечение и другие элементы, участвующие в обмене информации в рамках процедур аутентификации. Целью моделирования при этом является оценка рисков при выборе того или иного технического решения. Примерами могут служить работы по анализу рисков применения устройств, используемых для генерации и хранения АИ в виде защищенных цифровых контейнеров ключевого материала, или плагина, подгружаемого в сессии браузера по защищенному каналу с портала.

Согласно принятой в данной работе методике сначала рассмотрим надежность и безопасность СИА, потом последовательности входящих в нее процедур, а при необходимости, опустимся на более низкие уровни общей модели.

На первом (верхнем) уровне моделирования СИА рассматривается как один элемент с входными и выходными характеристиками, часть из которых задается, а часть определяется, как правило, хорошо развитыми аналитическими методами.

При проектировании СИА необходимо выполнить предварительный расчет производительности системы с учетом выбранных технологий, средств и режима работы (8*5*365, круглосуточно и др.). Главной целью расчетов является обеспечение заданных характеристик **доступности** информационных

ресурсов и технологий, необходимых для выполнения служебных обязанностей сотрудниками, при соблюдении конфиденциальности и целостности хранимой, передаваемой и обрабатываемой информации. Существующие методы проведения таких исследований, например, [15,17,22], как правило, основаны на применении автоматизированной обработки данных. Получаемые с помощью СМО результаты обычно связаны с расчетом вероятностных характеристик времени обработки заявок в СИА при заданных характеристиках входящего потока и процесса обслуживания заявок. При проектировании чаще всего решаются обратная задача: определение необходимого времени обработки заявок согласно выдвинутому заказчиком техническому заданию (в том числе учитывающему интенсивности потока λ) при заданном уровне средней задержки времени обработки требований на аутентификацию. Другим примером обратной задачи может являться расчет обязательности обработки СИА всех заявок на аутентификацию от легальных пользователей ИС. В виде выходных параметров расчетов в обоих случаях должны получаться величины параметров СИА, которые могут быть изменены на этапах проектирования системы.

Зачастую, особенно на ранних стадиях проектирования, у проектировщика отсутствует достаточный уровень знаний вероятностной структуры входящих потоков заявок и среднего времени их обслуживания. Поэтому исследователю необходимо дополнительно оценивать влияние априорных предположений о вероятностных характеристиках входящих потоков и потоков обслуживания. Для этого, как правило, предварительно выполняется анализ предположений, исходя из условий, для которых проектируется СИА.

Так, чаще всего, предполагается, что λ известна. Это предположение основывается на том, что обычно в техническом задании на проектирование задается число поступающих запросов в СИА за определенный период. При этом неопределенность проектировщика о входящем Потоке заявок отражается в предположении о дисперсии временного интервала между поступлениями соседних запросов. Основываясь на подходе, предложенном в работе [22],

будем рассматривать варианты простейшего и произвольного входящих потоков с независимыми интервалами поступления заявок.

Оценка временных характеристик СИА предусматривает определение интенсивности обработки заявок, гарантирующей выполнение заданных временных ограничений на средние времена прохождения требований в системе

$$\frac{1}{\mu} < \frac{1}{\lambda}, \text{ т.е. } \lambda < \mu \tag{3.3}$$

где μ – интенсивность потока обслуживания.

Во многих практических задачах потоки событий предполагаются обладающими тремя основными свойствами: стационарностью, ординарностью и отсутствием последействия. Стационарными называются потоки, для которых вероятность поступления определенного количества заявок в течение определенного промежутка времени не зависит от начала отсчета времени, а определяется только длиной промежутка. Ординарность означает, что вероятность появления двух и более событий на достаточно малом интервале пренебрежимо мала по сравнению с вероятностью появления одного события и вероятностью не появления ни одного. Отсутствие последействия означает независимость количества событий, попавших в любой неперекрывающихся между собой промежутков времени, от числа событий, попавших в другие промежутки.

Простейший поток описывается формулой Пуассона:

$$P_n(t) = \frac{(\lambda t)^n}{n!} e^{-\lambda t} \tag{3.4}$$

где n определяется из условия: вероятность того, что в интервале времени (0, t) наступит ровно n событий.

Для различных типов СМО, с учетом характера математических моделей их построения, принято трехбуквенное обозначение вида A/B/m, где A и B описывают распределение времени между заявками и временем их обслуживания соответственно, а m – число каналов (обслуживающих приборов [23]).

A и B принимают значения из следующего набора символов: M – показательное, E_a – распределение Эрланга порядка a, D – детерминированное, G – распределение общего вида. Иногда указывают длину очереди k, т.е. A/B/m/k. При этом емкость накопителя должна вмещать не менее k заявок.

Важнейшей характеристикой каждого канала является время обслуживания заявки. Величину времени обслуживания $t_{обсл}$ следует считать случайной величиной, полной характеристикой которой является закон распределения

$$F(t) = P\,[t_{\text{обсл}} < t] \tag{3.5}$$

где $P\,[t_{\text{обсл}} < t]$ вероятность того, что время обслуживания $t_{обсл}$ не превосходит некоторого значения t.

Законы распределения $F(t)$ могут быть различного вида. В теоретическом виде и практических приложениях наибольшее распространение получил показательный закон. Решения для показательных распределений входящего потока и времени обслуживания M/M/1 можно найти во многих работах, например в [15,22,23]. Выбор модели и распределения потоков заявок и их обработки на стадиях проектирования определяется техническим заданием для конкретной СИА.

3.5.3. Моделирование системы идентификации и аутентификации на втором уровне

На втором уровне моделирования на основе предварительной оценки рисков учитывается детализация составных частей СИА с целью уточнения влияния на доступность, конфиденциальность и целостность определенных параметров. Покажем это на простейшей модели процесса аутентификации [**Ошибка! Закладка не определена.**]. Для моделирования процесса аутентификации следует разделить его на однородные по функциональным и вероятностно-статистическим характеристикам блоки. При этом разные блоки имеют существенно отличающиеся характеристики по времени. Например, процедура регистрации производится единожды и может быть относительно

краткой по времени. Хранение идентификационных данных, АИ и электронных удостоверений – длительная процедура, к которой могут быть применены вероятностные и статистические методы. Остальные процедуры (предъявление идентификаторов, идентификация, предъявление АИ, проверка подлинности ИД с помощью АИ, валидация, принятие решения) тесно связаны с временем выполнения процедур и многократно повторяются в течение жизненного цикла АИ – как правило, минимум один раз в день. В итоге выделяем следующие блоки:

1) регистрация – не связан со временем (стационарный процесс);

2) хранение – связан со временем, длительная процедура, как правило, для строгой аутентификации от года до трех лет;

3) предъявление ИД и идентификация – как правило, процедура длится доли секунды, возможны ошибки пользователей (частое событие) и сбои сервера хранения учетных данных пользователей (редкое событие);

4) предъявление АИ и протоколы обмена – отказы (отказы аппаратного и программного компонентов, случайные, неслучайные ошибки пользователей, атаки – такие события происходят весьма редко);

5) валидация – вероятность отказа для корпоративных закрытых систем мала, для ИСОП – велика;

6) процедура принятия решения («свой-чужой») – простая; процесс принятия решения (положительный или отрицательный результат прохождения процедуры аутентификации) – фактически ответ «да или нет» для пропуска (или отказа в проходе) к следующей процедуре (проверке соответствия учетной записи и идентификатора определенной роли доступа для последующей авторизации пользователя).

Вслед за процедурой хранения секрета и ЭУ следует процедура предъявления ИД, а следом и АИ, ЭУ для отработки протокола аутентификации. Способ предъявления аутентификатора полностью зависит от протокола аутентификации и его настроек. Например, для аутентификации клиента

SSL/TLS и серверов в протоколе IPSec этот процесс происходит в автоматическом режиме. Процедуры предъявления секрета (подпись сообщений в виде отклика претендента) и проверки валидности ЭУ являются самыми длительными (порядка половины, а то и одной секунды каждая). Процедура принятия решения длится доли секунды и происходит на сервере аутентификации. Следовательно, можно представить динамические процедуры (предъявления, протоколов, валидации и принятия решения) в графической форме в виде структурных блоков (**Ошибка! Источник ссылки не найден.**):

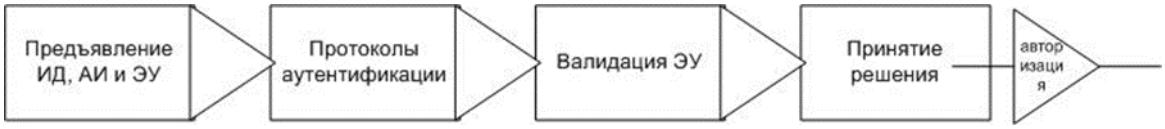

Рисунок 3.16 – Последовательность процедур аутентификации

Согласно основным положениям теории структурной надежности [35] сначала определим условия работоспособности системы и сформулируем критерии отказа. Предполагается, что элементы (в рассматриваемом случае C_i – процедуры аутентификации, i = 1,2,3.) отказывают независимо друг от друга, т. е. отказ любых элементов не изменяет надежности остальных элементов.

Пусть E_i будет событием элемента C_i, происходящего в определенный момент времени. Безотказность СИА для представленной модели

$$P_C = \prod_{i=1}^{n} P[E_i]. \tag{3.8}$$

В случае известных распределений наработок на отказ отдельных элементов $F_i(t) = 1 - P_i(t)$, для независимых элементов вероятность безотказной работы СИ определяется выражением:

$$P_C(t) = \prod_{i=1}^{n}[1 - F_i(t)] = \prod_{i=1}^{n} P_i(t) \tag{3.9}$$

Принятой в большинстве работ по надежности подобных систем функцией распределения отказов в каждом элементе $F_i(t)$ является экспоненциальное распределение наработки на отказ:

$$F_i(t) = 1 - P_i(t) = 1 - e^{-\lambda_i t} \quad (3.10)$$

с постоянной интенсивностью отказов $\lambda_i = const$, i=1,2,3.

Обозначим $\Lambda = \sum_{i=1}^{n} \lambda_i$, тогда

$$P_C(t) = exp(-\sum_{i=1}^{n} \lambda_i t) = exp(-\Lambda t) \quad (3.11)$$

При условии $\Lambda t << 1$ допустимы следующие приближенные выражения: $P_C(t) \approx 1 - \Lambda t$, и $Q(t) \approx \Lambda t$, где $Q(t) = 1 - P_C(t)$ – вероятность отказа.

Другими словами, вероятность безотказной работы системы идентификации и аутентификации в данном случае всегда меньше, чем вероятность отсутствия отказов самого ненадежного элемента. Она существенно возрастает при увеличении надежности самого ненадежного элемента.

Для ИС с большим числом пользователей одной из часто встречающихся проблем является производительность СИА, характеризующаяся потоком μ обработки входящих заявок λ на ИА. В работах [22,23] показано, что при $\frac{\lambda}{\mu} \leq$ 0,8 все заявки будут обработаны без очереди. Для большинства ИС эта проблема не актуальна, т.к. интенсивность входящего потока легко может быть рассчитана в пиковой нагрузке (начало рабочего дня) и условие $\frac{\lambda}{\mu} \leq 0{,}8$ может быть выполнено.

Покажем это на простейшей модели процесса аутентификации (рис.3.16), применив к этой схеме классическую задачу преодоления эшелонированной обороны, изложенную в работе [**Ошибка! Закладка не определена.**]. Представим выбранные блоки, участвующие в процессах ИА, в виде ряда последовательно расположенных групп устройств r_i (Рисунок), обслуживающих поток заявок с интенсивностью λ и средним временем обслуживания t. Заявки, которые не были обслужены первым устройством, попадают на второе устройство, заявки, которые не были обслужены вторым устройством, попадают на третье и т.д.

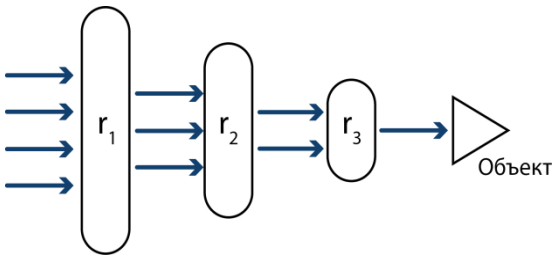

Рисунок 3.17 – Ряд устройств, обслуживающих поток заявок

Аналогом такой схемы является схема преодоления злоумышленником эшелонированной защиты информации [217]. Попробуем оценить эффективность такой обороны, состоящей из однотипных устройств, в предположении показательных законов распределения времени между заявками с интенсивностью λ.

Определим вероятность того, что заявки получат отказ на устройствах первой группы и поступят на устройства второй группы, с помощью формулы Эрланга:

$$P_1 = \frac{a_1}{d_1} \tag{3.12}$$

где $a_1 = \frac{\rho^{r_1}}{r_1!}$;

$$d_1 = \sum_{i=0}^{r_i} \frac{P_i}{i!}.$$

Если устройства второй группы также будут заняты, заявки получат отказ. Вероятность такого события:

$$P_2 = \frac{a_2}{d_2} \tag{3.13}$$

где $a_2 = \frac{\rho^{\sum_{i=1}^{k} r_1}}{(\sum_{i=1}^{k} r_i)!}$;

$$d_2 = \sum_{i=0}^{r_1+r_2} \frac{P_i}{i!}$$

Если число таких групп k, вероятность прохода злоумышленника сквозь всю систему обороны равна

$$P_k = \frac{a_k}{d_k} \tag{3.14}$$

где $$a_k = \frac{\rho^{\sum_{i=1}^{k} r_1}}{\left(\sum_{i=1}^{k} r_i\right)!}$$

$$d_2 = \sum_{i=0}^{k} \frac{P_i}{i!}$$

Для примера посчитаем вероятности, приняв значения $k = 1, 2, 3$. Поскольку $\rho = \lambda t$, положим интенсивность потока заявок $\lambda = 1$ и среднее время $t = 0{,}1$. Тогда

$$P_1 = \frac{a_1}{d_1} = \frac{0{,}1}{1{,}1} = 0{,}0909;$$

$$P_2 = \frac{a_2}{d_2} = \frac{0{,}005}{1{,}105} = 0{,}045249;$$

$$P_3 = \frac{a_3}{d_3} = \frac{0{,}000167}{1{,}10516},$$

из чего следует, что вероятность «прорыва» существенно уменьшается от эшелона к эшелону.

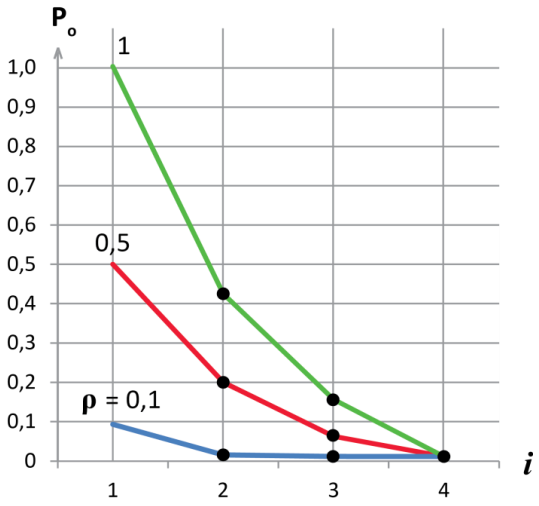

Рисунок 3.18 – Расчет вероятности прорыва через эшелоны обороны

Добавим в расчеты четвертый «эшелон» и получим кривые вероятности отказа P_o от количества эшелонов $k = 0,\ldots,4$ в зависимости от интенсивности

потока $\rho = \lambda t$, из которых видно, что с уменьшением ρ «пропускная» способность обороны падает по мере увеличения числа эшелонов обороны менее интенсивно. Возвращаясь к задаче аутентификации, отметим, что интерпретация четырех «эшелонов» обороны будет соответствовать блокам предъявления идентификатора и аутентификатора, проверки подлинности аутентификатора, валидации и принятия решения. Полученные расчетным путем значения P_o должны соответствовать вероятности отказа в аутентификации. Причем в рассматриваемом случае отказ не будет критичным для аутентификации: претенденту, как правило, дается минимум три попытки предъявления аутентификационных данных. Как и для моделей, рассмотренных выше, в данном случае решается обратная задача. Необходимо обеспечить выполнение всех заявок от легальных пользователей на аутентификацию.

Задача, таким образом, сводится к определению количества резервных каналов для обеспечения заданного потока интенсивности заявок на аутентификацию в единицу времени. Пример расчета реальных значений вероятности отказа P_0 одноканального потока заявок $\rho = \lambda t$ однократной парольной аутентификации с допустимым порогом отказа P_0 = 5% представлен ниже (Рисунок)

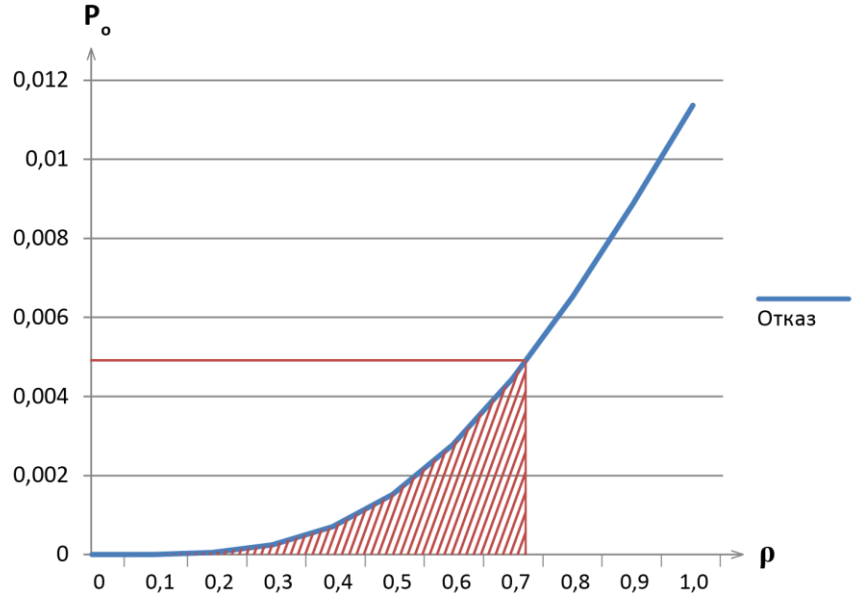

Рисунок 3.19 – Пример расчета допустимых значений отказов в аутентификации

Видно, что расчетные значения P_o в рабочем диапазоне значений $\rho \leq 0{,}5$ не достигают величины 0,05 с большим запасом.

Полученные соотношения позволяют определить такие параметры, как вероятность безошибочной работы системы в условиях заданного потока заявок и вероятность безошибочной работы за заданное время [35].

При дальнейшем развитии модели процедур аутентификации можно усложнять, последовательно вводя учет новых параметров. Покажем, как можно учесть влияние поглощения на примере укрупненной модели аутентификации. Обозначим состояния системы в процессе аутентификации: 1 – регистрация нового пользователя системы выполнена; 2 – произведено подтверждение подлинности предъявленных претендентом (пользователем) аутентификационных данных; 3 – процедура принятия решения «свой-чужой» выполнена; 4 – состояние отказа аутентификации легального пользователя; 5 – состояние опасного отказа (аутентификация злоумышленника под видом легального пользователя). Тогда работу системы аутентификации представим в виде направленного графа состояний (Рисунок).

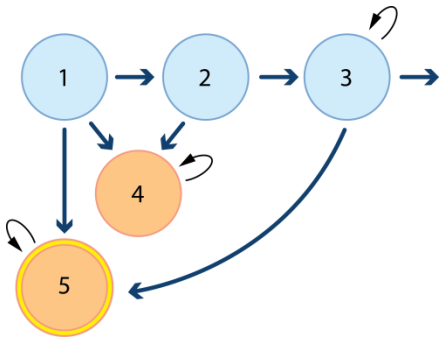

Рисунок 3.20 – Граф состояний укрупненной вероятностной модели аутентификации

Состояния системы 3–5 представим в виде поглощающих состояний [35]. Вероятность переходов из одного состояния в другое обозначим следующим образом:

p_{12} – вероятность перехода из состояния 1 (регистрация) в состояние 2 (подтверждение подлинности предъявленных идентификаторов);

p_{14} – вероятность перехода из состояния 1 в состояние 4 (отказ);

p_{15} – вероятность перехода из состояния 1 в состояние 5 (опасный отказ);

p_{23} – вероятность перехода из состояния 2 в состояние 3 (принятие решения);

p_{24} – вероятность перехода из состояния 2 в отказ;

p_{33} – вероятность поглощения в состоянии 3; заметим, что $p_{33} \neq 1$;

p_{35} – вероятность перехода из состояния 3 в состояние опасного отказа;

p_{44} – вероятность поглощения в состоянии отказа, при этом $p_{44} = 1$;

p_{55} – вероятность поглощения в состоянии отказа, при этом $p_{55} = 1$.

Применим к данной модели теорию цепей Маркова. Матрица переходов для такой схемы может быть записана в виде:

	1	2	3	4	5
1	0	ρ_{12}	0	ρ_{14}	ρ_{15}
2	0	0	ρ_{23}	ρ_{24}	0
3	0	0	ρ_{33}	0	ρ_{35}
4	0	0	0	1	0
5	0	0	0	0	1

Приведем полученную матрицу переходных вероятностей к каноническому виду, поставив поглощающие состояния первыми [35]:

$$P = \cdots \begin{pmatrix} I & O \\ R & Q \end{pmatrix} \cdots =$$

	4	5	1	2	3
4	1	0	0	0	0
5	0	0	0	0	0
1	ρ_{14}	ρ_{15}	0	ρ_{12}	0
2	ρ_{24}	0	0	0	ρ_{23}
3	0	ρ_{35}	0	0	ρ_{33}

Фундаментальная матрица будет вычисляться по формуле $N = (I - Q)^{-1}$.

Матрица вероятностей поглощения равна $B = NR$ [35].

3.5.4. Моделирование системы идентификации и аутентификации на третьем уровне

На третьем уровне производится моделирование процедур, составляющих процесс идентификации и аутентификации. Покажем, как можно моделировать отдельные процедуры аутентификации.

Рассмотрим процедуру регистрации, являющуюся наиболее критичной к использованию со стороны злоумышленника. Сформулируем критерий отказа и опасного отказа. Для процедуры регистрации отказом будем считать отсутствие регистрации для легального пользователя, а опасным отказом – регистрацию злоумышленника под именем легального пользователя.

В виде критериев функциональных отказов для рассматриваемой системы можно принять ошибки в работе системы, не приводящие к остановке выполнения основных заданных функций работы системы. Другими словами, ошибки и сбои не должны превышать определенного порога, начиная с которого система удаленной аутентификации может перестать выполнять заданный набор функций.

Сумма вероятностей выходов из каждого состояния есть полная группа несовместных событий:

$$\sum_{i=1}^{n} P_i = 1 \qquad (3.15)$$

где n – число состояний системы.

Для моделирования процедуру регистрации нового пользователя в информационной системе упрощенно можно представить в виде следующих состояний:

1 – претендент на регистрацию послал запрос на сервер ЦР с целью зарегистрироваться в ИС;

2 – идентификаторы претендента пришли на сервер вместе с запросом на регистрацию. С сервера ЦР высылается запрос на подтверждение наличия и

совпадения полученных от претендента идентификаторов в базах, содержащих идентификационные данные граждан;

3 – получены ответы на запрос сервера. Если данные совпали, ЦР создает учетную запись претендента, который стал новым легальным пользователем ИС;

4 – ЦР создал или зарегистрировал аутентификатор нового легального пользователя в соответствии с его учетной записью;

5 – ЦР выдал пользователю электронное удостоверение (например, в виде сертификата ключа проверки подписи) и аутентификатор в случае, когда аутентификатор был создан ЦР.

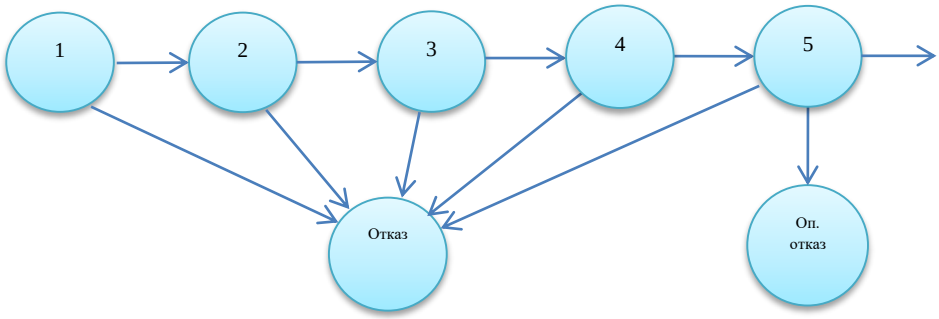

Рисунок 3.21 – Направленный граф состояний процедуры регистрации

В приведенных обозначениях состояний системы процесс регистрации можно представить в виде направленного графа [35, **Ошибка! Закладка не определена.**,217], где состояния системы обозначены цифрами 1–5 (Рисунок).

Определим вероятность работы системы до возникновения первого функционального отказа $P_{Ф0}$:

$$P_{Ф0} = 1 - P_1 + P_1(1 - P_2) + P_1P_2(1 - P_3) + P_1P_2(1 - P_3) + P_1P_2P_3(1 - P_4) + P_1P_2P_3P_4(1 - P_5)$$

где P_1 - вероятность перехода системы из состояния «1» в состояние «2» (это соответствует отсутствию отказов «клиентской» части у претендента при формировании

запроса: при личной явке в ЦР «отказом» может служить отсутствие паспорта или СНИЛС, неурочное время работы, отсутствие персонала в ЦР и т.д.);

P_i - вероятность перехода из состояния «i» в состояние «i + 1», i = 2, 3, 4.

Определим вероятность наступления функционального опасного отказа:

$$P_{Ф0п} = 1 - P_1 + P_1(1 - P_2) + P_1P_2(1 - P_3) + P_1P_2(1 - P_3) + P_1P_2P_3(1 - P_4) + P_1P_2P_3P_4(1 - P_5)$$

Для определения безопасности и надежности процедуры регистрации особенно важно определить параметры вероятности наступления опасного отказа, т.е. регистрации злоумышленника под именем легального пользователя системы.

При моделировании протоколов аутентификации рассмотрим один из наиболее используемых в настоящее время протоколов аутентификации – простейший сетевой протокол аутентификации с применением имени пользователя в качестве идентификатора доступа (*ID* пользователя) и пароля (password) в качестве аутентификационной информации.

Составим схему работы протокола, обозначив состояния системы:

1 – претендент на доступ к системе ввел логин и пароль;

2 – сервер аутентификации принял аутентификационные данные от претендента и переслал их для проверки соответствия в базу данных учетных записей (БДУЗ);

3 – присланные претендентом аутентификационные данные совпали с записями в БДУЗ;

4 – присланные претендентом аутентификационные данные не совпали с записями в БДУЗ;

5 - сервер аутентификации принял положительное решение о прохождении претендентом процедуры аутентификации;

6 - сервер аутентификации принял отрицательное решение о прохождении претендентом процедуры аутентификации;

«Отказ» - состояние отрицательного результата аутентификации для легального пользователя, которое наступает вследствие неверного пароля или логина;

«Опасный отказ» - состояние системы, в котором злоумышленник аутентифицирован под видом легального пользователя.

Состояния системы «претендент – сервер аутентификации» могут быть представлены в виде направленного графа (Рисунок).

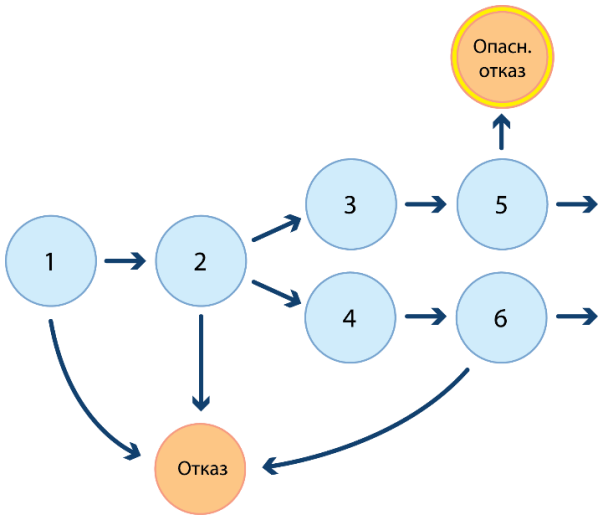

Рисунок 3.22 – Направленный граф состояний парольной аутентификации

По такому же принципу можно построить модели для наиболее часто используемых на практике протоколов аутентификации (Radius, Kerberos, SAML и т.д.).

Реальные значения параметров вероятности P_i лежат в пределах 0,8–1. Для систем аутентификации это означает, что ошибки при вводе аутентификационных данных (в случае парольной защиты) и сбои программного и аппаратного обеспечения могут приводить как к отказам или задержкам по времени, так и к опасным отказам, как правило, с незначительной вероятностью.

3.6 Принципы формирования уровней доверия к методам аутентификации

Традиционным и широко применяемым на западе является так называемый технологический подход к формированию уровней доверия к результатам аутентификации. При этом уровни доверия к аутентификации AAL

(Authentication assurance levels) вводятся априорно в зависимости от применяемого метода аутентификации и предварительно оцененного владельцем ИС уровня рисков. В основе такого подхода лежит уверенность в том, что применяемые в течение многих лет и хорошо исследованные за это время методы аутентификации дадут ожидаемые результаты при условии их аккуратной реализации. Классификация методов аутентификации (на западе – аутентификаторов) предоставляет шкалу доверия, которой пользуются многие страны при проектировании систем аутентификации. Достоинством такого подхода является простота и наглядность формирования уровней доверия - выбор метода аутентификации сразу дает представление об уровне доверия к результатам аутентификации. Самым существенным недостатком такого подхода является неполная прозрачность определения границ уровней доверия не к методу, а именно к результатам аутентификации. Это особенно актуально для самых «доверенных» способов аутентификации, называемых строгой аутентификацией, являющейся многофакторной взаимной аутентификацией с организацией двухстороннего, между субъектом доступа и объектом доступа, или многостороннего (при использовании третьей доверенной стороны) обмена аутентификационной информацией [153]. В процессе строгой аутентификации должны использоваться «сильные» криптографические протоколы аутентификации [28].

Восполним указанный недостаток подходов [1, 2], основываясь на результатах работ [82,**Ошибка! Закладка не определена.**,**Ошибка! Закладка не определена.**], в которых риски аутентификации подробно исследованы. На основе этих исследований в работах [**Ошибка! Закладка не определена.**, **Ошибка! Закладка не определена.**] показано, что в зависимости от способа генерации и хранения аутентификационной информации (для строгой аутентификации это закрытый ключ) уровни доверия к результатам аутентификации могут подразделяться на подуровни. Основным критерием такого подразделения является способ генерации закрытого ключа. Если ключ генерируется

в оперативной памяти компьютера с последующим импортированием в ключевой носитель, уровень доверия к результатам должен быть существенно ниже, чем в случае применения ключевых носителей, способных генерировать ключевой материал внутри специально спроектированного чипа с условием его гарантированной неизвлекаемости. Этот тезис подтверждается тем, что если в первом случае (генерация ключевого материала с помощью программного крипто-сервис-провайдера, называемого CSP – crypto service provider) срок применения закрытого ключа по условиям сертификации ФСБ России ограничен 13 месяцами, то для неизвлекаемых ключей срок применения закрытого ключа составляет три года [218]. Применительно к данной работе это является основанием для введения еще одного уровня доверия к результатам аутентификации в зависимости от используемого аутентификатора. Рассмотрим подробно предложенные в работах [**Ошибка! Закладка не определена.**,219] аутентификаторы.

Аутентификаторы. Под аутентификатором далее будем понимать совокупность характеристик аутентификации: используемого фактора (факторов) аутентификации, способа обмена аутентификационной информацией (односторонний, взаимный), способа генерации, хранения и предъявления аутентификационной информации доверяющей или проверяющей (при ее наличии) стороне, а также применения криптографии. Напомним, что фактором аутентификации называется форма (вид) представления информации. Стандарты выделяют всего 3 фактора:

- фактор знания: субъект доступа должен знать определенную информацию (при аутентификации с применением фактора знания может использоваться как аутентификационная информация, непосредственно известная пользователю, например пароль, графический пароль, изображение, так и информация, позволяющая получить доступ к аутентификационной информации, например, одноразовый пароль или PIN-код);
- фактор владения: субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию (при аутентификации с

применением фактора владения может использоваться, например, устройство аутентификации или механизм, приспособление, которые содержат аутентификационную информацию);

- биометрический фактор: субъекту доступа должен быть свойственен определенный признак (характеристика), информация (данные) о котором (которой) используется при аутентификации.

Предложенные в [**Ошибка! Закладка не определена.**,150] аутентификаторы модернизированы и дополнены автором в соответствии с нормативно-правовой базой и отечественной практикой построения СИА в работе [153]. Результаты работы представлены ниже.

1. **Запоминаемый секрет.** Аутентификатор с запоминаемым секретом – обычно называемый **паролем** или, если это числовое значение, *PIN-кодом* – является секретным значением, предназначенным для выбора и запоминания пользователем. Запоминаемые секреты должны быть достаточно сложными и скрытыми, чтобы нарушителю было невозможно отгадать или иным образом раскрыть правильное секретное значение. Запоминаемый секрет – это фактор **знания**. Рекомендуемая длина запоминаемого секрета должна быть не менее 8 символов, если их выбирает пользователь. Запоминаемые секреты, выбранные случайным образом регистратором, должны быть длиной не менее 6 символов и могут быть полностью числовыми. Если регистратор заносит выбранный запоминаемый секрет, на основе его внешнего вида, в черный список скомпрометированных значений, пользователь должен выбрать другой запоминаемый секрет.
2. **Поисковый секрет (одноразовый пароль).** Аутентификатор с поисковыми секретами (одноразовыми паролями) представляет собой физическую или электронную запись, где хранится совокупность секретов, совместно используемых заявителем и регистратором. Заявитель использует аутентификатор для поиска соответствующего секрета(-ов), необходимого для от-

вета на запрос проверяющей стороны. Примерами поисковых секретов могут являться блокнот шифровальщика, скрэтч-карта. Поисковый секрет – это фактор **владения**.

3. **Внеполосный аутентификатор («второй канал»).** Внеполосный аутентификатор – это физическое устройство, которое является уникально адресуемым и может безопасно взаимодействовать с проверяющей стороной по отдельному каналу связи, называемому вторым (дополнительным) каналом. Заявитель обладает и осуществляет контроль над устройством, которое поддерживает частную связь по этому дополнительному каналу, отделенному от основного канала для электронной аутентификации. Чаще всего в качестве второго канала используется смартфон. Должна жестко ограничиваться продолжительность аутентификации с использованием второго канала. Внеполосный аутентификатор – это фактор **владения**.
4. **Однофакторное OTP-устройство.** Однофакторное OTP-устройство генерирует динамически изменяющиеся пароли (OTP- One Time Password). Эта категория включает отделенные от компьютера аппаратные устройства и программные генераторы динамически изменяющихся паролей, установленные, например, на смартфоне. Эти устройства имеют встроенный секрет, который используется в качестве источника для генерации динамически изменяющихся паролей и не требует активации через второй фактор. Однофакторные OTP устройства аналогичны аутентификаторам с поисковым секретом за исключением того, что секреты криптографическим и независимым способом генерируются аутентификатором и доверяющей стороной и сравниваются доверяющей стороной. Секрет вычисляется на основе одноразового кода, который может быть основан на текущем времени или по событию (например, нажатию кнопки на устройстве OTP), или исходя из счетчика на аутентификаторе и у доверяющей стороны.
5. **Многофакторное OTP устройство.** Многофакторное OTP устройство генерирует динамически изменяющиеся пароли для использования при аутентификации после активации с помощью дополнительного фактора

аутентификации. Сюда включаются аппаратные устройства и программные OTP генераторы, установленные на таких устройствах, как мобильные телефоны. Второй фактор аутентификации может реализовываться с помощью некоей интегральной клавиатуры, интегрального биометрического считывающего устройства (например, отпечатки пальцев) или прямого компьютерного интерфейса (например, USB-порт). Динамически изменяющийся пароль отображается на устройстве и вводится ручным образом для передачи доверяющей стороне. Многофакторное OTP устройство – это фактор **владения**, который активируется посредством использования фактора **знания** или **биометрии**.

6. **Однофакторный криптографический программный аутентификатор.** Представляет собой криптографический ключ, хранящийся на диске или в незащищенной паролем флешке. Аутентификация осуществляется путем подтверждения обладания и контроля над ключом. Выходные данные аутентификатора сильно зависят от конкретного криптографического протокола, но обычно это некий вид подписанного сообщения. Однофакторный программный криптографический аутентификатор – это фактор **владения**.
7. **Однофакторное криптографическое устройство.** Однофакторное криптографическое устройство представляет собой аппаратное устройство, осуществляющее криптографические операции с использованием защищенного(-ых) криптографического(-их) ключа(-ей) и предоставляющее выходные данные аутентификатора через прямое соединение с конечной пользовательской точкой. Устройство использует встроенные симметричные или асимметричные криптографические ключи и не требует активации через второй фактор аутентификации. Аутентификация осуществляется путем подтверждения обладания устройством посредством протокола аутентификации. Выходные данные аутентификатора предоставляются путем прямого соединения с конечной пользовательской точкой и сильно зависят от конкретного криптографического устройства и протокола, но обычно это

некий вид подписанного сообщения. Однофакторное криптографическое устройство – это фактор **владения**.

8. **Многофакторное криптографическое программное обеспечение:** СВТ с криптографическим ПО и второй фактор в виде ключа с доступом к нему по паролю**.** На средстве вычислительной техники должен быть установлено СКЗИ, сертифицированное по требованиям ФСБ России. Многофакторный программный криптографический аутентификатор представляет собой криптографический ключ, хранящийся на диске или каком-либо другой «гибком» носителе, который требует активации посредством второго фактора аутентификации. Аутентификация осуществляется путем подтверждения обладания и контроля над ключом. Выходные данные аутентификатора сильно зависят от конкретного криптографического протокола, обычно это некий вид подписанного сообщения. Многофакторный программный криптографический аутентификатор – это фактор **владения**, который активируется посредством использования фактора **знания** или **биометрии**.

В отличие от западных стран в Российской Федерации де-факто используются ключевые носители двух типов: носители в прямом смысле, в которые импортируются криптографические ключи, сформированные программными криптографическими средствами, и ключевые носители, способные внутри защищенного чипа генерировать ключевой материал. Такой ключ согласно западной терминологии называется Secure Signature Creation Device или коротко SSCD. Поэтому, основываясь на результатах работ [10, 11] вместо одного аутентификатора (как в западных стандартах) предлагается ввести ещё два аутентификатора.

9. **Многофакторное криптографическое программно -аппаратное обеспечение:** СВТ с криптографическим ПО и отдельное от СВТ устройство с импортированным в него ключом, а также доступ к ключу по паролю и/или биометрии СВТ с криптографическим ПО и отделённое от СВТ устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) +

доступ к ключу по паролю. Средство вычислительной техники должно содержать СКЗИ, сертифицированное по требованиям ФСБ России. Устройство для многофакторной аутентификации представляет собой аппаратное устройство, осуществляющее хранение одного или нескольких защищенных криптографических ключей и требующее активации посредством второго фактора аутентификации (например, знание PIN-кода). Устройство для многофакторной аутентификации должно быть сертифицировано по требованиям ФСТЭК России. Аутентификация осуществляется путем подтверждения обладания устройством и контроля над ключом. Многофакторное устройство для хранения ключей – это фактор **владения**, который активируется посредством использования фактора **знания** или **биометрии**.

10. **Многофакторное криптографическое аппаратное обеспечение:** СВТ с криптографическим ПО и отдельное от СВТ устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии. Средство вычислительной техники должно содержать полное или часть СКЗИ, связанную с многофакторным аппаратным криптографическим устройством, сертифицированного по требованиям ФСБ России и способным самостоятельно осуществлять криптографические преобразования для генерации одного или нескольких защищенных криптографических ключевых пар. Таким СКЗИ разрешено использовать закрытый ключ до 3 лет. Для применения закрытого ключа, никогда не покидающего защищенного раздела чипа, требуется активация посредством второго фактора аутентификации (чаще пароль или PIN-код). Иногда дополнительно к этому применяется биометрия. Аутентификация осуществляется при подтверждении обладания устройством и контроля над ключом. Многофакторное криптографическое устройство – это фактор **владения**, для применения неизвлекаемого закрытого ключа используется фактор **знания** и/или **биометрии.**

Результаты рассмотрения аутентификаторов сведены в таблицу 3.10.

Таблица 3.10 - Аутентификаторы и уровни доверия

№	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 импортированным в него ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание 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

В таблице в наглядном виде представлены типовые сочетания видов аутентификационной информации и задач по ее защите, факторов и способов обмена информацией в процессе аутентификации.

3.7 Формирование и оценка уровней доверия к результатам аутентификации

Задача формирования уровней доверия к результатам аутентификации, несмотря на кажущуюся сложность и наличие в большинстве протоколов аутентификации криптографических алгоритмов, гораздо проще, чем аналогичная задача для идентификации, поскольку степень неопределенности однозначного определения субъекта доступа существенно сужается при регистрации. В задаче аутентификации мы имеем дело с зарегистрированным пользователем системы, успешно прошедшим процедуру первичной идентификации (ПИ) по

правилам конкретной ИС (см. главу 2). Как уже упоминалось во введении и первой главе, целью аутентификации в каждой ИС является определение, является ли стремящийся получить доступ субъект тем зарегистрированным пользователем, за кого себя выдает. При этом ключевым словом является «зарегистрированным», то есть после регистрации система аутентификации оперирует только с теми данными, которые остались в ней после регистрации нового пользователя.

Следовательно, формально доверие к процессу аутентификации и его практической реализации не зависит от качества проведения регистрации, но на конечный результат работы СИА качество регистрации и особенно ПИ оказывает весьма существенное влияние. Заметим, что ответ на вопрос связи личности пользователя с его уникальным идентификатором (например, в простейшем случае - логином) и зарегистрированной АИ (в простейшем случае – паролем) определяется выполнением требований конкретной ИС к регистрации нового пользователя. Например, если для регистрации достаточно предъявить копию паспорта, то доверие к этой связи будет практически нулевое, поскольку в копию с помощью современных средств техники легко могут быть внесены изменения в данные, к примеру, может быть заменена фотография. Различные аспекты доверия к результатам аутентификации рассмотрены в работах [220,221,222,223,224,225]. Основываясь на результатах работ [81,155,226,227] можно сделать вывод о том, что составляющими доверия к результатам аутентификации могут быть функциональная надежность и безопасность работы СИА, достоверность результатов ИА и безопасность АИ и идентификационных данных. При этом основным инструментом анализа является оценка рисков. Как показано в работах [223,224], доверие в ИС обратно пропорционально величине рисков. Риски аутентификации подробно рассмотрены в работах [82,**Ошибка! Закладка не определена.**], основанных на анализе применимости методов оценки рисков [82] и предложенных в [**Ошибка! Закладка не определена.**] модели и методики оценки рисков [**Ошибка! Закладка не определена.**]. В качестве основного вывода из рассмотренных 12

вероятных опасных событий в работе [**Ошибка! Закладка не определена.**] установлено два наиболее критичных ВОС для достижения заданного уровня доверия к результатам аутентификации. Первое связано с необходимостью защиты от несанкционированного доступа АИ на протяжении всего жизненного цикла. Второе – с соответствующим (адекватным) выбором метода аутентификации, определяемого сочетанием факторов аутентификации, способов обмена АИ и применяемого протокола обмена претендент – сервер аутентификации.

3.8 Критерии доверия к результатам идентификации и аутентификации

На основе анализа результатов перечисленных выше работ автора можно заключить, что доверие к результатам идентификации и аутентификации складывается из:

- доверия к надежности результатов ПИ при регистрации нового пользователя (характеризующего качество ПИ) - насколько присвоенный уникальный в данной информационной системе идентификатор и соотнесенные с ним идентификационные данные соответствуют субъекту, т.е. насколько достоверно определено, что заявитель является тем субъектом, за кого себя выдает;
- доверия к обеспечению конфиденциальности секрета (аутентифицирующей информации) на протяжении всего его жизненного цикла. Примеры: пароль в случае простой аутентификации или закрытый ключ доступа в случае строгой аутентификации – условия его генерации, хранения, использования, утилизации;
- доверия к корректности реализации методов аутентификации, включающих в себя организацию обмена аутентификационной информации между заявителем и сервером аутентификации (односторонний или взаимный обмен), используемые при этом факторы аутентификации и протоколы обмена. Факторы аутентификации подвержены атакам (пароль –

подбор или перехват, ключевой носитель с секретом можно украсть, биометрию можно эмулировать). Протоколов аутентификации разработано более десяти, планируемый к использованию протокол должен соответствовать заданному уровню доверия к методу аутентификации.

3.9 Оценка доверия к результатам аутентификации

На основании выполненных исследований предлагается метод оценки доверия к результатам аутентификации субъекта доступа в пространстве безразмерных параметров, где обобщенная функция доверия Ψ может быть представлена в виде:

$$\Psi = f\left(\frac{\varphi_{\text{р}}}{R_{\text{р}}}; \frac{\varphi_{\text{кс}}}{R_{\text{кс}}}; \frac{\varphi_{\text{ма}}}{R_{\text{ма}}}\right),$$

где $\varphi_{\text{р}}$ – показатель качества результата регистрации нового субъекта доступа, $\varphi_{\text{кс}}$ – показатель защищенности аутентифицирующей информации (конфиденциальности секрета), $\varphi_{\text{ма}}$ – показатель корректности реализации метода аутентификации, $R_{\text{р}}$ – величина суммарного риска при регистрации, $R_{\text{кс}}$- величина суммарного риска при генерации, хранении, использовании и утилизации конфиденциальности секрета, $R_{\text{ма}}$ - величина суммарного риска при реализации метода аутентификации. Обобщенная функция доверия пока недостаточно исследована. По определению она может изменяться в пределах $0 \leq \Psi \leq 1$. Поясним физический смысл этой функции. Чем ближе получаемая в результате оценок поверхность функции Ψ к границам единичного куба с направляющими, характеризующими показатели качества регистрации, защищенности аутентифицирующей информации и реализации соответствующего метода аутентификации, отнесенными к соответствующим рискам (см.рис.2.9), тем больше может быть уверенность в достоверности, надежности и безопасности полученных результатов аутентификации субъекта доступа.

3.10 Формирование уровней доверия к идентификации и аутентификации

Как было показано в первой главе, международные стандарты рекомендуют введение по крайней мере трех уровней доверия к аутентификации. Напомним, что процесс аутентификации при доступе субъекта доступа к объекту доступа должен включать в себя действия по проверке подлинности субъекта доступа, а также принадлежности субъекту доступа предъявленного идентификатора и аутентификационной информации. Целью аутентификации является формирование необходимой уверенности в том, что субъект (объект) доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за кого себя выдает. При доступе доказательство подлинности субъекта доступа должно основываться на проверке соответствия аутентификационной информации, предъявленной субъектом доступа, с аутентификационной информацией, которая ассоциирована с предъявленным идентификатором доступа у доверяющей стороны. Доказательство принадлежности субъекту идентификатора и аутентификационной информации должно основываться на проверке актуальности (действительности) аутентификационной информации и проверке связи идентификатора и аутентификационной информации с субъектом доступа.

С учетом вышеизложенного методика формирования уровней доверия к результатам аутентификации может быть представлена в наглядной форме в виде таблицы 3.11.

Таблица 3.11 – Принципы формирования уровней доверия к аутентификации

Метод аутентификации субъекта (объекта) доступа			Вид аутентификации субъекта (объекта) доступа	Уверенность в том, что субъект и/или объект доступа действительно является тем субъектом (объектом) доступа, за кого себя выдает	Уровень доверия к результатам аутентификации субъекта (объекта) доступа
Однофакторная	Односторонняя	Соответству-	Простая	Некоторая уверенность	Низкий уровень доверия

аутентификация	аутентификация	ющие протоколы аутентификации, в том числе и криптографические			
Многофакторная аутентификация	Односторонняя или взаимная аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Усиленная	Умеренная уверенность	Средний уровень доверия
Многофакторная аутентификация	Взаимная аутентификация	Криптографические протоколы аутентификации	Строгая	Значительная уверенность	Высокий уровень доверия

В итоге установлено, что доверие к результатам аутентификации определяется достигнутым доверием к первичной идентификации субъекта доступа при регистрации, доверием к обеспечению конфиденциальности секрета (аутентифицирующей информации) на протяжении всего его жизненного цикла, а также доверием к корректности реализации методов аутентификации, включающих в себя организацию обмена аутентификационной информации между заявителем и сервером аутентификации (односторонний или взаимный обмен), используемые при этом факторы аутентификации и протоколы обмена.

Как показано в работе [**Ошибка! Закладка не определена.**], на итоговый уровень доверия существенное влияние оказывает соотношение уровней доверия к результату идентификации и аутентификации (таблица 3.12)

Таблица 3.12 – Соотношение уровней доверия к результатам аутентификации и идентификации

Уровень доверия к результатам аутентификации	Уровень доверия к результатам идентификации		
	низкий уровень доверия к результатам идентификации	средний уровень доверия к результатам идентификации	высокий уровень доверия к результатам идентификации

Низкий уровень доверия к результатам аутентификации	Низкий уровень доверия	Низкий уровень доверия	Низкий уровень доверия
Средний уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Средний уровень доверия
Высокий уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Высокий уровень доверия

Указанные уровни доверия должны согласовываться между собой. Поясним это на простом примере. Если для определенных транзакций применяется строгая взаимная многофакторная аутентификация и используемая аутентификационная информация прекрасно защищена, но регистрация нового пользователя проводится только по копии паспорта, итоговый уровень доверия к результатам ИА практически равен нулю.

Выводы к главе 3

1. 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 систем ИА. 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 должны исследоваться с помощью методов теории массового обслуживания, теории функциональной надежности и безопаности.

2. Рассмотрены основные информационные потоки и участники процессов ИА пользователей при УЭВ, в том числе при переходе к облачным вычислениям, с целью определения методов анализа безопасности и надёжности как самих процессов, так и формируемой, передаваемой, хранимой и обрабатываемой идентификационной и аутентификационной информации. В виде основного инструмента анализа определён анализ рисков с помощью нисходящих и восходящих методов. Сделан вывод о необходимости декомпозиции процедур и процессов аутентификации для уточнения количественных значений рисков. Определены последовательность процедур, составляющих процесс аутентификации, участники электронного взаимодействия и основные информационные потоки в процессах аутентификации с целью их последующего моделирования для анализа рисков и оценки надёжности.

3. Рассмотрены основные современные и перспективные технологии и средства ИА с целью оценки рисков и основанного на анализе рисков уровня доверия к результатам аутентификации. Разработана классификация технологий и средств идентификации и аутентификации по признакам выполнения основных целей, функций и обеспечения безопасности, а также для определения

границ областей применения наиболее развитых технологий аутентификации по критериям цели, задач и степени защищённости электронного взаимодействия при УЭВ, что позволило на базе выполненных классификаций и анализа рисков сформулировать критерии доверия и создать методологию иерархии доверия к результатам аутентификации.

4. Впервые проведен системный анализ рисков аутентификации для многоуровневой модели аутентификации. В виде методической основы анализа взяты рекомендации стандартов серии ГОСТ Р. Выполнен анализ применимости известных методов оценки рисков применительно к процессам идентификации и аутентификации. Показана применимость 17 из 31 рекомендованных стандартом ГОСТ Р 30100 методов для анализа рисков аутентификации. Установлено, что для управления рисками аутентификации применимы 5 методов, показаны их достоинства и недостатки, что позволяет применение рассмотренных методов для практического использования.

5. Усовершенствована общая схема анализа рисков применительно к анализу аутентификации, включающая в себя исследование угроз, уязвимостей, определение вероятных опасных событий и степень последствий их наступления до и после использования контрмер. Усовершенствование состоит в рассмотрении многоуровневых пространств (угроз, уязвимостей, последствий) и применения многоуровневой модели системы идентификации и аутентификации, что позволяет уточнять величину рисков и обосновывать новые подходы к оценке защищённости системы. В частности, применение многоуровневой модели угроз позволяет детализировать влияние компонент СИА по принципу от «общего к частному» на величину остаточных рисков, что способствовало обосновать необходимость введения уровней доверия к результатам первичной идентификации субъекта при регистрации нового пользователя в ИСОП. Установлено, что наиболее критичными являются процессы первичной идентификации субъекта доступа и хранения аутентификационной информации. Проведенный углублённый анализ на втором и третьем уровне детализации

показал, что к наиболее опасным события необходимо также отнести и процедуру предъявления аутентификационной информации. Разработаны методы управления информационной безопасностью процессов аутентификации на основе рассмотренных усовершенствованных методов.

6. На основе анализа рисков впервые сформулированы критерии доверия к результатам аутентификации, что позволило разработать методологию построения уровней доверия к результатам аутентификации в зависимости от достигнутого уровня доверия к результатам первичной идентификации, применяемых методов аутентификации, способа генерации, хранения и предъявления аутентификационной информации и уровней требований информационной безопасности к работе самой системы идентификации и аутентификации, а также защите идентификационных атрибутов, являющихся персональными данными. Предложен метод оценки доверия к результатам аутентификации зарегистрированного субъекта доступа в пространстве безразмерных параметров, разработанный в соответствии с предложенными критериями доверия. На основе выполненного анализа разработана концепция формирования уровней доверия к результатам идентификации и аутентификации, отличающаяся от известных зарубежных аналогов учетом специфики применения сертифицированных средств криптографической защиты информации и средств аутентификации.

7. Для исследования функциональной надежности и безопасности системы идентификации и аутентификации применены известные и разработаны новые математические модели, позволяющие провести оценки безотказной работы СИА. Система многоуровневых моделей для исследования безопасности и надежности систем идентификации и аутентификации на этапах проектирования должна включать модели исследования поведения СИА, описываемых с помощью инструментов СМО. Модели второго уровня детализации системы идентификации и аутентификации, на котором учитываются процедуры, составляющие процесс идентификации и аутентификации, позволяют провести исследования влияния безопасности и надежности выполнения отдельных

процедур и определить их вероятностные характеристики. Модели третьего уровня детализации системы идентификации и аутентификации дают возможность разработать методику оценки влияния отказов и опасных отказов на выполнение критичных процедур.

8. Обоснована необходимость выработки рекомендаций к проектированию, построению и эксплуатации систем идентификации и аутентификации, позволяющих учитывать требования к функциональной надежности и безопасному выполнению процедур аутентификации. На основе рекомендаций необходима модернизация нормативной базы по регулированию указанных процедур.

4 Примеры применения разработанной методологии к решению важных народнохозяйственных задач

4.1 Разработка национальных стандартов по идентификации и аутентификации

В целях сокращения отставания системы национальных стандартов по идентификации и аутентификации по сравнению с международными стандартами, установленного в главе 1 и в наглядной форме представленного на рис. 1.1, в 2016 г. на встрече с руководством ФСТЭК России был представлен и согласован план развития системы национальных стандартов по идентификации и аутентификации. В минимальный план были включены четыре стандарта:

1) ГОСТ Р 58.833 «Идентификация и аутентификация. Общие положения». Настоящий стандарт должен войти в систему стандартов в области защиты информации, определенную ГОСТ Р 52069.0-2013 [228]. Документ уточняет и дополняет положения стандартов [209,229 и 228]. Кроме того, данный стандарта дополняет и уточняет положения нормативных документов ФСТЭК России [230, 231, 232]. Целью стандарта является уточнение национальных стандартов и нормативных документов в части состава, содержания и правил проведения идентификации, а также определяет уровни доверия к ее результатам. В частности, стандарт устанавливает единообразную организацию процессов идентификации и аутентификации в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила применения методов идентификации и аутентификации, обеспечивающих необходимую уверенность в результатах; разработка стандарта началась в январе 2017г., стандарт утвержден согласно приказу Росстандарта от 10 апреля 2020 г. после длительных согласований текста с ТК-26 и ТК-098; в стандарт вошли многие положения диссертационной работы как в части новых терминов и определений, так и в разделы «Основы идентификации» и «Основы аутентификации». Текст стандарта находится на сайте Росстандарта.

2) ГОСТ Р ХХХ.ХХ «Идентификация и аутентификация. Уровни доверия к результатам идентификации». Стандарт базируется на всех перечисленных в п.1) нормативных документах, включая предыдущий стандарт (Идентификация и аутентификация. Общие положения). Объектом стандартизации национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия к результатам идентификации» является процесс идентификации. Аспектами стандартизации национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия к результатам идентификации» являются состав и содержание процесса идентификации, включая состав и содержание необходимой идентификационной информации, а также методы реализации данного процесса и обеспечение доверия к его результатам; по итогам обсуждений внутри ТК-362 сформирована окончательная редакция, которая передана заказчику;
3) ГОСТ Р ХХХ.ХХ «Идентификация и аутентификация. Уровни доверия к результатам аутентификации». Этот стандарт, основанный на предыдущих, будет написан в течение 2020-2021 годов. Объектом стандартизации этого документа является процесс аутентификации. Целью стандарта являются меры по обеспечению доверия к результатам аутентификации.
4) ГОСТ Р ХХХ.ХХ «Идентификация и аутентификация. Управление идентификацией и аутентификацией». Срок подготовки данного документа также 2020-2021 годы, объектом стандартизации является управление идентификацией и аутентификацией субъектов доступа прежде всего внутри корпоративной сети организации, при этом целью стандарта является система доверия к результатам обоих процессов применительно к управлению доступом пользователей. В связи с развитием цифровизации отраслей экономики в стандарте будут затронуты проблемы доверия к пе-

редаче результатов идентификации и аутентификации от одной информационной системы к другой.

Место перечисленных стандартов в системе нормативно - правовой информации представлено на рис.4.1.

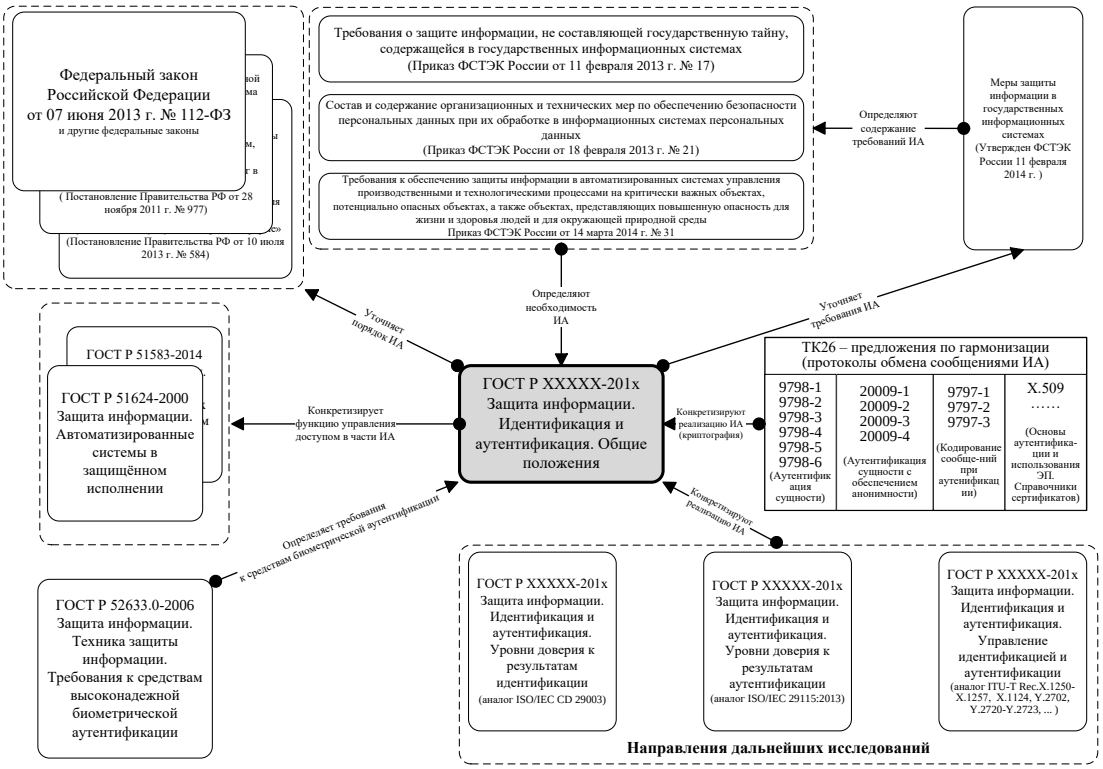

Рисунок 4.1 – место разрабатываемых стандартов в системе нормативно-правовой информации по теме идентификация и аутентификация

Тексты ГОСТ Р ХХХ.ХХ «Идентификация и аутентификация. Уровни доверия к идентификации» и последующих стандартов согласно правилам Росстандарта будут публиковать только после их утверждения.

Для согласования разрабатываемого в 2020-2021 гг. стандарта «ровни доверия к результатам аутентификации совместным решением ТК 362 и ТК 26 создана временная рабочая группа.

В соответствии с официальной просьбой ТК-22 коллективом под руководством автора одновременно разрабатывается еще 5 проектов стандартов по тематике идентификации, аутентификации и защиты персональных данных.

4.2 Примеры внедрений положений диссертационной работы в практику построения и модернизации систем идентификации и аутентификации в организациях различных сегментов экономики

Самым первым и до момента написания диссертационной работы самым крупным внедрением является Пенсионный фонд Российской Федерации (ПФР). В 2005г. ПФР проводил работы по выбору персональных носителей ключевой информации для идентификации и аутентификации при организации доступа сотрудников к информационным ресурсам организации. Специально для ПФР была разработана концепция единого персонального ключевого носителя, в защищенном чипе которого генерируются ключевые пары для доступа и электронной подписи, а также хранятся ключи VPN, ключи шифрования и другая ключевая и идентификационная информация. Обобщение этой концепции на любое предприятие отражено в статье [190], после ПФР были открыты сотни подобных проектов в организациях различных отраслей.

Начиная с 2006 года под руководством автора данной диссертационной работы по заказу Пенсионного фонда Российской Федерации был выполнен ряд государственных контрактов (например, № 09.0298-Д от 12 сентября 2006г., № 09-0493-Д от 26 декабря 2006г., № 09 – 0330-Д от 07 сентября 2007г., № 14-0317-Л от 31 октября 2008г., № 14-245-Д от 13 июля 2009г., № 14-141-Д от 18 мая 2009г., № 23-158-Д от 04 мая 2010г., далее поставки и работы через партнеров, в 2019 г. - через «Ростелеком- Солар» и «Техносерв») на поставку, настройку и услуги по техническому сопровождению средств аутентификации пользователей и программных комплексов централизованного управления индивидуальными ключами пользователей. Внедрение указанных аппаратных и программных средств существенно повысило защищенность информационной системы Пенсионного фонда Российской Федерации и сократило время, затрачиваемое на администрирование доступа пользователей, на 30-35%.

Аналогичными по первичной постановке задачи, но достаточно сложными

и интересными были проекты в Федеральной таможенной службе (ФТС России), макрорегиональном филиале «Дальний Восток» ОАО «Ростелеком», ФГУ «Центр систем мониторинга и связи Рыболовства Российской Федерации», Администрации Ленинградской области, ГНИВЦ ФНС, РУСАЛ, МИАЦ и др., всего 12 внедрений в организации различного подчинения и банки, а также внедрения в учебный процесс 3 вузов по специальности «защита информации». Как правило, внедрение положений диссертационной работы снижает время на администрирование системы управления доступом, как минимум, на 30%.

Как специалиста по идентификации и аутентификации, автора данной работы нередко привлекают к научно-исследовательским работам в качестве исполнителя (соисполнителя) или эксперта, поскольку в связи с развитием цифровизации экономики задача организации защищенного доступа к информационным ресурсам встречается все чаще. В качестве примеров можно привести работы по проекту Министерства образования и науки 14.577.21.0172 от 01.11.2015 г., по заказу ФСТЭК России (3 НИР в течение 2016-2020 гг.) и др.

Отдельные положения диссертационной работы использовались при проектировании и производстве средств защиты информации JaCarta SF ГОСТ (подтверждено патентом №2635927), Secret Disk Enterprise, JaCarta Management System, средства криптографической защиты информации «КриптоБД».

4.3 Способы достижения доверия к результатам идентификации и аутентификации

На основе проведенного анализа международных стандартов, исследованных научных работ и результатов диссертационной работы сформулируем способы формирования уровней доверия к результатам идентификации и аутентификации.

В зависимости от уровня рисков операций, производимых пользователем СКПЭП, выделяются следующие способы идентификации:

– упрощенная идентификация. При упрощенной идентификации используются, например, номер мобильного телефона, адрес электронной почты и т.п.;

– стандартная идентификация. При стандартной идентификации могут рассматриваться СКПЭП, выданный недоверенным УЦ, или данные, представленные при личной явке заявителя для регистрации. Личная явка заявителя в центр регистрации, в отличие от скана паспорта, высланного по электронной почте, может значительно повысить достоверность идентификации путем проверки ИНН и СНИЛС, а также сличения фотографии в паспорте с личностью предъявителя;

– усиленная идентификация. Проверки паспорта на подлинность с помощью процедур, принятых в ряде финансовых и федеральных органах власти, могут повысить доверие к идентификации. Также возможна видеозапись сдачи биометрических характеристик, что снижает риск отказа от регистрации и существенно повышает доверие к степени связанности электронных идентификационных данных с личностью субъекта доступа.

Следует учитывать, что доверие к идентификации личности при первичном обращении заявителя зависит от следующего:

– основным критерием выполнения требований доверия должно являться качество идентификации – отличие одного субъекта от другого, достигается путем верификации всех предъявленных идентификационных атрибутов с занесенными в государственные базы данных для проверки их уникальности и существования (в базах данных государственных органов), а также проверки связи предъявленной совокупности идентификационных атрибутов с личностью субъекта;

– необходимо введение уровней доверия от достигнутой степени связи идентификационной информации с конкретной личностью;

– для БИС требуется введение уровней доверия к результатам идентификации в зависимости от числа подтвержденных идентификаторов и, главное, от

надежности и безопасности механизмов сравнения,

– необходим учет ошибок идентификации, поскольку в процессе идентификации могут возникать ошибки первого (злоумышленник идентифицирован как легальный пользователь) и второго (легальный пользователь не идентифицирован) рода;

– требуется протоколирование результатов подтверждения предъявленных идентификаторов с находящимися в государственных базах данных при возникновении конфликтных ситуаций. При этом указанные официальные подтверждения должны быть соответствующим образом оформлены – должны содержать усиленную квалифицированную подпись и метку времени;

– при отсутствии официальных подтверждений совпадения предъявленных идентификаторов с находящимися в государственных базах данных должны быть собраны необходимые подтверждающие свидетельства из источников, вызывающих доверие [**Ошибка! Закладка не определена.**].

В итоге при предъявлении идентификационных атрибутов (адрес электронной почты, номер телефона, паспорт, СНИЛС и т.д.) достоверность первичной идентификации в результате верификации предъявленных идентификационных атрибутов может накапливаться, и в ряде случаев приближаться к единичному значению. Качественно в наглядной форме этот процесс можно представить в виде графика, изображенного на рис.4.2

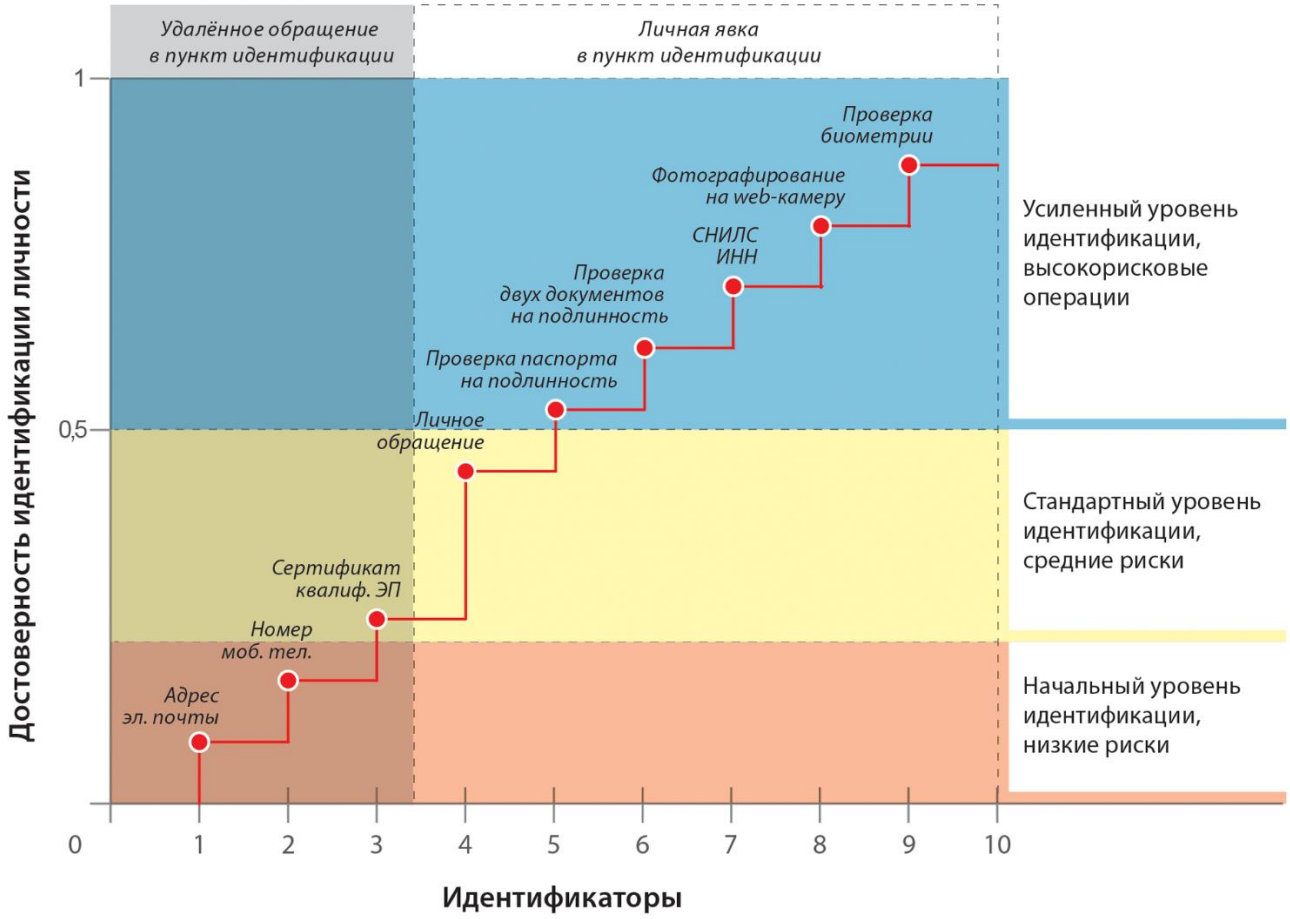

Рисунок 4.2 – Изменение достоверности первичной идентификации

Для конкретной ИС в зависимости от требований к процессу регистрации и выполнения требований величина достоверности может иметь другие параметры, и представленная на рисунке качественная картина может существенно меняться. Например, корректная профессиональная проверка паспорта на подлинность с применением необходимого оборудования и получение официального свидетельства от уполномоченного сотрудника МВД может существенно повысить достоверность идентификации субъекта.

Предлагаемые в [**Ошибка! Закладка не определена.**] уровни идентификации и аутентификации также могут быть разбиты на подуровни доверия к результатам в зависимости от используемых технологий и механизмов аутентификации. Они, по сути, тоже связаны с рисками авторизации злоумышленника под именем легального пользователя. Пример оценки достоверности идентификации

в терминах такого обобщенного подхода приведены выше (Рисунок 4.3). Поясним некоторые точки, изображенные на рисунке.

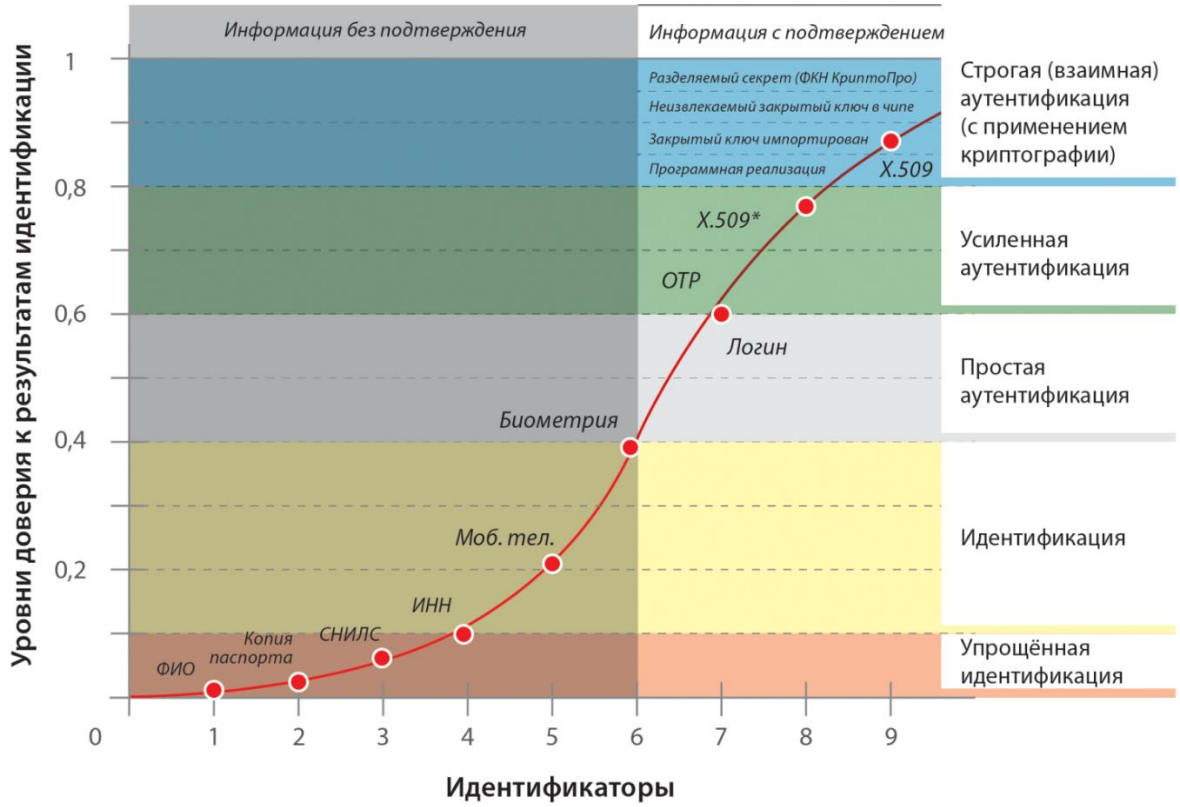

Рисунок 4.3 – Уровни идентификации и аутентификации личности

Так, предоставление паспортных данных в удаленном режиме (например, в виде скана второй и третьей страниц паспорта) может служить основанием для проведения упрощенной идентификации в терминах 115-ФЗ [**Ошибка! Закладка не определена.**]. Заметим, что предъявление не скана, а самого паспорта при личной явке и проверка его подлинности, описанная выше, существенно повышает уровень идентификации (**Ошибка! Источник ссылки не найден.**). Если при проверке паспорта уполномоченным представителем центра регистрации (задавались бы вопросы, на которые может знать ответ только его владелец (например, ФИО и дата рождения родственника), это являлось бы аутентификацией владельца паспорта.

Следующей интересной точкой (Рисунок 4.3) является предоставление заявителем его биометрической информации. Достоверность идентификации в таких случаях зависит от механизма и технологий, используемых в ее процессе, и их практической реализации. Часто это сильно снижает нативную точность используемого метода. Например, при нативной точности метода анализа ДНК, оцениваемого как 10^{-8}, средняя точность идентификации личности путем поиска и экспертного анализа сопоставляемых образцов в базе данных из 10 млн. образцов составляет всего 0,036% [173]. Биометрические данные заявителя в дальнейшем могут использоваться не только для его идентификации, но, в частности, для разблокирования токена, содержащего ключевой материал для сертификатов доступа и СКПЭП.

Рассмотрим самую верхнюю точку, помеченную знаком X.509* (Рисунок 4.3). Она отличается от точки X.509 тем, что в данном случае применяется устройство безопасной генерации ключей подписи SSCD (Secure Signature Creation Device) с неизвлекаемым закрытым ключом [218]. Достоверность идентификации и аутентификации владельца такого устройства выше, чем в случае применения устройств для хранения ключевых контейнеров (точка X.509), где существует отличная от нуля вероятность подмены ключевого материала (например, не взведен флаг «неэкспортируемость»).

Сформулируем промежуточные выводы:

- в отсутствие видеозаписи сдачи биометрических характеристик и предъявления идентификационных атрибутов в процессе регистрации только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и наиболее достоверная аутентификация основана на цифровом сертификате доступа. При этом самым надежным устройством является устройство класса SSCD с неизвлекаемыми закрытыми ключами;
- основными критериями качества аутентификации являются безопасность и надежность;

- существует необходимость определения уровней доверия к аутентификации.

Для государственных ИС минимально необходимым является введение как минимум трех уровней доверия к результатам аутентификации субъектов доступа в зависимости от применяемых технологий аутентификации [**Ошибка! Закладка не определена.**].

В работе [**Ошибка! Закладка не определена.**] показано, что по аналогии с тремя видами ЭП вводятся три типа аутентификации (Таблица 4.3).

Таблица 4.3 – Типы аутентификации в зависимости от видов ЭП

Типы аутентификации	Виды ЭП		
	Простая	Усиленная	Строгая
Простая	+	-	-
Усиленная	+	+	-
Строгая	+	+	+

При этом типы аутентификации могут определяться основными технологиями, т.е. видами учетных записей в БДУЗ и уровнем защиты от подбора или копирования секрета – аутентификатора, с помощью которого подтверждается подлинность идентификатора и доказывается принадлежность идентификатора и аутентификатора конкретному объекту (Таблица 4.4).

Таблица 4.4 – Типы аутентификации в зависимости от видов учетных записей и применяемых аутентификаторов

Учетная запись пользователя	Секрет (аутентификатор)	Уровень строгости (тип аутентификации)
Имя пользователя	Пароль	1.Простая
Имя пользователя	OTP (one-time password, одноразовый пароль)	2.Усиленная

Заданные поля цифрового сертификата X.509 доступа, выданного доверенным для данной ИС УЦ	Закрытый ключ	3.Строгая

Для предложенных трех уровней строгости аутентификации в дополнение к таблицам 4.3 и 4.4. можно привести соответствующие аутентификаторы, лежащие в основе системы аутентификации (Таблица 4.5).

Таблица 4.5 – Типы аутентификаторов, которые можно использовать на различных уровнях строгости

Тип аутентификатора	Уровень 1	Уровень 2	Уровень 3
Аппаратный криптографический аутентификатор	√	√	√
Устройство одноразовых паролей	√	√	
Программный криптографический аутентификатор	√	√	
Пароли и PIN-коды	√		

На основе предложенного подхода можно выделить требования к взаимодействию основных групп участников. Например, гражданин при запросе государственной услуги со своего уровня 1 может аутентифицироваться и пользоваться своей простой подписью, а уполномоченный сотрудник госоргана при ответах на запросы граждан будет скреплять ответ своей квалифицированной подписью, при этом подлинность автора и валидность подписи можно легко проверить. Для основных групп участников электронного взаимодействия соответствие уровней строгости аутентификации представлено ниже (Таблица 4.6).

Таблица 4.6 – Соответствие уровней строгости аутентификации группам участников электронного взаимодействия

Участники электронного взаимодействия	Уровень 1	Уровень 2	Уровень 3
Граждане	√	√	√
Сотрудники негосударственных предприятий и организаций		√	√
Сотрудники государственных предприятий и учреждений			√

Также можно рассмотреть и требования к уровням строгости аутентификации при доступе на информационные ресурсы. Например, для доступа на информационный ресурс организации (к комплексной информационной системе – КИС) организации гражданину надо «играть по правилам» данной организации и получить легальное ЭУ, а также предъявить принятый для данной организации аутентификатор. Возможные комбинации требований к уровню строгости аутентификации для основных участников электронного взаимодействия для данной задачи представлены ниже (Таблица 4.6).

Таблица 4.7 – Рекомендуемое соответствие уровней строгости аутентификации группам участников электронного взаимодействия при доступе в ИС

Участники электронного взаимодействия/ИС	Граждане	КИС	ГИС
Граждане	1	2	3
Сотрудники негосудартственных предприятий и организаций	1-2	2	3
Сотрудники государственных предприятий и учреждений	1-3	2-3	3

Основные защитные меры для различных уровней строгости аутентификации представлены ниже (Таблица 4.8).

Таблица 4.8 – Защитные меры для удаленного доступа через открытые сети связи

Защита от:	Уровень 1	Уровень 2	Уровень 3
Угадывания	√	√	√
Воспроизведения (повтор)		√	√

Перехвата		√	√
Имитации проверяющей стороны			√
Атак класса «Человек посередине»			√

4.4 Юридическая сила и юридическая значимость электронных документов

Поскольку в законах и нормативных актах вопросы юридической силы (ЮС) и юридической значимости (ЮЗ) применительно к ЭД пока не имеют согласованной трактовки и однозначного толкования, рассмотрим их подробнее. Термин "юридическая сила" в теории права применительно к традиционным документам на твердом носителе рассматривается только в отношении нормативных актов. Российская система нормативных правовых актов представляет собой иерархию законных и подзаконных актов: Конституция - Основной Закон, имеющий высшую юридическую силу; затем в порядке убывания - конституционные законы; законы (акты законные), акты Президента; акты Правительства; нормативные правовые акты министерств и ведомств (подзаконные акты); НПА субъектов РФ и органов местного самоуправления. ЮС актов применения права основывается на властной компетенции правоприменяющих органов, иных субъектов, их правовом статусе и полномочиях. ЮС акта зависит от положения органа, издавшего этот акт, в системе органов государства и его компетенции. Акты вышестоящих органов, таким образом, обладают большей ЮС по отношению к актам нижестоящих органов. Акты нижестоящих государственных органов должны соответствовать актам вышестоящих органов и не могут им противоречить. Правоприменительные акты обладают более высокой юридической силой, чем индивидуальные акты реализации и применения права. Отсюда их

особая роль в правовом регулировании. ЮС придает правоприменительным актам способность властно порождать определенные правовые последствия, вызывать возникновение, изменение или прекращение правоотношений [233]. Таким образом, применительно к электронным документам (ЭД) можно обобщить определение ЮС как свойство электронного документа, обусловленное действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления, порождать правовые последствия. Юридическая сила ЭД может быть обеспечена комплексом нормативно правовых, организационных и технических мер. Юридическую силу электронному документу придают:

- обязательные реквизиты;
- идентификация издателя и автора подписи;
- подтверждение полномочий автора электронной подписи;
- подлинность и аутентичность документа.

Рассмотрим, что подразумевается под ЮЗ ЭД и как она соотносится с ЮС. Термин "юридическая значимость" применительно к ЭД появился благодаря развитию информационных технологий и появлению электронного документооборота (ЭДО). Юридическая значимость позволяет судить о ЮС ЭД, но не является доказательством того, что ЭД действительно имеет ЮС. Дело в том, что ЮЗ относится к форме электронного документа, но не к его содержанию. Например, ЭД может быть зафиксирован системой ЮЗ ЭДО и иметь в ней официальное хождение, но не обладать ЮС в силу наличия каких-либо недостатков, скажем, отсутствию ЭП. Таким образом, это совершенно разные понятия и ЮС ≠ ЮЗ.

Прежде чем рассматривать доверенные сервисы УЦ, отвечающие требованиям обеспечения ЮС, определим общие требования к ЭД.

Общие требования к электронному документу

С юридической точки зрения документ – один из самых распространенных способов фиксации правовых отношений. Согласно Федеральному закону "О техническом регулировании" выполнение стандартов не является обязательным.

Тем не менее, развитие информатизации принуждает разработчиков и пользователей все чаще обращаться к стандартам для обеспечения интероперабельности и совместимости различных ИС. Так, ГОСТ Р ИСО 15489-1-2007 устанавливает требования к электронным документам. Стандарт устанавливает (раздел 7, пп. 7.2.1-7.2.5), что принципы политики, процедуры и практика управления документами должны обеспечивать создание подлинных документов, обладающих определенными характеристиками, а именно: аутентичность, целостность, достоверность, пригодность для использования.

Рассмотрим эти характеристики и какими сервисами безопасности они могут быть обеспечены более подробно.

По ГОСТ Р ИСО 15489-1-2007 документ является аутентичным, если он соответствует установленным правилам, был создан или отправлен лицом, уполномоченным на это, был создан или отправлен в то время, которое обозначено в документе. При электронном взаимодействии аутентичность обеспечивается следующими сервисами безопасности:

"соответствует установленным правилам" - в подавляющем числе случаев это принадлежность к конкретной системе ЭДО, системе документооборота органа власти, имеющего право издания документа или подчинение установленным требованиям к определенным видам документов для индивидуальных актов (правила составления договора, доверенности и т.д.);

"был создан или отправлен лицом, уполномоченным на это" – для обеспечения этого условия требуется, как минимум, три сервиса безопасности - аутентификация, ЭП и реестр полномочий, поддерживаемый в актуальном состоянии;

" был создан или отправлен в то время, которое обозначено в документе" – обеспечивается применением сервиса доверенного времени.

Достоверным является документ, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или

фактов и которому можно доверять в последующих операциях или в последующей деятельности. Для ЭД достоверность может опосредованно определяться статусом организации, издавшей документ, идентификацией этой организации, а также автора документа.

Целостность документа определяется его полнотой и неизменностью. Обеспечивается применением электронной подписи.

Пригодным для использования является документ, который можно найти (имеется в виду - в информационной системе), воспроизвести и интерпретировать. При воспроизведении должны сохраняться связи между документами, фиксирующие последовательность действий, связи с деловой деятельностью или операциями, в которых эти документы были созданы и применялись.

Рассмотрев общие требования к ЭД, перейдем к анализу сервисов безопасности, доверенное состояние которых должно обеспечиваться УЦ для придания ЮС ЭД.

Доверенные сервисы, обеспечивающие юридическую силу электронному документу

Выше показано, что электронные реквизиты являются необходимым условием наличия ЮС у ЭД. При определении электронных реквизитов, необходимых для придания ЮС электронному документу, надо учитывать ряд особенностей.

Так, в Рекомендациях Европейской экономической комиссии ООН в отношении функциональной совместимости подписанных электронных документов подчеркивается, что между цифровыми и бумажными документами много общего, но есть и ряд важных различий, в частности, «подписанные бумажные документы, как правило, содержат собственноручную подпись подписанта, тогда как цифровая подпись под электронным документом не имеет графической формы. Обычно только компьютерная программа способна произвести сложные математические расчеты, необходимые для проверки цифровой подписи».

Правовой режим электронной подписи у нас в стране установлен Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», в ст. 6 которого определены условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью. Эти условия различаются в зависимости от того, какой электронной подписью подписан документ, и состоят в следующем:

«1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

2. Информация в электронной форме, подписанная простой ЭП или неквалифицированной ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи...».

Кроме того, этим законом (ст. 11) установлен порядок признания квалифицированной электронной подписи, который включает ряд условий, одним из которых является положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с

помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания.

Из приведенных положений закона вытекает, что возможность использования для подписания электронных документов того или иного вида ЭП должна быть установлена нормативными правовыми актами или соглашением сторон (в случае использования неквалифицированной или простой электронной подписи), а при получении ЭД, подписанного ЭП, обязательна процедура проверки, которая должна подтвердить (или не подтвердить) принадлежность владельцу квалифицированного сертификата квалифицированной электронной подписи и отсутствие искажений в подписанном ЭД.

В этом месте начинаются особенности, обусловленные используемыми технологиями, применяемыми при переходе к электронному взаимодействию. Принадлежность владельцу сертификата КЭП отражается в сертификате, который связывает идентификационные данные владельца, секрет, с помощью которого он подтверждает подлинность идентификационных данных (или о наличии которого должен знать УЦ – это случай ключевого материала, открытый ключ известен УЦ, значит, у владельца сертификата имеется соответствующий закрытый ключ, который он согласно ст.10 закона должен хранить в тайне) и саму личность владельца сертификата, которая при первичном обращении в УЦ называется заявителем.

Обратившись к ст.18 закона, читаем: " При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

1) установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

2) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата".

Таким образом, в обязанность аккредитованного УЦ входит установление

личности заявителя, т.е. его идентификация. К сожалению, в Положении и правилах аккредитации УЦ, разработанные Минкомсвязи России, требований о регламенте проверки предъявленных заявителем идентификаторов и правил, гарантирующих достоверность идентификации личности заявителя, не предусмотрено.

Таким образом, корректность решения обратной задачи определения принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи зависит от корректности решения задачи первичной идентификации заявителя при обращении в УЦ за получением сертификата КЭП.

ЭП – уникальный сервис безопасности, который одновременно выполняет функции обеспечения целостности подписанной информации, аутентификации источника данных и неотрекаемости того, кто подписал эту информацию. Применение подписи для обеспечения целостности гарантирует, что все изменения в передаваемых данных будут обнаружены независимо от того, чем они вызваны ошибками при передаче или целенаправленным воздействием противника в канале. Под аутентификацией источника данных обычно понимают возможность передачи подписанного сообщения с последующей отложенной проверкой подписи. Неотрекаемость (невозможность отрицания) является более сложным сервисом, поэтому технологические решения в виде ЭП должны дополняться нормативными требованиями и обязательной предварительной аутентификацией подписанта. Кроме основных перечисленных сервисов безопасности ЭП часто (например, в электронных торгах) используется для идентификации владельца по определенным полям сертификата ключа проверки подписи.

Между обычной (собственноручной) и электронной подписями имеются существенные различия (Таблица 4.9)

Таблица 4.9 – Сравнение цифровой и собственноручной подписи [29]

Собственноручная подпись	Электронная подпись

Не зависит от подписываемого текста, всегда одинакова	Зависит от подписываемого текста, разная для различных текстов
Неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	Определяется секретным ключом, принадлежащим подписывающему лицу, который может быть утерян владельцем
Неотделима от носителя (бумаги), поэтому отдельно подписывается каждый экземпляр документа	Легко отделима от документа, поэтому верна для всех его копий
Не требует для реализации дополнительных механизмов	Требует дополнительных механизмов, реализующих алгоритмы её вычисления и проверки
Не требует создания поддерживающей инфраструктуры	Требует создания доверенной инфраструктуры сертификатов открытых ключей
Не имеет срока давности	Имеет ограничения по сроку действия (для владельца сертификата КЭП – 1 или 3 года)

Надёжность схемы ЭП оценивается сложностью решения следующих задач:

подделка подписи, то есть нахождение значения подписи под заданным документом лицом, не являющимся владельцем секретного ключа;

подделка документа, то есть модификации подписанного сообщения без знания секретного ключа;

подмена сообщения, то есть подбор двух различных сообщений с одинаковыми значениями подписи без знания секретного ключа;

генерация подписанного сообщения, то есть нахождение хотя бы одного сообщения с правильным значением подписи без знания секретного ключа.

Защита от данных атак обеспечивается выбором схемы электронной подписи, обладающей соответствующими криптографическими свойствами.

Согласно [72] разрешено использовать простую, усиленную и усиленную квалифицированную подписи. Сначала напомним, как различаются эти виды ЭП.

Простая ЭП. Согласно [72] «простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт создания электронной подписи определённым лицом». Такое определение не вносит ясности в понимание того, чем может являться простая электронная подпись и какие технологии допустимы для её реализации, тем более что все последующие уточнения касаются только квалифицированной подписи. В западном законодательстве введение понятия простой подписи было обусловлено её широким использованием на ранних этапах развития технологий. Применение простой ЭП не обеспечивают выполнения свойств невозможности отрицания, а в отдельных случаях и обеспечения целостности документов. Формального определения простой электронной подписи не существует. Можно обсуждать условия существования простой ЭП путем логического перебора возможных ситуаций, приводящих к нарушению имеющегося формального определения квалифицированной подписи. Множество подписей, которые не являются квалифицированными и поэтому не могут быть признаны равнозначными собственноручной подписи, распадается на два класса: усиленные и не являющиеся усиленными (в [72] они названы «простыми»). Такой подход к определению (через отрицание) предполагает, что к этим классам можно отнести те электронные подписи, которые хотя и имеют электронную форму, но не удовлетворяют основным условиям КЭП, то есть для них не выполнено хотя бы одно из условий определения квалифицированной подписи. Заметим, что простая подпись обеспечивает только один сервис безопасности из вышеперечисленных – аутентификацию, и ту с определенной (как правило, недостаточной) степенью надежности.

Усиленная ЭП. Согласно Директиве [205], усиленная электронная подпись должна удовлетворять следующим требованиям:

ЭП однозначно связана с лицом, подписавшим данные;

с её помощью можно подтвердить подлинность лица, подписавшего данные;

ЭП создана с использованием средств, которые находятся под единоличным контролем лица, подписавшего данные;

ЭП связана с данными, которым она соответствует, таким способом, что с её помощью можно обнаружить любые последующие изменения подписанных данных.

Таким образом, здесь говорится о выполнении свойств однозначной аутентификации источника и обеспечения целостности. Как известно, эти свойства могут быть обеспечены только применением схемы ЭП. При этом согласно №63-ФЗ подпись может использовать неквалифицированный сертификат. Например, это может быть ЭП, сертификат которой сформирован и поддерживается УЦ, не аккредитованным Минкомсвязи России.

Квалифицированная ЭП. На основе анализа законов, принятых в различных странах мира, в [205] закреплены наиболее существенные моменты. Они сформулированы в ст. 5: необходимо использовать усиленную электронную подпись, которая должна быть основана на квалифицированном сертификате и сформирована с помощью защищённого устройства создания подписи, так называемого SSCD (Secure Signature Creation Device), что в переводе означает «устройство, генерирующее ключи, в том числе закрытый ключ, внутри защищенного чипа». Последнее до сих пор не узаконено в РФ, хотя в приходящем на смену [205] Регламенте [**Ошибка! Закладка не определена.**] требование применения устройств SSCD для того, чтобы ЭП стала квалифицированной, с 1 июля 2014 г. стало обязательным для всех стран Евросоюза. В №63-ФЗ приводится такое определение понятия квалифицированной электронной подписи: «Квалифицированной ЭП является ЭП, которая соответствует всем признакам неквалифицированной ЭП и двум дополнительным признакам:

ключ проверки электронной подписи указан в квалифицированном сертификате;

для создания и проверки ЭП используются средства подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом».

Как было указано выше, для обеспечения ЮС ЭД должен быть реализован комплекс мероприятий, включающих нормативно-правовые, организационные и технические меры. Рассмотрим технические меры. ЮС ЭД может придать только совокупность применения нескольких доверенных сервисов, в число которых, прежде всего, входит усиленная квалифицированная электронная подпись (КЭП). Одним из достаточно распространенных заблуждений является мнение о том, что применение одной лишь КЭП достаточно для того, чтобы ЭД стал обладать ЮС. Основываясь на результатах работы [234], можно показать, что минимальный набор доверенных сервисов для придания ЮС в электронном документообороте состоит из:

инфраструктуры и доверенных средств генерации, применения и проверки усиленной квалифицированной подписи;

развитой системы проставления меток доверенного времени, синхронизированного в каждом аккредитованном удостоверяющем центре с временем корневого УЦ;

поддерживаемой в актуальном состоянии с заданным интервалом времени (в часах) системы реестров полномочий и правомочий владельцев УКП;

доверенных сервисов идентификации и аутентификации, строго регламентированных для каждого аккредитованного УЦ с регулярным внешним контролем порядка и правил выполнения основных процедур.

Перечислим набор доверенных сервисов, минимально необходимых для обеспечения юридической силы электронного документа.

1) Электронная подпись. Электронная подпись является уникальным сервисом безопасности, вобравшем в себя сразу три доверенных сервиса:

аутентификация источника данных – подтверждение подлинности источника полученных данных (ISO 7498-2);

обеспечение целостности данных, означающее, что данные не были модифицированы или уничтожены неавторизованным образом (ISO 7498-2);

невозможность отрицания авторства – сервис защиты от отрицания автором факта создания или отправления им сообщения (ISO/IEC 13888-1).

2) Сервис аутентификации. Аутентификация при удаленном взаимодействии также является сложным сервисом, состоящем из трех составляющих:

обеспечение доказательства подлинности предъявленного идентификатора (ISO/IEC 10181-2);

доказательство принадлежности аутентификатора, с помощью которого производится доказательство подлинности, конкретному субъекту (ISO/IEC 10181-2);

аутентификация сторон – подтверждение того, что взаимодействующая сторона является той, за которую себя выдает (ISO 7498-2).

3) Сервис доверенного времени. Сервис меток доверенного времени совместно с сервисом штампов времени (RFC 3161 «Time-Stamp Protocol (TSP)») образуют Службу доверенного времени . Суть сервиса состоит в синхронизации серверного времени для всех УЦ, участвующих в формировании и проверки статуса сертификата.

4) Сервис валидации. Сервис валидации (RFC 2459), как правило, входит в состав службы "Заверения электронных сообщений" и может являться дополнительным сервисом в автоматизированной системе, выполняющей функции Удостоверяющего Центра (УЦ). Проверка действительности данных, связанных с подписанным сообщением или документом, а также сертификатов ключей подписи может проводиться по стандартизованному

протоколу Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS) с квитанцией за подписью сервера (RFC 3029). Для проверки статуса сертификата также используется On-line Certificate Status Protocol - OCSP (RFC 2560). Отдельно может проводиться проверка действительности сертификата открытого ключа - Validation of Public Key Certificates (VPKC).

5) Сервис проверки действительности полномочий субъекта на момент подписи. Проще всего поддерживается с помощью атрибутных сертификатов. Также подтверждается квитированием (подписанной сервером квитанцией).
6) Сервис гарантированной доставки документов и/или сообщений.

Перечисленные сервисы могут стать доверенными при условии создания и поддержки соответствующих инфраструктурных решений [235].

4.5 Разработка способа построения решений по защите персональных данных и управления доступом при переходе к облачным вычислениям

В условиях противодействия западным разведкам и методам сбора информации о российских гражданах класса Big Data весьма актуальной становится задача импортозамещения. Проблема заключается в том, что подавляющая часть хранящейся в базах данных информации может быть подвержена передаче противоборствующим сторонам, используя уязвимости, заложенные в системное и прикладное программное обеспечение. Так, наиболее распространенной СУБД, применяемой для хранения и обработки персональных данных граждан России, де-факто является СУБД Oracle. Процесс импортозамещения для перевода данных под более "доверенную" платформу может занимать, как минимум, 3-5 лет. В этих условиях необходимо найти решение задачи, позволяющее снизить риски перемещения критически важных данных за рубеж. Особенно актуальной данная задача становится при переходе к облачным вычислениям, где все предлагаемые

платформы имеют импортное происхождение. К тому же часть серверов, хранящих персональные данные (ПДн), до сих пор находится за рубежом и полностью контролируется западными специалистами.

Для решения данной задачи сначала предлагается метод защиты данных на платформе Oracle, основанный на применении наложенных средств шифрования по ГОСТ 28147-89, используемый без нарушений лицензионных соглашений с импортным поставщиком, но надежно защищающий данные от НСД. В целях разработки предлагаемого метода сначала были исследованы возможности встроенных средств СУБД Oracle [236], затем была разработана общая методология защиты данных [237]. Наиболее существенной частью методологии является безопасная схема распределения ключей шифрования и предоставления защищенного доступа легальным пользователям к защищаемым данным [238]. Разработанный алгоритм управления доступом исключает доступ к конфиденциальным данным администраторов баз данных, существенно снижая риски самого распространенного способа утечки и перекрывая самые используемые средства хищения данных, включая SQL-инъекции. В работе [239] метод был доработан для использования в облачных средах. Рассмотрим метод подробнее.

Предлагаемые провайдерами способы защиты конфиденциальной информации, которая хранится и обрабатывается в "облаках", как правило, основаны на шифровании всего объёма информации (всей базы данных) или различные варианты фрагментации и шифрования. Для задачи обработки персональных данных такое предложение имеет два существенных недостатка. Во-первых, такие подходы подразумевают значительную вычислительную нагрузку на компьютере клиента и серверов в "облаке". Во-вторых, в данных подходах ситуация с разделением ответственности за обеспечение конфиденциальности ПДн между оператором персональных данных и провайдером облачных услуг перед субъектами ПДн становится запутанной не только с юридической точки зрения, но и с

точки зрения организационно - технической. Поскольку обеспечение конфиденциальности, как правило, достигается путем шифрования ПДн, то самым существенным с точки зрения безопасности становится вопрос об управлении ключами шифрования и особенно задача их безопасного распределения.

Предлагается модель, позволяющая решить некоторые наиболее актуальные проблемы обеспечения конфиденциальности информации в "облачных" средах. Основная идея предлагаемого подхода заключается в шифровании минимально необходимой части информации на стороне клиента "облачного" приложения. Предполагая, что клиентская часть находится в защищенной корпоративной сети и является доверенной средой, управление ключами шифрования также отдаётся стороне клиента, а «облачной», т.е. недоверенной среде, остается задача хранения уже безопасных (т.е. не интересных для атак) данных. Такой подход при использовании строгой аутентификации, основанной на применении цифровых сертификатов доступа к данным в облаке и закрытого ключа пользователя в качестве аутентификатора, позволяет существенно снизить риски несанкционированного доступа к конфиденциальной информации при переходе к «облачным» вычислениям.

Несмотря на то, что поставщики услуг "облачных сервисов" берут на себя полную ответственность за управление данными клиента, остаётся проблема доверия к "облакам". Можно ли доверить все вопросы хранения данных, в том числе, шифрование конфиденциальной информации, провайдеру «облачных» услуг? На провайдера и так возлагается слишком много задач. В частности, обеспечение высокой доступности внешних данных не может полностью гарантировать тайну содержания информации (появился даже термин "честный, но любопытный сервер" - honest-but-curious). Помимо известных рисков нарушения конфиденциальности и иных угроз для внешних данных появляется угроза неправомерного использования информации: персонал или кто-либо ещё может извлечь,

перепродать или использовать значительную часть данных в коммерческих целях. Поскольку традиционные (применимые к корпоративной сети) методы управления доступом не могут помешать персоналу "облака" несанкционированно получать данные, их следует шифровать, либо разделять информацию на открытую и конфиденциальную. Немаловажное значение имеет и проблема выполнения запросов по зашифрованным данным [240,241]. Очевидный недостаток большинства существующих решений является то, что поскольку данные шифруются одним ключом шифрования, то остаются вопросы по управлению ключами шифрования, а также их распределения среди пользователей или групп пользователей. Предлагаемый в данной работе подход основан на разделении исходного отношения (набора) данных R на два фрагмента Fc (открытый текст) и Fe (зашифрованный текст). Оба фрагмента хранятся в "облаке" в «недоверенной» среде, вычисление исходного отношения R происходит на «доверенной» стороне клиента с помощью криптографического преобразования алгоритмами A и набора ключей K.

Как правило, информация в «облаках» хранится в базах данных, а для ее обработки используются двухзвенная (клиент - сервер) или трехзвенная (клиент-сервер приложения – сервер хранения данных) архитектура. Предположим, что информация, подлежащая хранению в "облаке", представлена отношением r. При этом r относится к схеме $R(d1,...dn)$, которая для "облака" в общем случае может быть реляционной, либо не являться таковой. Далее будем трактовать r как набор атрибутов в схеме R. Требования безопасности будем представлять как набор ограничений, определенных на единственном или нескольких элементах R.

Определение 1. Пусть $R(d1,...dn)$ есть множество отношений, а ограничение доступа c на R есть подмножество атрибутов множества R.

Иными словами, ограничение доступа есть один или несколько атрибутов, для которых определены по тем или иным критериям требования приватности.

Для единственного атрибута (синглетон - singleton [242]) требование приватности относится к самому значению атрибута. Для нескольких атрибутов (non-singleton) требование приватности выводится, исходя из ассоциаций, позволяющих получить информацию из комбинации значений данных атрибутов. Поясним данное определение на примере. Предположим, имеется некоторый набор данных, представляющий информацию об операциях по карточному счету клиента (отношение) и набор ограничений, которые требуется соблюсти (Таблица 4.1, Таблица 4.2).

Таблица 4.1 – Пример данных карточного счета

ФИО	Адрес	e-mail	Телефон	№ карты	Операция	Сумма
Иванов И.И.	Адр.1-1	i@m.ru	111-1111	1234567890	ОР-1	9000.00
Петров П.П.	Адр.2-3	p@m.ru	222-1111	1234123467	ОР-1920	12000.00
Сидоров С.С.	Адр.3-3	si@m.ru	222-3333	2345123456	ОР-1111	45.50
Сергеев С.П.	Адр.4-1	se@m.ru	111-7777	6789012345	ОР-9902	-1000.00

Таблица 4.2 – Пример ограничений

$c0$	{№ карты}
$c1$	{ФИО,Адрес}
$c2$	{ФИО,Телефон}
$c3$	{Телефон,e-mail}
$c4$	{ФИО,Сумма,Операция}

В приведенном примере:

$c0$ - синглетон, номер карты клиента, который желательно, а иногда даже обязательно, надо скрыть;

$c1$, $c2$ - ассоциативные ограничения, представляющие персональные данные клиента и дополнительную информацию о нем;

$c3$ - ассоциативное ограничение, которое может позволить идентифицировать клиента (косвенный идентификатор);

$c4$ - ассоциативное ограничение, такой набор информации может представлять собой коммерческую тайну.

Выполнение ограничения ci однозначно подразумевает выполнения ограничения cj, такого, что $ci \subseteq cj$. Исходя из этого следует определить набор $C = \{c1, ... cm\}$ хорошо определенных ограничений, таких, что $\forall ci$, $ci \in C$, $i \neq j$, $ci \not\subset cj$.

Целью выведения такого набора ограничений является разделение исходного отношения R на фракции Pc и Pe так, чтобы значения и ассоциации были бы защищены. Здесь Pc - часть отношения, которая может быть передана на хранение в "облако" в открытом виде, а Pe - подлежит зашифрованию на доверенной стороне клиента. Таким образом, ограничения-синглетоны $c = \{d\}$ должны попадать в Pe безусловно, и не появляться ни в каких ограничениях, входящих в Pc даже в качестве ассоциаций. Результирующий набор ограничений $P = \langle Pc, Pe \rangle$ должен соответствовать двум требованиям:

все атрибуты отношения R должны входить как минимум в Pe или Pc для возможности полного восстановления отношения (полнота информации);

по атрибутам, входящим в Pe, невозможно корректно восстановить отношение R на стороне "облака" (конфиденциальность информации).

Из перечисленных требований можно определить корректную фрагментацию отношения R.

Определение 2. Корректной фрагментацией $P = \langle Pc, Pe \rangle$ отношения R и определенных на нем ограничений C, будем считать множество P, для которого выполняются условия

1) $Pe \cup Pc = R$, 2) $\forall c \in C$, $c \not\subseteq Pc$. Условие 1 - полнота - атрибуты отношения R должны находиться в одном из фрагментов, условие 2 - конфиденциальность -

фрагмент, хранящийся в "облаке" не является надмножеством любого ограничения. Для нашего примера можно определить корректную фрагментацию: $P = (\{$Адрес,Операция,Сумма$\},\{$№ карты,ФИО,Телефон,e-mail$\})$. Для минимизации ресурсов, используемых для шифрования на доверенной стороне клиента, следует также минимизировать количество шифруемых атрибутов.

Определение 3. Неизбыточной фрагментацией будем считать фрагментацию $P = (P_c, P_e)$ такую, что $P_c \cap P_e = \emptyset$. Свойство неизбыточности ни в коей мере не нарушает свойства корректности фрагментации. Если любой атрибут d появляется в обоих фрагментах, он может быть удален из P_e без нарушения **Определения 2**: полноту обеспечивает присутствие d в P_c , конфиденциальность также выполняется, т.к. атрибут не нарушает ни одного ограничения. Таким образом, корректная фрагментация отношения всегда может быть сделана неизбыточной путем изъятия атрибутов из P_e.

Предлагаемая методика решения. Определим множество алгоритмов $A = \{a_k \mid k=1,K\}$ и ключей шифрования $K = \{k_m \mid m=1,M\}$ таких, что $\forall ki$, $\exists! aj$, $|A| \le |K|$. Предполагаем также, что каждый ключ k_m генерируется случайным образом. Соответственно определим функцию преобразования f, реализующую алгоритм симметричного шифрования $a \in A$, так, что $\forall d \in P_e$, $k \in K$: $d_{ei} = f(d_i, k_j)$ и $d_i = f(d_{ei}, k_j)$ для $i = 1,M$, $j = 1, |P_e|$. Обозначим множество *пользователей* "облачного" приложения $U=\{u_l \mid l=1,L\}$, $\forall u_l$, $\exists! \{X,Y\}$, где X,Y - открытый (*public*) и личный ключи (*private*) пользователя (ключевая пара пользователя). Определим множество ключей шифрования пользователя $K' = \{k'_{m'} \mid m'=1,M', M' \le M\}$, при этом выполняется условие $k'_{m'} = \varepsilon(k_{m'}, X) \wedge k_{m'} = \varepsilon(k'_{m'}, Y)$, где - функция асимметричного криптографического преобразования.

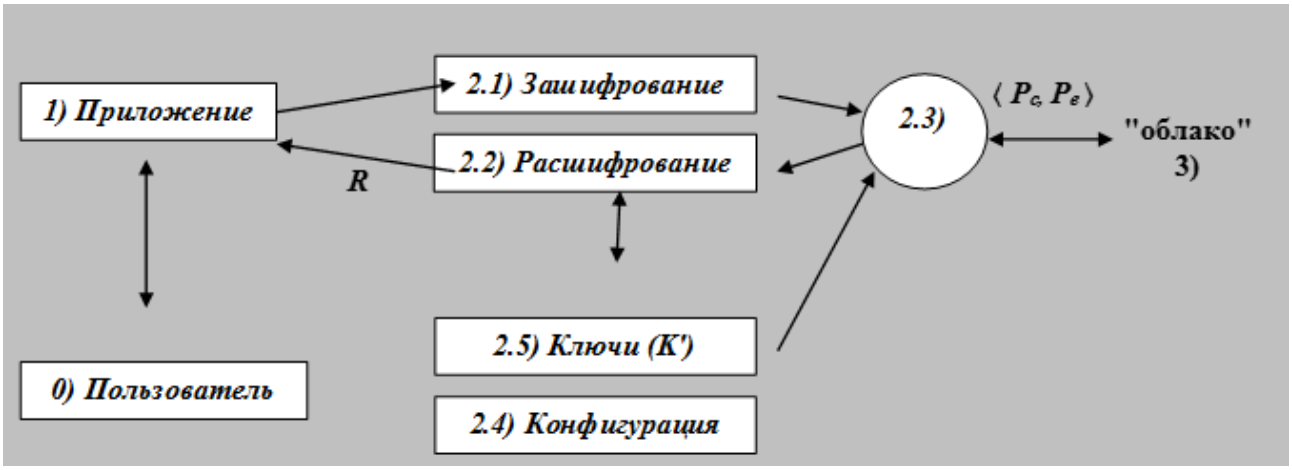

Рисунок 4.4 – Схема решения

Компоненты схемы 0, 1, 2.x - есть доверенная сторона клиента, 3 - недоверенная сторона "облака". Определим, что сети обеих сторон изолированы, доступ разрешен только по протоколам, определенным для облачного приложения. Общая схема функционирования данного решения (не рассматриваем процесс аутентификации и авторизации в "облачном" приложении):

пользователь *0* обращается к приложению *1*, предъявляя открытый ключ *X* в качестве своего идентификатора;

приложение обращается к шифратору *2.x* с запросом на авторизацию пользователя, также передавая *X*;

Шифратор извлекает из хранилища ключей 2.5 набор ключей пользователя *K'* и возвращает приложению *1*;

Приложение запрашивает у пользователя личный ключ *Y* и расшифровывает значения ключей шифрования $k_m' = \varepsilon(k_m', Y)$;

расшифрованные ключи передаются шифратору *2.x* и кэшируются в оперативной памяти процесса;

шифратор обращается в "облако" *3* для работы приложения;

при получении данных, множество P_e идентифицируется на основании анализа тегов данных и расшифровывается $\forall d \in P_e,\ k \in K : d_i = f(d_i, k_j)$;

при отправке данных, множество Pe идентифицируется на основании конфигурации приложения 2.4 и зашифровывается $\forall d \in Pe, k \in K : di = f(di, kj)$;

Упрощенная модель нарушителя. Для данной системы Пользователь - Приложение - Шифратор - "облако" (которое в общем случае является "честным - но - любопытным сервером"), в качестве потенциального нарушителя будем рассматривать технические средства и персонал, обслуживающий "облако". При этом полагаем, что указанный персонал обладает неограниченными (административными) правами доступа как к оборудованию, так и к системному и прикладному ПО "облака". Таким образом, потенциальному нарушителю полностью доступна следующая информация:

$$P = \langle Pc, Pe \rangle$$

Краткий анализ угроз. Для известных угроз нарушения конфиденциальности информации, защищаемой с помощью шифрования, можно выделить основные классы:

- криптоанализ зашифрованных данных;
- атака на ключи шифрования.

Реализацию угрозы 1 считаем ничтожной, принимая во внимание следующие факторы:

- нарушителю неизвестен конкретный алгоритм симметричного шифрования;
- нарушителю неизвестны исходные данные.
- нарушителю неизвестен ключ шифрования. Потенциально нарушитель может попытаться получить набор зашифрованных значений Pe , по набору известных ему значений, путем переноса данных $d \in Pe$ в Pc и отправкой результирующего множества доверенной стороне клиента. Такая атака может быть блокирована проверкой полноты Pe и Pc при обработке процессом 2.3 (рис.4.4);
- нарушителю недоступна среда выполнения шифрования;
- нарушителю недоступно хранилище ключей пользователя.

Угроза 2 может быть реализована как методом полного перебора (*brute force*), так и иными методами, направленными на завладение ключевой парой пользователя и получению доступа к хранилищу ключей пользователя. Однако, реализация данной угрозы также маловероятна, так как:

- при достаточной длине ключа шифрования атака полного перебора на практике нереализуема;
- подбор ключа по "радужным" таблицам и с использованием словаря нереализуем при достаточной длине ключа и случайной природе ключа;
- завладение ключевой парой пользователя и ключами шифрования пользователя маловероятна по причине недоступности среды выполнения шифрования и хранилища ключей по сети. Возможность получения такой информации появляется в случае факта сговора пользователя и нарушителя. Данный вопрос не в настоящей работе не рассматриваем. Однако, значительно снизить риск реализации такой угрозы может применение аппаратных носителей (смарт-карт) для хранения ключевой пары пользователя.

Критерии выбора основных параметров. Провайдеры "облачных" приложений обычно предлагают услуги полного шифрования данных как на уровне устройств хранения, так и на уровне отдельных файлов, например, относящихся к базе данных. Такая технология помимо нерешенных вопросов доверия, управления ключами (см. Введение) добавляет и проблему производительности приложения. Процедуры зашифровывания и расшифровывания данных на уровне диска/файла могут серьезно повысить нагрузку на процессоры "облачных" серверов, что соответственно увеличивает время отклика приложения при обработке персональных данных *Тр*. Как правило в стоимость эксплуатации "облачного" приложения входит и стоимость аренды процессорного времени. Поэтому, несмотря на понимание необходимости защиты ПДн в соответствии с [241] применение шифрования в "облаке" не является приемлемым средством защиты для большинства операторов ПДн, где время и стоимость обработки данных является

весьма критичным для существования бизнеса (типичный пример - операторы связи). Рассматриваемый подход позволяет (с известными ограничениями) устранить данный сдерживающий фактор путём распределения нагрузки при шифровании на несколько компьютеров, находящихся в доверенной сети оператора ПДн.

Далее сформулируем основные в данном случае критерии выбора ключевых параметров:

$$Tp \leq Tmax;$$

$$N_p \leq N_{max};$$

$$A_p \geq A_{min}, \text{ где}$$

T_p –время обработки персональных данных;

T_{max} – максимально допустимое время обработки ПДн, определяемое оператором ПДн;

N_p – количество данных, подлежащих обработке, в т.ч. шифрованию;

N_{max} – максимальное количество данных, определяемое оператором ПДн, подлежащих хранению в "облаке";

A_p – алгоритм, выбранный для зашифровывания данных;

A_{min} – минимально-стойкий алгоритм шифрования с точки зрения обеспечения конфиденциальности данных от возможных атак в соответствии с конкретной моделью нарушителя.

Для оценки влияния данных параметров будем рассматривать алгоритм шифрования ГОСТ28147-89, реализованный на основе способа [238] в прототипе системы, приведенном на рис. 4.4. Алгоритм включает в себя следующие режимы шифрования, описанные в [237]:

ECB - режим простой замены;

ECB-MAC - режим простой замены с выработкой/проверкой имитовставки;

CBC-UKM - режим сцепления блоков с первоначальной диверсификацией

ключа и последующей диверсификацией через каждые 1024 байт исходного текста;

CBC-UKM-MAC - режим сцепления блоков с первоначальной диверсификацией ключа и последующей диверсификацией через каждые 1024 байт исходного текста и выработкой имитовставки.

Время обработки. Приблизительная оценка скорости зашифрования проводилась на ноутбуке следующей конфигурации:

процессор Intel Core 2 Duo T5900 @ 2.2 GHz;

2Гб ОЗУ;

250 Гб НЖМД;

ОС Microsoft Windows 7 SP1 64 bit.

Зашифровывались данные d_i различной длины циклами по 50 000, вычислялось среднее время зашифрования (Таблица 4.3).

Таблица 4.3 – Результаты оценки времени шифрования

| di |, байт	Скорость (vi), Mbit/s	Снижение производительности по сравнению с режимом ECB, %		
	ECB	CBC-UKM	ECB-MAC	CBC-UKM-MAC
8	41.35	22.2	58.6	93.8
64	41.20			
256	41.16			
512	41.04			
1024	40.96			
2048	40.90			
4096	32.77			
8192	36.46			
16384	36.48			
32759	37.49			

Скорость расшифрования для режимов ECB и ECB-MAC приблизительно

равна скорости зашифрования. Для режима CBC производительность расшифрования улучшилась примерно на 35-40%, так как отсутствует операция выработки вектора инициализации (IV), который генерировался при зашифровании с использованием генератора псевдослучайных чисел ОС.

В качестве тестируемого "облачного" приложения использовалось приложение Oracle CRM on Demand. В качестве клиента "облачного" приложения - браузер MS Internet Explorer. Защищались персональные данные клиентов и некоторая дополнительная информация (Таблица 4.4).

Таблица 4.4 – Параметры шифруемых данных

d_i	$\lvert d_i \rvert_{max}$, байт	$\lvert d_i \rvert_{avg}$, байт	Режим шифрования
Фамилия	64	16	ECB-MAC
Имя	64	16	ECB-MAC
Отчество	64	18	ECB-MAC
Домашний адрес	128	72	ECB
Организация	128	54	CBC-UKM
Адрес организации	256	92	CBC-UKM
Телефоны	18	12	ECB-MAC
Дополнительные сведения (произвольные заметки)	512	200	CBC-UKM

где:

d_i - фрагмент данных, передаваемых/получаемых в/из "облака";

$|d_i|_{max}$ - максимально допустимый размер фрагмента d_i. Определяется провайдером приложения;

$|d_i|_{avg}$ - средний размер d_i.

Средний суммарный размер защищаемых данных, отображаемых на странице составил:

табличная форма или отчет (100 строк) - 11400 байт (114 байт на запись) - {Фамилия, Имя, Отчество, Организация, Телефоны};

форма ввода/редактирования - 504 байт {Фамилия, Имя, Отчество, Организация, Домашний адрес, Адрес организации, Телефон1, Телефон2, Телефон3, Дополнительные сведения}.

Суммарное усреднённое время формирования (рендеринга) страницы приложения для указанных форм (отчетов) без применения шифрования (целевой показатель T_{max}) заняло около 1.5-3 секунд.

Суммарное усредненное время увеличения формирования (рендеринга) страницы приложения с применением шифрования фрагмента d_i алгоритмом a_i (t_{avg}^r) можно вычислить по формуле:

$$t_{avg}^r = (\sum | d_i |_{avg} / v_i)/8,\ i = 1,M,$$

где

M - число фрагментов данных формы приложения;

$| d_i |_{avg}$ - средний размер фрагмента данных d_i;

v_i - средняя скорость работы алгоритма a_i.

Для нашего случая:

$t_{avg}^r \approx 0.0007$ секунд для формы ввода и

$t_{avg}^r \approx 0.0056$ секунд для формы(отчета) списка из 100 позиций.

Таким образом можно утверждать, что $t_{avg}^r = o(T_{max})$ и условие $T_p \leq T_{max}$ всегда истинно.

Объём данных. Зашифрование фрагмента данных для последующей передачи в «облако» гарантированно увеличивает размер данного фрагмента по сравнению с исходным. На это влияет ряд факторов:

реализация криптографического алгоритма;

реализация конкретного приложения;

особенности передачи данных при использовании стандартных протоколов.

В зависимости от комбинации данных факторов результирующий размер защищенного набора данных ($|P_e|$) может значительно отличаться от исходного

(до зашифрования) набора. Это оказывает влияние как на требуемое количество дискового пространства, так и на количество сетевого трафика, которые арендуются у провайдера "облака". Для приведённого выше прототипа защищённого приложения величина "утяжеления" данных (Δ_d) выглядит следующим образом:

$$\Delta_d = (\Delta_{alg} + \Delta_{app}) * \Delta_{tr},$$

где Δ_{alg} - количесво байт, зависящее от алгоритма. Применяемые в приложении алгоритмы требуют выравнивания данных до величины, кратной размеру блока (например, 8 байт для ГОСТ28147-89 и 16 байт для AES);

Δ_{app} - количество байт, зависящее от приложения. Например, если с данными передаётся контрольная сумма;

Δ_{tr} - множитель количества байт, которого требует среда передачи данных "облачного" приложения. Практически все приложения так или иначе используют для передачи данных HTTP протокол, который не позволяет передавать данные форм в бинарном представлении. Для передачи таких данных используются различные кодировки, например UUEncode или base64. Рассмотрим далее возможное увеличение объёма данных при зашифровании на примере приложения, приведённого выше. Исходные размеры и применяемые алгоритмы приведены выше (Таблица 4.4). В качестве алгоритма кодирования бинарных данных использовался base64 [242]. Для заданных условий каждый зашифрованный фрагмент данных d_i^e будет иметь следующую структуру (в скобках - длина в байтах):

для режима шифрования ECB:

{Метка доступа (1), код ключа(4), данные ($|d_i|$), дополнение блока(1...8)}.

для режима шифрования CBC:

{ Метка доступа (1), код ключа(4), UKM+IV(16), данные ($|d_i|$), дополнение блока(1...8)}.

где:

метка доступа - тег, специфический для приложения;

код ключа - идентификатор ключа шифрования данного фрагмента (k_i);

UKM+IV - вектор инициализации ключа и вектор инициализации шифрования соответственно.

Таким образом, с учётом максимальной длины заполнения блока:

для режима шифрования ECB:

$$\Delta_{alg} + \Delta_{app} = 13 + /d_i/$$

для режима шифрования CBC:

$$\Delta_{alg} + \Delta_{app} = 29 + /d_i/$$

Для выбранного алгоритма кодирования Δ_{tr} = 4/3.

Зависимость результирующей длины от исходной в приведенных условиях приведена ниже (Таблица 4.5).

Таблица 4.5 – Зависимость результирующей длины данных от исходной

$\|d_i\|$ Байт	Параметры шифрования и результирующее увеличение длины $\|d^e\| / \|d\|$	
	ГОСТ28147-89 в режиме ECB	ГОСТ28147-89 в режиме CBC-UKM
16	2.66	3.75
32	2.00	2.54
64	1.67	1.94
256	1.42	1.48
1024	1.35	1.37
4096	1.33	1.33
16384	1.33	1.33

Для нашего примера:

$|d| = \sum|d_i|$ = 504 байт,

$d^e| = (\sum(13+|d_I^{ECB}|) + \sum (29 + |d_I^{CBC}|))$ * 4/3 = (223 + 433)*4/3 ≈ 875 байт.

Таким образом "утяжеление" данных составит:

Δ_d= (875*100)/504 ≈ 173.6 %.

Преимущества предложенного подхода. Основными преимуществами предлагаемого подхода по сравнению с традиционными методами являются:

кардинальное снижение возможности реализации угроз, характерных для современных криптосистем защиты конфиденциальной информации, в том числе при переходе к облачным вычислениям;

надёжное управление доступом пользователей к зашифрованным данным;

применение строгой аутентификации для доступа к защищаемым данным;

защита конфиденциальной информации с помощью шифрования и хранения ключей шифрования на доверенной стороне клиента;

снятие экспортных и юридических ограничений, накладываемых применением криптографии на стороне "облачных" серверов;

распределение нагрузки (процессорное время, оперативная память) процесса шифрования среди конечных потребителей - "тонких" клиентов.

Представленный способ реализован для защиты данных под управлением различных СУБД. На его основе разработано СКЗИ «Крипто БД», сертифицированное по требованиям ФСБ России по классам КС1, КС2 и КС3 для самых распространенных СУБД:

- Oracle;
- Microsoft SQL Server (только по классам КС1 и КС2);
- PostgresPRO;
- PostgreSQL;
- Tibero.

Клиентское ПО системы работает под управлением операционной системы Microsoft Windows XP/Vista/7/8/10 (32- и 64-бит). Решение достаточно успешно внедряется там, где хранится и обрабатывается критичная к разглашению информация. СКЗИ «КриптоБД» позволяет защищать конфиденциальную информацию, в частности, персональные данные граждан в актах гражданского состояния в рамках АИС ЗАГС ФНС России, во всех нотариальных действиях граждан в Единой информационной системе нотариата России и ряде других систем.

Средство криптографической защиты информации «Крипто БД» обеспечивает надежный контроль и защиту данных от несанкционированного доступа, включая администратора системы управления базами данных (СУБД) и других нарушителей.

Выводы к главе 4

1.Приведенные в главе примеры показывают возможности применения основных положений данной работы к различным теоретическим и практическим задачам.

2.Показано, что глубокий анализ международных стандартов, национальной нормативно-правовой базы и применение положений диссертационной работы предоставляют возможности синтеза стандартов национальной системы ГОСТ Р на уровне лучших мировых образцов. Непосредственное участие автора в разработке системы национальных стандартов по идентификации и аутентификации (ГОСТ Р 58833 «Идентификация и аутентификация. Общие положения» и последующие стандарты в рамках ТК 362 является примером синтеза науки и нормотворчества.

3.Примеры внедрений разработанных и модернизированных в данной работе методов и методик анализа процессов идентификации и аутентификации показывают не только научный, но и прикладной характер данного исследования. Применительно к конкретной информационной системе нередко удается дойти до количественных характеристик рисков идентификации и аутентификации, что позволяет выполнить оценки достоверности и надежности результатов, а также оценить защищенность персональных данных, содержащихся в учетных записях. Разработанная многоуровневая система оценки рисков идентификации и аутентификации предоставляет возможности дойти до необходимого уровня детализации оценок достигнутого уровня доверия, что позволило, например, создать защищенное средство отчуждения и переноса информации JaCarta SF ГОСТ, выполненное с учетом профиля ФСТЭК России к средствам отчуждения информации на съёмных носителях с учетом возможных атак [152] с использованием USB-стек протоколов, классифицированных в работе [243]. Это изделие можно применять в информационных системах, в которых обрабатывается информация,

содержащая сведения, составляющие государственную тайну до степени секретности СС включительно. Участие автора в разработке и создании данного изделия подтверждено патентом №2635927 от 05.09.2016 г. «Компактный аппаратный электронный носитель информации с многоуровневым регулированием доступа к отдельным разделам памяти» (соавтор), который внесен в список «100 лучших изобретений России» за 2017 год.

4.Приведены способы достижения определенных уровней доверия к результатам идентификации и аутентификации, а также разработаны примеры требований к аутентификации определенных групп пользователей при их взаимодействии для достижения указанных уровней доверия. Для государственных информационных систем рекомендуется введение, как минимум, трех уровней доверия. Установлено, что самым безопасным с наиболее достоверными результатами методом аутентификации является строгая аутентификация, основанная на цифровом сертификате доступа. При этом самым надежным и безопасным устройством аутентификации является смарт-карта класса SSCD с неизвлекаемыми закрытыми ключами.

5.Рассмотрена задача обеспечения юридической силы и юридической значимости электронных документов. Показано, что аналогом реквизитов бумажных документов являются сервисы безопасности, применяемые для создания, оформления и подписи электронного документа. Установлено, что минимально необходимым, и достаточным для большинства операций с электронными документами, является следующий набор сервисов безопасности:

- Аутентификация (ISO 29115: 2013, ISO/IEC 10181-2:1996, 9798-3:1998)
- Электронная подпись (ISO 7498-2, 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.

Указанные сервисы безопасности базируются на возможностях инфраструктуры открытых ключей. Использование совокупности указанных сервисов позволит поднять уровень доверия к электронному документу до уровня официальных бумажных документов, что необходимо для развития цифрового общества и цифровой экономики.

6.Способ защиты данных под управлением различных СУБД и разработанное на его основе СКЗИ «Крипто БД» сочетает в себе синтез лучших практик аутентификации и шифрования данных, что позволяет надежно защищать конфиденциальную информацию, в частности, персональные данные граждан в ряде критичных к разглашению информации информационных систем Российской Федерации.

ЗАКЛЮЧЕНИЕ

В диссертации приведено решение важной народнохозяйственной задачи - разработана методология построения иерархии уровней доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии, позволяющая значительно развить методы исследования идентификации и аутентификации, и формировать уровни доверия к результатам идентификации и аутентификации в информационных системах различного назначения. Впервые сформулированы критерии доверия к результатам идентификации и аутентификации. Установлено, что доверие к результатам идентификации в задачах управления доступом пользователей определяется главным образом уровнем доверия, достигнутым при первичной идентификации заявителя при его регистрации в конкретной информационной системе. Доверие к результатам первичной идентификации зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем идентификационных атрибутов, доверия к результатам верификации этих идентификационных атрибутов и доверия к привязке идентификационной информации к конкретной личности заявителя. Доверие к результатам аутентификации зависит от качества первичной идентификации при регистрации, способа генерации, хранения и использования аутентификационной информации (секрета), а также методов аутентификации (протоколов, применяемых для аутентификации, количества используемых факторов и способов обмена аутентификационной информацией). На основе разработанных и модернизированных моделей и методов исследования процессов идентификации и аутентификации предложены методики формирования уровней доверия к результатам идентификации и аутентификации для информационных систем различного назначения. Таким образом, в работе содержатся основные положения, методы и модели для совершенствования способов и средств защиты информации применительно к задаче идентификации и аутентификации участников удаленного электронного взаимодействия, позволяющие

проводить оценку рисков, а также достоверности, надежности и безопасности идентификации и аутентификации.

Впервые формализованы процедуры первичной и вторичной идентификации, разработаны методики и модели анализа достоверности, безопасности и надежности идентификации при удаленном электронном взаимодействии на основе анализа рисков, позволяющие определить требования к первичной идентификации в информационных системах с неограниченным числом субъектов доступа. Разработан метод оценки рисков первичной идентификации 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 информационных систем. Впервые построены матрицы рисков первичной идентификации, что позволяет проводить научно обоснованный анализ рисков на основе определенных из матриц рисков допустимых уровней рисков для типовых вероятных опасных событий. Проведенный анализ процесса идентификации субъектов доступа позволяет применять полученные научные результаты на стадиях проектирования и эксплуатации систем идентификации и аутентификации, что допускает возможность существенного сокращения сроков проектирования и/или модернизации существующих информационных систем с учетом требований безопасности, надежности и достоверности идентификации. Установлено, что для открытых ИС уровень рисков первичной идентификации на порядок выше, чем для корпоративных, при этом фактор лично явки существенно снижает относительные риски. Проведен параметрический анализ влияния ошибок первичной идентификации 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 позволяет значительно снизить результирующие ошибки.

Для оценки рисков аутентификации известными методами разработаны и

модернизированы модели и методики, позволяющие проводить анализ рисков с необходимой глубиной детализации для информационных систем различного назначения. Разработаны многоуровневые модели и методы анализа рисков нарушения информационной безопасности, включающие в себя рассмотрение угроз, уязвимостей, вероятных опасных событий и возможных последствий. Установлено, что наиболее высокий уровень рисков аутентификации наиболее вероятен при регистрации, генерации и хранении аутентификационной информации, а также ее обмене при взаимодействии сторон.

Разработаны математические модели и методики оценки функциональной надежности и безопасности процессов аутентификации, а также методика оценки достоверности результатов идентификации при удаленном электронном взаимодействии, что позволяет формировать уровни надежности результатов идентификации и аутентификации в различных информационных системах.

На основе предложенной концепции и разработанных методов, моделей и методик решён ряд практических задач, позволяющих существенно повысить уровень защищённости информационных ресурсов Российской Федерации. На базе проведенного анализа международных стандартов и нормативной базы, а также принятого 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 идентификации и аутентификации. В диссертационной работе приведены способы достижения определенных уровней доверия к результатам идентификации и аутентификации, а также разработаны примеры требований к аутентификации определенных групп пользователей для достижения указанных уровней доверия. Для государственных информационных систем рекомендовано введение, как минимум, трех уровней доверия к результатам аутентификации. Установлено, что самым безопасным с

наиболее достоверными результатами методом аутентификации является строгая аутентификация, основанная на цифровом сертификате доступа. При этом выявлено, что самым надежным и безопасным устройством аутентификации является интеллектуальная смарт-карта со специальным защищенным чипом, способным генерировать ключевые пары с гарантией неизвлекаемости закрытых ключей. Рассмотрена задача обеспечения юридической силы и юридической значимости электронных документов. Показано, что аналогом реквизитов бумажных документов являются сервисы безопасности, применяемые для создания, оформления и подписи электронного документа. Установлено, что минимально необходимым, и достаточным для большинства операций с электронными документами, является набор сервисов безопасности, состоящий из аутентификации автора подписи, электронной подписи, меток доверенного времени, валидации сертификата ключа проверки электронной подписи, проверки полномочий на подпись и гарантированной доставки документов и сообщений. Развитие и поддержка перечисленных сервисов безопасности в доверенном состоянии обеспечит электронным документам юридическую силу, то есть возможность вызывать правовые последствия, что позволит обеспечить полный переход от бумажного документооборота к электронному документообороту с сохранением заданного для бумажных документов уровня доверия к электронным документам; это необходимо для развития цифрового общества и цифровой экономики. Способ защиты данных под управлением СУБД и разработанное на его основе СКЗИ «Крипто БД» сочетает в себе синтез лучших практик аутентификации и шифрования данных, что позволяет надежно защищать конфиденциальную информацию и персональные данные граждан в ряде критичных к разглашению информации систем Российской Федерации.

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ААА	–	Аутентификация, авторизация, администрирование
АИ	–	Аутентификационная информация
БДУЗ	–	База данных учетных записей
ВОС	–	Вероятное опасное событие
ГИС	–	Государственная информационная система
ДТС	–	Доверенная третья сторона
ЕСИА	–	Единая система идентификации и аутентификации
ЗИ	–	Защита информации
ИА	–	Идентификация и аутентификация
ИИ	–	Идентификационная информация
ИД	–	Идентификационные данные
ИОК (PKI)	–	Инфраструктура открытых ключей (Public Key Infrastructure)
ИС	–	Информационная система
ИСО (ISO)	–	Международная организация по стандартизации (International Organization for Standardization)
ИСОП	–	Информационная система общего пользования
КИИ	–	Критическая информационная инфраструктура
МСЭ (ITU)	–	Международный союз электросвязи (International Telecommunication Union)
МЭК (IEC)	–	Международная электротехническая комиссия (International Electrotechnical Commission)
НПА	–	Нормативно – правовая информация
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПДн	–	Персональные данные
ПКТД	–	Программный комплекс терминального доступа

ПО	–	Программное обеспечение
СЗИ	–	Средство защиты информации
СКЗИ	–	Средство криптографической защиты информации
НСД	–	Несанкционированный доступ
СКПП	–	Сертификат ключа проверки подписи
СКПЭП	–	Сертификат ключа проверки электронной подписи
УДА		Уровень доверия к результатам аутентификации
УДИ		Уровень доверия к результатам идентификации
УКЭП	–	Усиленная квалифицированная электронная подпись
УЭВ	–	Удаленное электронное взаимодействие
ФН	–	Функциональная надежность
ЭП	–	Электронная подпись
ЭУ	–	Электронное удостоверение
ЮЗЭДО	–	Юридически значимый документооборот
SSCD	–	Security signature creation device
QSCD	–	Qualified signature creation device

СПИСОК ТЕРМИНОВ

анонимный субъект доступа, «аноним»: зарегистрированный субъект доступа, идентификационные данные которого не соответствуют требованиям к первичной идентификации или не подтверждались при первичной идентификации.

Примечание – аутентификация, используемая для подтверждения подлинности анонимного субъекта доступа, является анонимной аутентификацией.

атрибут: характеристика или свойство субъекта доступа или объекта доступа.

аутентификационная информация: информация, используемая при аутентификации субъекта доступа или объекта доступа.

аутентификация: действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

биометрические данные: сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

верификатор идентификации: доверенный объект, выполняющий вторичную идентификацию субъекта доступа при доступе.

верификатор аутентификации: доверенный объект, выполняющий аутентификацию субъекта доступа при доступе.

верификация: процесс проверки информации путем сопоставления предоставленной информации с ранее подтвержденной информацией.

взаимная аутентификация: обоюдная аутентификация, обеспечивающая для каждого из участников процесса аутентификации, и субъекту доступа, и объекту доступа, уверенность в том, что другой участник процесса аутентификации является тем, за кого себя выдаёт.

вторичная идентификация: действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации.

доверенная третья сторона: участник процесса аутентификации, предоставляющий один или более сервисов в области защиты информации, которому доверяют другие участники процесса аутентификации как поставщику данных услуг.

Примечания

1 При аутентификации доверенной третьей стороне имеется доверие как у субъекта доступа, так и у объекта доступа.

2 В качестве доверенной третьей стороны могут рассматриваться: организация (например, осуществляющая функции удостоверяющего центра), администратор автоматизированной (информационной) системы, устройство.

доверие: выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

Примечание – результаты, получаемые в рамках обеспечения доверия рассматриваются в качестве оснований для обоснования уверенности.

доступ: получение одной стороной информационного взаимодействия возможности использования ресурсов другой стороны.

Примечания

В качестве ресурсов стороны информационного взаимодействия, которые может использовать другая сторона информационного взаимодействия, рассматриваются информационные ресурсы, вычислительные ресурсы средств вычислительной техники и ресурсы автоматизированных (информационных) систем, а также средства вычислительной техники и автоматизированные (информационные) системы в целом.

закрытый ключ: ключ из состава асимметричной пары ключей, сформированных для объекта, который должен быть использован только этим объектом.

Примечания

1 Закрытый ключ не является общедоступным.

2 Ключ электронной подписи является примером закрытого ключа.

закрытый ключ неизвлекаемый: закрытый ключ, который при его формировании и хранении невозможно извлечь из устройства аутентификации, в котором он был создан.

Примечание – неизвлекаемость закрытого ключа заключается в отсутствии возможности его извлечения из устройства аутентификации, в котором он был создан, штатными средствами, предоставляемыми средой функционирования, не включающей данное устройство. Неизвлекаемость закрытого ключа в данных устройствах аутентификации, как правило, обеспечивается применяемыми схемотехническими решениями и гарантируется производителями устройств.

идентификатор доступа субъекта (объекта) доступа, идентификатор доступа, идентификатор: признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию.

идентификационная информация: совокупность значений идентификационных атрибутов, связанных с конкретным субъектом доступа или конкретным объектом доступа.

идентификационные данные: совокупность идентификационных атрибутов и их значений, которая связана с конкретным субъектом доступа или конкретным объектом доступа.

идентификационный атрибут: атрибут, который характеризует субъект доступа или объект доступа и может быть использован для его опознания.

идентификация: действия по присвоению субъектам и объектам доступа

идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ключ: изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

метод: путь исследования, способ достижения цели, совокупность приемов и операций практического и теоретического освоения действительности.

метод аутентификации: реализуемое при аутентификации предопределенное сочетание факторов аутентификации, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации.

Методика: как правило, некий готовый «рецепт», алгоритм, процедура для проведения каких-либо нацеленных действий. **Методика** отличается от **метода** конкретизацией приемов и задач.

метод обеспечения доверия: общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

методология: совокупность методов, способов реализации, которые представлены в виде последовательных этапов их применения для достижения основной цели.

многофакторная аутентификация: аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации.

несанкционированный доступ: доступ субъекта доступа к объекту доступа, нарушающий правила управления доступом с использованием штатных средств, предоставляемых средой функционирования.

объект доступа: одна из сторон информационного взаимодействия, которая предоставляет доступ.

одноразовый пароль: однократно используемый пароль.

Примечание – Возможность использования для аутентификации одноразового пароля прекращается (исключается) при наступлении события получения

доступа субъектом доступа или события отказа субъектом доступа от получения доступа или события отказа объектом доступа в предоставлении доступа.

односторонняя аутентификация: аутентификация, обеспечивающая только лишь для одного из участников процесса аутентификации – объекта доступа– уверенность в том, что другой участник процесса аутентификации – субъект доступа– является тем, за кого себя выдаёт предъявленным идентификатором доступа.

однофакторная аутентификация: аутентификация, при выполнении которой используется один фактор аутентификации.

открытый ключ: ключ, из состава асимметричной пары ключей, сформированных для объекта, который может быть общедоступным.

пароль: конфиденциальная аутентификационная информация, обычно состоящая из строки знаков.

первичная идентификация: действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов.

подлинность: свойство, гарантирующее, что субъект или ресурс идентичен заявленному.

подтверждающая информация: Информация, собранная и использованная для подтверждения идентификационных данных в соответствии с установленными требованиям к первичной идентификации.

правила управления доступом: правила, регламентирующие условия доступа субъектов доступа к объектам доступа на основе прав доступа.

Примечания

1 Права доступа определяют набор действий, которые субъекты доступа могут выполнять над объектами доступа.

2 Условия доступа определяют перечень разрешенных (запрещенных) действий субъектов доступа над объектами доступа в конкретной среде функционирования.

простая аутентификация: аутентификация с применением метода однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации.

протокол аутентификации: протокол, позволяющий участникам процесса аутентификации, осуществить аутентификацию.

Примечание – протокол реализует алгоритм (правила), в рамках которого субъект доступа и объект доступа последовательно выполняют определенные действия и обмениваются сообщениями.

процесс: совокупность взаимосвязанных и(или) взаимодействующих видов деятельности, использующих входы для получения намеченного результата.

санкционирование доступа, авторизация: предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом.

Примечание – положительный результат идентификации и аутентификации является одним из оснований для авторизации субъекта доступа.

санкционированный доступ: Доступ субъекта доступа к объекту доступа, не нарушающий правила управления доступом.

свидетельство: подтверждение, обеспечивающее уверенность в том, что субъект доступа или объект доступа соответствует заявленным идентификационным данным.

Примечание – в качестве свидетельств могут рассматриваться, например, результаты верификации заявленных идентификационных данных, документальные подтверждения (официальные документы), представленные субъектом доступа, а также другая подтверждающая информация.

строгая аутентификация: аутентификация с применением только метода

многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.

субъект доступа: одна из сторон информационного взаимодействия, которая инициирует получение и получает доступ.

Примечание – субъектами доступа могут являться как физические лица (пользователи), так и ресурсы стороны информационного взаимодействия, а также вычислительные процессы, инициирующие получение и получающие доступ от их имени.

уверенность: убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно, в соответствии с политикой безопасности).

управление доступом: предоставление санкционированного и предотвращение несанкционированного доступа.

уровень доверия: степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия.

Примечания

1 Уровень доверия не измеряется количественными показателями.

2 Степень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.

усиленная аутентификация: аутентификация с применением метода многофакторной односторонней или взаимной аутентификации и соответствующих данному методу протоколов аутентификации.

устройство аутентификации: техническое (аппаратное) или виртуальное устройство, содержащее информацию о его обладателе, которая может использоваться при идентификации и/или аутентификации.

фактор аутентификации: вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа или объектом доступа при аутентификации.

электронное удостоверение: совокупность идентификационной информации и аутентификационной информации (или прямого указания ее существования) субъекта доступа или объекта доступа, подлинность которой подтверждена доверенной третьей стороной.

Примечания

1 Электронное удостоверение может выпускаться доверенной третьей стороной с возможностью проверки его действительности на момент предоставления доступа конкретному субъекту доступа к конкретному объекту доступа.

2 Электронное удостоверение может представлять собой: в простейшем случае – идентификатор доступа и пароль; в других случаях – совокупность идентификатора доступа, открытого ключа и другой информации.

СПИСОК ЛИТЕРАТУРЫ

1 Сабанов А.Г. Обзор иностранной нормативной базы по идентифика-

ции и аутентификации // Инсайд. Защита информации. – 2013. – № 4 (52). – С. 82–88.

2 Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации субъектов при доступе к информации. Часть 1 // Инсайд. Защита информации. – 2016. – № 2. – С. 2–5.

3 Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации субъектов при доступе к информации. Часть 2 // Инсайд. Защита информации. – 2016. –№3. - С.70-73.

4 ГОСТ Р ИСО/МЭК 9594-8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации – Введ. 1999-01-01. [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов) – Электрон. Дан. – М.: Госстандарт России: ИПК Издательство стандартов, 1998 – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-9594-8-98/, свободный. – Загл. с экрана.

5 Баранов А.П. Методологические основы обнаружения вторжения в системах информационного противоборства. Диссертация на соискание ученой степени доктора технических наук. – Санкт-Петербургский государственный технический университет. 2000. – 303с.

6 Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Екатеринбург: Изд-во Урал. ун-та, 2003. – 328с.

7 Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х томах. – М.: Энергоатомиздат, Т.1; Т2. 1994. – 568с.

8 Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997. – 497с.

9 Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 291с.

10 Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы

компьютерной безопасности – М.: Академия, 2009. – 272с.

11 Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 332с.

12 Зегжда П.Д., Ивашко А.М. Моделирование информационной безопасности компьютерных систем // Проблемы информационной безопасности. Компьютерные системы, 1991. №1. С.8-13.

13 Конявский В.А. Методы и аппаратные средства защиты информационных технологий электронного документооборота. Диссертация на соискание ученой степени доктора технических наук. – М.: ВНИИПВТИ, 2005. – 360с.

14 Конявский В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией. Минск, 2004. – 327с. (Серия «Библиотека журнала «УЗИ»).

15 Костогрызов А.И., Нистратов Г.А. Применение математического моделирования для анализа и рационального управления процессами при создании и функционировании сложных систем // Дистанционное и виртуальное обучение. 2006. №2. С.32-54.

16 Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд-во ВПК, 2008. – 404с.

17 Вероятностный прогноз нарушения безопасности функционирования типовой системы инженерного обеспечения предприятия. А.И. Костогрызов [и др.]. //Системы высокой доступности. 2011. Т.7, №3. С.48-60.

18 Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса / Под ред. проф. В.А. Минаева. – М.: Гелиос АРВ, 2002. – 432с.

19 Коробец Б.Н., Минаев В.А., Сычев М.П. Информационные операции и проблема формирования современной культуры информационной безопасности // Системы высокой доступности. 2017. Т.13 , № 3, С. 38-46.

20 Минаев В.А., Сычев М.П., Вайц Е.В., Грачева Ю.В. Моделирование угроз информационной безопасности с использованием принципов системной

динамики // Вопросы радиоэлектроники. 2017. № 6. С.75-82.

21 Минаев В.А., Сычев М.П., Вайц Е.В., Грачева Ю.В. Риск-ориентированный подход к моделированию процесса противодействия угрозам информационной безопасности // Вопросы радиоэлектроники. 2017. № 6. С.83-92.

22 Смирнов С.Н. Метод проектирования систем обработки данных с заданными характеристиками доступности // С.Н. Смирнов/ Известия ЮФУ. Технические науки. – 2008. №8. С.64-71.

23 Смирнов С.Н. Метод проектирования систем с заданными задержками обслуживания // С.Н. Смирнов/ Вестник Российского университета дружбы народов. Серия прикладная и компьютерная математика. – М.: Изд-во Российского университета дружбы народов. 2003. Т.2. №1, С.52-67.

24 Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы: Монография. М.: МЦНМО – МГУ им. М.В. Ломоносова, 2002. 296 с.

25 Тарасов А.А. Функциональная устойчивость информационных систем: проблемы и пути их решения /А.А. Тарасов//Вопросы защиты информации. 2012. №4. С.73-80.

26 Тарасов А.А. Методы реконфигурации компьютерных систем для обеспечения функциональной устойчивости в условиях информационного противоборства. Диссертация на соискание ученой степени доктора технических наук. – МТУСИ. 2004.

27 Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ. 1996. – 112с.

28 Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования / А.В. Черемушкин. – М.: Издательский центр «Академия», 2009. – 272 с.

29 Черемушкин А.В. О содержании понятия «электронная подпись» // ПДМ, 2012, № 3, 53–69.

30 Шаньгин В.Ф. Комплексная защита информации в корпоративных системах / В.Ф, Шаньгин. – М.: ИД «ФОРУМ» : ИНФРА-М, 2010. – 592с.

31 Миронова В.Г., Шелупанов А.А. Модель нарушителя безопасности конфиденциальной информации //Информатика и системы управления. 2012, №1. С.28-35.

32 Миронова В.Г., Шелупанов А.А., Сопов М.А. Сети Петри-Маркова как инструмент создания моделей для основных видов несанкционированного доступа в информационные системы //Доклады Томского университета систем управления и радиоэлектроники. 2012, №1-2. С.20-24.

33 Шелупанов А.А., Скрыль С.В. Основы системного анализа в защите информации: Учебное пособие для студентов высших учебных заведений. М.: Машиностроение, 2008. 138 с.

34 Шерстюк В.П. Проблемы обеспечения информационной безопасности в современном мире // В кн. Математика и безопасность информационных технологий. Материалы конференции МГУ (Москва, 28-29 октября 2004г.) – М.: МЦНМО. 2005. – С.11-17.

35 Шубинский И.Б. Функциональная надёжность информационных систем. Методы анализа/ И.Б.Шубинский - Ульяновск: областная типография «Печатный двор», 2012. – 296с.-ил.

36 Шубинский И.Б., Замышляев А.М., Прошин Г.Б. Функциональная надёжность программного обеспечения информационных систем/ И.Б. Шубинский, А.М. Замышляев, Г.Б. Прошин // Надёжность. 2011. №3. С.72-81.

37 Щеглов А., Щеглов К. Цикл статей «Компьютерная безопасность». Глава 11. Идентификация и аутентификация. 24.05.2005. [Электронный ресурс]. – Режим доступа: http://news.sec.ru.

38 Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие. – М.: Книжный мир, 2009. – 352с.

39 Основы криптографии: Учебное пособие. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин – М.: Гелиос АРВ, 2005. - 480с.

40 Зубов А.Ю. Математика кодов аутентификации. – М.: Гелиос АРВ, 2007. – 278с.

41 Запечников С.В., Милославская Н.Г., Толстой А.И. и др. Информационная безопасность открытых систем: учебник для вузов в 2-х томах. Том 1 – М.: Горячая линия-Телеком, 2006. – 536с.

42 Афанасьев А.А., Веденьев Л.Т., Воронцов А.А., Газизова Э.Р., Додохов А.Л., Крячков А.В., Кузнецов С.Б., Полянская О.Ю., Сабанов А.Г., Скида М.А., Халяпин С.Н. Аутентификация. Теория и практика. Под ред. Проф., д.т.н. Шелупанова. М.: Горячая линия-Телеком, 2009,- 552с.: ил.

43 Конявская С.В. Плюсы и минусы двухфакторной аутентификации. [Электронный ресурс]. – Режим доступа: http://www.okbsapr.ru/konyavskaya_2007_13.html, свободный. – Загл. с экрана.

44 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во «Триумф», 2003. – 816 с.

45 NIST SP 800-63. Electronic Authentication Guideline (Руководство по электронной аутентификации). June 2006. [Электронный ресурс]. Режим доступа: URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf, свободный

46 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. [Электронный ресурс]. Режим доступа: URL: https://allgosts.ru/01/040/gost_r_iso!m_k_17799-2005, свободный.

47 ITU Rec.X.509 (08/1988) Series X: The Directory: authentication framework [Директория: Основы аутентификации] [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных. – Электрон. Дан. – Geneva, Switzerland,

International Telecommunication Union, [1988]. - Режим доступа: https://www.itu.int/rec/T-REC-X.509-198811-S/en, свободный. – Загл. с экрана.

48 ITU-T Rec.X.509 (08/1997) Series X: Information technology - Open Systems Interconnection - The Directory: Authentication framework [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [1997]. – Режим доступа: https://www.itu.int/rec/T-REC-X.509-199708-S/en, свободный. – Загл. с экрана.

49 ISO/IEC 9798-1:1991 Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [1991]. – Режим доступа: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=17661/, свободный. – Загл. с экрана.

50 ISO/IEC 9798-2:1991 | ITU Rec.X.800 (1991) Security architecture for Open Systems Interconnection for CCITT applications [Информационные технологии. Методы защиты. Аутентификация объектов. Архитектура безопасности для взаимодействия открытых систем для приложений МКТТ] [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [1991]. – Режим доступа: http://www.itu.int/rec/T-REC-X.800-199103-I/, свободный. – Загл. с экрана.

51 ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология (ИТ). Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации [Электронный ресурс], режим доступа: http://docs.cntd.ru/document/1200028710, свободный.

52 ISO/IEC 9798-3:1998 Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [1998]. – Режим доступа: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=29062/, свободный. – Загл. с экрана.

53 ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems – Part 2: Authentication framework. [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [1996]. – Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso-iec:10181:-2:ed-1:v1:en свободный. – Загл. с экрана.

54 ITU-T Rec.X.811 (04/1995) Series X: Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [1995]. – Режим доступа: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=3107&lang=ru/ свободный. – Загл. с экрана.

55 ITU-T Rec.X.810 (11/1995) Series X: Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [1995]. – Режим доступа: http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663Anqzm45z846q&cof=ORID:9&ie=UTF-

8&q=18.%2509ITU-T+X.810+/, свободный. – Загл. с экрана.

56 ITU-T Rec.Y.2720 (01/2009) Серия Y: Глобальная информационная инфраструктура, аспекты протокола интернет и сети последующих поколений. Сети последующих поколений – Безопасность. Структура управления идентичностью в сетях последующих поколений [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [2009]. – Режим доступа: https://www.itu.int/rec/T-REC-Y.2720-200901-I/, свободный. – Загл. с экрана.

57 ISO/IEC 24760-1:2011 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [2011]. – Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-1:v1:en, свободный. – Загл. с экрана.

58 ITU-T Rec.Y.2721 (09/2010) Серия Y: Глобальная информационная инфраструктура, аспекты протокола интернет и сети последующих поколений. Сети последующих поколений – Безопасность. Требования к управлению определением идентичности в сетях последующих поколений и случаи применения [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [2010]. – Режим доступа: https://www.itu.int/rec/T-REC-Y.2721-201009-I/en, свободный. – Загл. с экрана.

59 ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники

и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [2013]. – Режим доступа: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138, свободный. – Загл. с экрана.

60 ITU-T Rec.X.1254 (09/2012) Серия X: Сети передачи данных, взаимосвязь открытых систем и безопасность. Безопасность киберпространства – Управление определением идентичности. Структура гарантии аутентификации объекта [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [2012]. – Режим доступа: https://www.itu.int/rec/T-REC-X.1254-201209-I/en, свободный. – Загл. с экрана.

61 ISO/IEC 24760-2:2015 Information technology – Security techniques – A framework for identity management -- Part 2: Reference architecture and requirements [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [2015]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57915, свободный. – Загл. с экрана.

62 ITU-T Rec.X.1255 (09/2013) Серия X: Сети передачи данных, взаимосвязь открытых систем и безопасность. Безопасность киберпространства – Управление определением идентичности. Структура обнаружения информации по управлению определением идентичности [Электронный ресурс]: база данных содержит более 4000 документов, включая публикации, справочники, отчеты, программное обеспечение и базы данных – Электрон. Дан. – Geneva, Switzerland, International Telecommunication Union, [1988]. – Режим доступа: https://www.itu.int/rec/T-REC-X.1255-201309-I, свободный. – Загл. с экрана.

63 ISO/IEC 24760-3:2016 Information technology – Security techniques – A framework for identity management -- Part 3: Practice [Электронный ресурс]: база

данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [2016]. – Режим доступа: https://www.iso.org/standard/57916.html, свободный. – Загл. с экрана.

64 ISO/IEC 9798-5:2009 Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. – Geneva, Switzerland, International Organization for Standardization, [2009]. – Режим доступа: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:9798:-5:ed-3:v1:en, свободный. – Загл. с экрана.

65 Lindeman R. Scalable authentication [Электронный ресурс]. – Режим доступа: https://fidoalliance.org/specifications/additionalresources/, свободный. – Загл. с экрана.

66 FIDO. The State of Strong Authentication 2019. Adoption Rises under Threat of New Risks and Regulation. Javeling [Электронный ресурс]. – Режим доступа: https://fidoalliance.org/specifications/download/, свободный. – Загл. с экрана.

67 Сабанов А. Г. Некоторые проблемы идентификации при удаленном электронном взаимодействии // Первая миля (Last Mile). – февраль 2014. – № 41. – С. 94–97.

68 Об информации, информационных технологиях и о защите информации: федер. закон № 149-ФЗ: принят Гос. Думой 08.07.2006 г.: одобр. Советом Федерации 14.07.2006 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2006] – Режим доступа: http://docs.cntd.ru/document/901990051, свободный. – Загл. с экрана.

69 О персональных данных: федер. закон № 152-ФЗ: принят Гос. Думой

08.07.2006 г.: одобр. Советом Федерации 14.07.2006 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2006] – Режим доступа: http://docs.cntd.ru/document/901990046, свободный. – Загл. с экрана.

70 Об организации предоставления государственных и муниципальных услуг: федер. закон № 210-ФЗ: принят Гос. Думой 07.07.2010 г.: одобр. Советом Федерации 14.07.2010 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2010] – Режим доступа: http://docs.cntd.ru/document/902228011, свободный. – Загл. с экрана.

71 О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон № 112-ФЗ: принят Гос. Думой 24.05.2013 г.: одобр. Советом Федерации 29.05.2013 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2013] – Режим доступа: http://docs.cntd.ru/document/499024915, свободный. – Загл. с экрана.

72 Об электронной подписи: федер. закон № 63-ФЗ: принят Гос. Думой 25.03.2011 г.: одобр. Советом Федерации 30.03.2011 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2011] – Режим доступа: http://docs.cntd.ru/document/902271495, свободный. – Загл. с экрана.

73 О государственной автоматизированной системе Российской Федерации «Выборы»: федер. закон № 20-ФЗ: принят Гос. Думой 20.12.2002 г.: одобр. Советом Федерации 27.12.2002 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2003] – Режим доступа: http://docs.cntd.ru/document/901837887,

свободный. – Загл. с экрана.

74 О связи: федер. закон № 126-ФЗ: принят Гос. Думой 18.06.2003 г.: одобр. Советом Федерации 25.06.2003 г.: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [2003] – Режим доступа: http://docs.cntd.ru/document/901867280, свободный. – Загл. с экрана.

75 О занятости населения в Российской Федерации: федер. закон № 1032-1: [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов). – М., [1991] – Режим доступа: http://docs.cntd.ru/document/9005389, свободный. – Загл. с экрана.

76 Обеспечение информационной безопасности бизнеса. В.В. Андрианов [и др.]. Под ред. А.П. Курило. М.: Издательство Альпина Паблишер. 2010. – 392с.

77 Барсуков В.С., Дворянкин С.В., Шеремет И.А. Безопасность связи в каналах телекоммуникаций // Технологии электронных коммуникаций. 1992. Том 20. – 297с.

78 Бобов М.Н. принципы построения систем разграничения доступа в интегрированных телекоммуникационных системах // Российско-Белорусский научно-технический журнал «Управление защитой информации». 2001. Том 5. №3. С.267-273.

79 Большаков Ю.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. Часть 1: Методы, средства и механизмы защиты данных. – Санкт-Петербург. 1995. – 199с.

80 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО ТИЛ ДС, 2001. – 688с.

81 Ермаков А.С., Аманжолова С.Т. Модели аутентификации и идентификации распределенной вычислительной системы на примере системы дистанционного образования // Известия НТО «КАХАК». – 2009. - №1/32. С.11-17.

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

83 Девянин П.Н. Базовая ролевая ДП-модель // ПДМ, 2008, 1(1), С. 64–70.

84 Аманжолова С.Т., Жакаев Н.О. Моделирование процессов защиты информации // Вестник КазНТУ. 2013. С.3-11.

85 Аманжолова С.Т., Жакаев Н.О. Моделирование процессов защиты информации // Вестник КазНТУ. 2013. С.3-11.

86 Сабруков А., Грушо А. Аутентификация в компьютерных системах // Системы безопасности. 2003. №5 (53).

87 Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. О комплексной аутентификации. Системы и средства информации. 2017. Том 27, вып.3, С. 4-11.

88 Кузовкин К.Н. Удаленный доступ к информационным ресурсам. Аутентификация //Директор информационной службы. Изд-во Открытые системы. М.: 2013. №9. – Режим доступа: http://www.osp.ru/cio/2003/09/172866/, свободный. – Загл. с экрана.

89 Горбенко Ю.И., Олешко И.В. Модели и методы оценки защищенности механизмов многофакторной аутентификации // Восточно-Европейский журнал передовых технологий. 2013. №6/2. С.4-10.

90 Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015. – 93с.

91 Щеглов К.А., Щеглов А.Ю. Методы и модели идентификации и аутентификации пользователя при доступе к файловым объектам. 20 ноября 2013г. [Электронный ресурс] http://www.securitylab.ru/blog/personal/Information-security/34882.php Режим доступа: свободный . Дата проверки: 05.06.2019.

92 М. Бондаренко, С. Тихонов Биометрия в аутентификации //[Электронный ресурс]: BIS Journal №4(31)/2018, режим доступа – свободный , дата проверки 24.03.2020.

93 Phillip Griffin. Biometric Electronic Signatures //ISSA Journal. November 2017, pp. 29-32.

94 Бродский А. Риск-ориентированная аутентификация // BIS Journal №2 (29)/2018.

95 Wiefling, Stephan; Lo Iacono, Luigi; Dürmuth, Markus. "Information website on Risk-based Authentication". Risk-based Authentication. Retrieved 2019-04-29.

96 Wiefling, Stephan; Lo Iacono, Luigi; Dürmuth, Markus (2019). Dhillon, Gurpreet; Karlsson, Fredrik; Hedström, Karin; Zúquete, André (eds.). "Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild". ICT Systems Security and Privacy Protection. IFIP Advances in Information and Communication Technology. Springer International Publishing: 134–148. doi:10.1007/978-3-030-22312-0_10. ISBN 9783030223120.

97 ГОСТ Р ИСО/МЭК. 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс] http://gostexpert.ru/gost/gost-17799-2005 Режим доступа: свободный . Дата проверки: 05.06.2018.

98 NIST SP 800-33. Gary Stoneburger. Unerlying Technical Models for Information Technology Security. 2001. (Технические модели, лежащие в основе безопасности информационных технологий) [Электронный ресурс]. URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf, Режим доступа: свободный.

99 Федеральный закон Российской Федерации от 15 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями на 29 июля 2017 года). [Электронный ресурс] http://docs.cntd.ru/document/901836556

100 О внесении изменений в ФЗ «О техническом регулировании //ФЗ от

21 июля 2011 г. № 255-ФЗ.

101 О внесении изменений в ФЗ «О техническом регулировании» //ФЗ от 30 ноября 2011 г. № 347-ФЗ.

102 ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения (Руководство ИСО 73:2009).

103 ГОСТ Р 51901.12-2007. Метод анализа видов и последовательность отказов.

104 ГОСТ Р 51901.13-2005 (МЭК 61025:1990) Анализ дерева неисправностей (FTA).

105 ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство.

106 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

107 ГОСТ Р ИСО/МЭК 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

108 ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 1 Введение и общая модель.

109 ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

110 ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

111 Методика оценки рисков нарушения ИБ, принятая Банком России

11.11.2009 № Р-1190.

112 ГОСТ Р 54505-2011. Управление рисками на железнодорожном транспорте. М., Стандартинформ. 2011.

113 Шепитько Г.Е. Теория информационной безопасности и методология защиты информации: учебно-методическое пособие. – М.: РГСУ, 2012.-128с.

114 Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах: монография / М. Ю. Монахов [и др.]; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2015. – 208 с.

115 English L.P. Information Quality Management: The Next Frontier // Quality Congress AsQs. Annual Quality Congress Proceeding. 2001. P. 529-533.

116 Сабанов А.Г. Вопросы доверия при построении электронного правительства // Инсайд. Защита информации. 2010. №2 (32). С.66-70.

117 Илларионов Ю.А., Монахов М.Ю. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах. Владимир: Владим. гос. ун-т. Владимир, 2004. 204 с.

118 Приказ ФСТЭК России от 21 сентября 2016 г. N 131, утверждающий «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [Электронный ресурс]: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1189-prikaz-fstek-rossii-ot-21-sentyabrya-2016-g-n-131, доступ свободный, дата проверки: 25.03.2020.

119 ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем.

120 NIST SP 800-30. Revision 1, *Guide for Conducting Risk Assessments*, September 2012. [Электронный ресурс]. – Режим доступа: https://doi.org/10.6028/NIST.SP.800-30r1, также http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, свободный.

121 Thomas R. Peltier. Information Security Risk Analysis. – 2005. CRC Press Taylor & Francis Group. 6000 Broken Sound Parkway NW, Suite 300. 361p.

122 ГОСТ Р ИСО/МЭК 16085-2007 Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения.121

123 ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

124 ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска.

125 ГОСТ Р 51901.13-2005 (МЭК 61025:1990) Анализ дерева неисправностей (FTA)

126 Moghissi A.A., Narland R.E., Congel F.J. Eckerman K.F. Methodology for environmental human exposure and health risk assessment // Dyn. Exposure and Hazard Assessment Toxic chem. – Ann Arbor, Michigan, USA 1980, p. 471–489.

127 Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь, 2013. №4. С.27-32.

128 Сабанов А.Г. Основные процессы аутентификации / А.Г. Сабанов // Вопросы защиты информации. 2012г. №3. С. 54-57.

129 Сабанов А.Г. Аутентификация в распределенных системах // Инсайд. Защита информации. 2008. № 4. С.69-73.

130 Сабанов А.Г. Сабанов А.Г. Обзор технологий идентификации и аутентификации // Документальная электросвязь. 2006. №17. С.23-27.

131 Сабанов А.Г. Классификация процессов аутентификации // Вопросы защиты информации. 2013. № 3. С. 47-52.

132 Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности //Электросвязь. 2014. № 2. С.6-9.

133 Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов

аутентификации //Вопросы защиты информации. – 2014. – № 1(104).

134 Кузнецов В.П. Интервальные статистические модели. – М.: Радио и связь, 1991. – 367с.

135 Zio E. Reliability Engineering: Old Problems and New Challenges //Reliability Engineering and System Safety. – 2009. – № 94(2).

136 Shmerko V., Levashenko V., Yanushkevich S. Parallel Algorithms for Calculation Direct Logic Derivatives of Multi-Valued Functions //Cybernetics and System Analysis (Plenum/Kluwer Academic Publishers, USA). – 1996. – № 32(6).

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

138 ISO/IEC 14598-1:1999. Information technology - Software product evaluation - Part 1: General overview.

139 Сабанов А.Г. Надежность идентификации и аутентификации // Материалы регионального семинара ITU. Москва, 25 – 27 ноября 2013г. [Электронный ресурс], режим доступа: http://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2013/11_Moscow/Session_6_Sabanov.pdf, свободный.

140 Сабанов А.Г. Аутентификация при электронном обмене конфиденциальными документами /А.Г. Сабанов// Доклады Томского государственного университета систем управления и радиоэлектроники, 2011г., №2(24), С.263-266.

141 Мельниченко П.С., Сабанов А.Г. Предоставление защищенного доступа к информационным системам массового использования при оказании государственных услуг в электронном виде // Вестник Российской таможенной академии. 2011. № 3. С. 73-78.

142 Сабанов А.Г. Об уровнях строгости аутентификации // Доклады ТУСУР. 2012. № 2-1 (26). С. 134-139.

143 Сабанов А.Г. Вопросы идентификации и аутентификации в информационных системах общего использования // Информационно-измерительные и

управляющие системы 2013. Т.11 № 7, Изд-во «Радиотехника», 2013. С.081-084.

144 Сабанов А.Г. проблемы идентификации при удаленном электронном взаимодействии // Первая миля. 2014. № 2 (41). С. 94-97.

145 Кузьмин А.С., Сабанов А.Г. Анализ зарубежной нормативной базы по идентификации и аутентификации. Инженерный журнал: наука и инновации. 2013. Вып.11 (23). С.1-13. URL: http://engjournal.ru/catalog/it/security/1021.html (см.также Российское правосудие. 2013.)

146 Сабанов А.Г. Биометрическая идентификация: помогут ли новые нормативные документы в снижении рисков? // Внутренний контроль в кредитной организации. Методический журнал. ИД "Регламент-Медиа" 2018. №3(39). С.81-93.

147 Сабанов А.Г., Смолина С.Г. Сравнительный анализ биометрических методов идентификации личности. Труды ИСА РАН. Том 66 3/2016. С.12-21.

148 Сабанов А.Г. Методы исследования надежности удаленной аутентификации. Журнал «Электросвязь» №10, 2012г., стр.20-24.

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

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

151 Сабанов А.Г. О концепции формирования уровней доверия к результатам идентификации и аутентификации субъектов доступа. В сборнике докладов XI Всероссийской межведомственной научной конференции «Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации». Орёл. 5-6 февраля 2019 г. Часть 10. С.21-24.

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

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

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

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

156 Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии. //Доклады Томского государственного университета систем управления и радиоэлектроники. 2014.№2(32) июнь. С.180-184.

157 Сабанов А.Г. Методика идентификации рисков процессов аутентификации. Доклады Томского государственного университета систем управления и радиоэлектроники. 2013. №4 (30), С.136-141.

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

159 Сабанов А.Г. Метод многоуровневого анализа рисков аутентификации при удаленном электронном взаимодействии // Вопросы защиты информации. 2014. №2. С.29-36.

160 Сабанов А.Г. Анализ рисков аутентификации при удаленном электронном взаимодействии // Методы и технические средства обеспечения безопасности информации. 2014. №23. С.53.

161 Сабанов А.Г. Концепция моделирования процессов аутентификации //

Доклады Томского государственного университета систем управления и радиоэлектроники, №3(29) сент. 2013. С.71-75.

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

163 Сабанов А.Г. Об уровнях доверия к первичной идентификации // Методы и технические средства безопасности информации. 2018. №27. С.67-69.

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

165 Сабанов А.Г. Способы оценки надежности аутентификации. Доклад на постоянно действующем научном семинаре «Надежность и качество функционирования систем» РАН и Международной академии наук высшей школы. Московский государственный университет путей сообщения. 25 октября 2012 г.

166 Додохов А.Л., Сабанов А.Г. Способ защиты баз данных, содержащих персональные данные // Вопросы защиты информации. 2012. №3. С.4-9.

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

168 ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы – Введ. 2012-07-01. [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации – Электрон. дан. (17 млн. документов) – Электрон. Дан. – М.: Стандартинформ, 2012 – Режим доступа: http://docs.cntd.ru/document/1200091394/, свободный. – Загл. с экрана.

169 ISO/IEC 29146: 2016 Information technology – Security techniques – Framework for Access Control. – URL: https:// www.iso.org/ru/standard/45169.html

170 ISO/IEC 29003: 2017 Information technology – Security techniques – Identity Proofing. – URL: https://www.iso.org/ru/ standard/62290.html

171 ГОСТ Р 58833-2020 Идентификация и аутентификация. Общие положения. [Электронный ресурс]: http://docs.cntd.ru/document/437254729

172 S.Soviany, H.Jurian A Hierarchical Data Fusion and Classification Model for Biometric Identification Systems. http://www.agir.ro/buletine/1577.pdf

173 Перепечина И.О. Проблема категорического экспертного вывода в судебной ДНК-идентификации и разработка подхода к его решению. http://www.k-press.ru/bh/2003/2/perepechina/perepechina.asp

174 NIST SP 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. Gaithersburg, Maryland, USA, National Institute of Standards and Technology, 2017. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-63a/final, свободный. – Загл. с экрана.

175 NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management [Электронный ресурс]: база данных содержит более 21000 международных стандартов, касающихся всех аспектов техники и бизнеса – Электрон. Дан. Gaithersburg, Maryland, USA, National Institute of Standards and Technology, 2017. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-63b/final, свободный. – Загл. с экрана.

176 Гапанович В.А., Шубинский И.Б., Замышляев А.М. Построение и использование матриц рисков в системе управления рисками на железнодорожном транспорте // Надежность. 2011, №4. С. 56-68.

177 Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. 2016, №2, С. 49-53.

178 Новожилов Е.О. Принципы построения матрицы рисков // Надежность. 2015, №3. С. 73-79.

179 ГОСТ 33433-2015 Безопасность функциональная. Управление рисками на железнодорожном транспорте. http://docs.cntd.ru/document/1200127759

180 Гапанович В.А., Замышляев А.М., Шубинский И.Б. Некоторые вопросы управления ресурсами и рисками на железнодорожном транспорте на основе состояния эксплуатационной надежности и безопасности объектов и процессов (проект УРРАН) // Надежность. 2011. №1. С. 2-8.

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

182 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены Приказом ФСТЭК России от 11 февраля 2013 года № 17. Зарегистрировано в Минюсте России 31 мая 2013 года № 28608.

183 Методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год. [Электронный ресурс]. Режим доступа: http://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god, свободный.

184 Методические указания 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432. [Электронный ресурс], Режим доступа: http://www.fsb.ru/files/PDF/Metodicheskie_recomendacii.pdf, свободный.

185 Harrison, M. (2004). Human error analysis and reliability assessment. Workshop on Human Computer Interaction and Dependability, 46th IFIP Working Group 10.4 Meeting, Siena, Italy, July 3–7, 2004.

186 ITU-T Rec. X.660 (08/2004) Interconnection technology-Open Systems Interconnection – Procedure for the operation of OSI Registration Authorities: General procedure and top arcs of the ASN.1 Object Identifier tree. http://www.itu.int/ITU-T/2005-2008/com17/oid/X.660-E.pdf.

187 Сабанов А.Г. Проблема доверия к результатам идентификации и аутентификации граждан при переходе к цифровой экономике. Доклад на пленарном заседании VII Международной научно-практической конференции «управление информационной безопасностью в современном обществе» Москва, 29-30 мая 2019 г. [Электронный ресурс]. Режим доступа: https://vipforum.ru/upload/events/vshe/VII%20МЕЖДУНАРОДНАЯ%20НАУЧНО-ПРАКТИЧЕСКАЯ%20КОНФЕРЕНЦИЯ.pdf, свободный.

188 Цыгичко В.Н. Прогнозирование социально-экономических процессов. Изд.3. М.: УРСС. 2009. – 240с.

189 Сычев А.М. Обоснование требований к межсетевым экранам и системам управления безопасностью в распределенных информационных системах. Диссертация на соискание ученой степени кандидата технических наук. – Санкт-Петербургский государственный политехнический университет. 2002.

190 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.

191 Сабанов А.Г. О роли аутентификации при беспроводном доступе // Мобильные телекоммуникации», 2004. №3, С.57-60.

192 Сабанов А.Г. Роль аутентификации в организации защиты документооборота при использовании открытых сетей связи / Материалы Третьей Всероссийской практической конференции «Эффективный документооборот в органах государственного управления: от традиционного к электронному», 2005, С.126-129.

193 Сабанов А.Г. Защита от дилетантов //А.Г.Сабанов/ ИнформКурьерСвязь. 2013. №11. С.53.

194 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.

195 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.

196 Ministerial Declaration on Authentication for Electronic Commerce. 7-9 October 1998. [Электронный ресурс]. Режим доступа: http://www.oecd.org/internet/ieconomy/35842032.pdf, свободный.

197 FIPS 196, "Entity authentication using public key cryptography" Federal Information Processing Standards Publication 196, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997. [Электронный ресурс]. Режим доступа: http://csrc.nist.gov/publications/fips/fips196/fips196.pdf, свободный

198 FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006. [Электронный ресурс]. Режим доступа: URL: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf, свободный.

199 FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2011. [Электронный ресурс]. Режим доступа: http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf, свободный.

200 Haufe, K. (2017). Maturity based approach for information security management system Governance. [Электронный ресурс]. Режим доступа: https://archivo.uc3m.es/bitstream/handle/10016/25128/tesis_knut_haufe_2017.pdf?sequence=3, свободный.

201 PEPPOL. DeliverableD1.3 Demonstrator and functional Specifications for Cross-Border Use of e-Signature in Public Procurement. Part 7: eID and Signature Qualify Classification, rev. 1.3.

202 Ричард Э. Смит. Аутентификация: от паролей до открытых ключей. – М.: «Вильямс», 2002.- 432с.

203 Сабанов А.Г. Модели для исследования безопасности и надежности

процессов аутентификации // Электросвязь. 2013. №10, С.38-42.

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

205 Directive 1999/93/EC of the Parliament and the Council on a Community Framework for Electronic Signatures// Official J. of European Communities. OJ L 13. 19.01.2000.

206 EU Regulaton 910/2014 of 23 July 2014 eIDAS (Electronic Identification, Authentication and Trust Services). [Электронный ресурс], режим доступа: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, свободный.

207 State Identity Credential and Access Management (SICAM). Guidance and Roadmap. Sept. 2012. [Электронный ресурс], режим доступа: URL: http://www.nascio.org/publications/documents/SICAM.pdf, свободный.

208 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

209 ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования

210 OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003 & OMB Circular A-130 2003. [Электронный ресурс]. Режим доступа: URL: http://csrc.nist.gov/drivers/documents/m04-04.pdf свободный,

211 ISO 31000:2009. Risk Management – Principles and Guidelines

212 Федеральный закон от 27.12.2019 N 476-ФЗ "О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" [Электронный ресурс]. Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_341757/, свободный.

213 Boneh D., DeMillo R.A., Lipton R.J. On the Importance of Checking Cryptographic Protocols for Faults. // http://citeseer.ist.psu.edu. – Bellcore, Morristown, NJ.

214 Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C. The Sorcerer's Apprentice Guide to Fault Attacks. // http://citeseer.ist.psu.edu.

215 Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009, - 576с, ил:.

216 Методика оценки нарушения рисков информационной безопасности. Принята распоряжением №Р-1109 Банка России от 11.11.2009. http://www.zakonprost.ru/content/base/part/648065

217 Шубинский И.Б. Основы анализа сложных систем. Учеб. пособ. – Л.: Министерство обороны СССР, 1986.

218 Сабанов А.Г. О неизвлекаемости закрытых ключей / Inside. Защита информации. 2015. №2. С.30-33.

219 User authentication guidance for information technology systems. ITSP 30.031.v.3. Government od Canada. April 2018. [Электронный ресурс]. Режим доступа: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng_0.pdf, свободный.

220 Маллаев Ш.Р. Использование методов аутентификации в развитии электронной торговли // Вопросы структуризации экономики. 2014. № 2. С. 80-85.

221 Никитин В.В., Гунченко Ю.И., Басов О.О. Оценка условных вероятностей байесовской сети доверия при априорной информации о взаимодействии между ее узлами в системе многомодальной аутентификации пользователя // Научный результат. Информационные технологии. 2017. Т. 2. № 3. С. 3-10.

222 Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // System Sciences. 2002. P. 2431-2439.

223 Шиверов П.К., Бондаренко В.В. Понятие доверия в контексте информационной безопасности // Информационные технологии и нанотехнологии-

2016. – 2016. – с. 414–418.

224 Шиверов П.К., Новосад Т.Г., Осипов М.Н. Доверие в контексте анализа стойкости протоколов аутентификации // Ползуновский вестник. 2014. № 2. С. 248-250.

225 Шведова Л.Е. Средства защиты доступа к информационным системам // Математические методы и информационно-технические средства: материалы XI Всероссийской научно-практической конференции (г. Краснодар, 19 июня 2015 г.). С. 318-321.

226 Губка О.А. Как организовать аутентификацию в сети взаимодействующих предприятий. Инсайд. Защита информации. 2018. №2(80). С.75-77.

227 Бобов М.Н. принципы построения систем разграничения доступа в интегрированных телекоммуникационных системах // Российско-Белорусский научно-технический журнал «Управление защитой информации». 2001. Том 5. №3. С.267-273.

228 ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 февраля 2013 г. № 3-ст.

229 ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

230 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены Приказом ФСТЭК России от 11 февраля 2013 года № 17. Зарегистрировано в Минюсте России 31 мая 2013 года № 28608.

231 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены Приказом ФСТЭК России от 18 февраля 2013 г. № 21. Зарегистрировано в Минюсте России 14 мая 2013 года

№ 28375.

232 Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены Приказом ФСТЭК России от 14.03.2014 г. № 31. Зарегистрировано в Минюсте России 14 июня 2014 года № 32919.

233 Наджарян Р.В. Проблемы юридической силы документа в условиях применения информационных технологий. 2010. Электронный ресурс: http://www.juristlib.ru/book_9392.html

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

235 Сабанов А.Г. О доверии к сервисам безопасности, обеспечивающим юридическую силу электронным документам // Первая миля. 2016. №1 (#54). С.42-43 (часть 1). №2 (#55). С.34-37 (часть 2).

236 Додохов А.Л., Сабанов А.Г. Исследование применения СУБД Oracle для защиты персональных данных //Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. №2(24). С.267-270.

237 Додохов А.Л., Сабанов А.Г. К вопросу о защите персональных данных с использованием СУБД Oracle. /А.Л. Додохов, А.Г. Сабанов// Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. №2(26). С.129-133

238 Додохов А.Л., Сабанов А.Г. Способ защиты баз данных, содержащих персональные данные // Вопросы защиты информации» 2012. №3. С.4-9.

239 Бондарчук С.С., Додохов А.Л., Сабанов А.Г. Технология защиты персональных данных с использованием СУБД Oracle. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета.

2012г., №152, С.36-40.

240 Changyu Dong, Giovanni Russello and Naranker Dulay. Shared and Searchable Encrypted Data for Untrusted Servers. Data and Applications Security XXII: 22ndAnnual IFIP WG 11.3 Working Conference on Data and Applications Security. London, UK, July 13—16, 2008.

241 Peishun Wang, Huaxiong Wang and Josef Pieprzyk. An Efficient Scheme of Common Secure Indices for Conjunctive Keyword-Based Retrieval on Encrypted Data. Information Security Applications: 9th International Workshop, WISA 2008. Jeju Island, Korea, September 23—25, 2008.

242 Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi and Pierangela Samarati. Enforcing Con□dentiality Constraints on Sensitive Databases with Lightweight Trusted Clients.Data and Applications Security XXIII: 23rd Annual IFIP WG 11.3 Working Conference. Montreal, Canada, July 12—15, 2009.

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