Томский государственный университет систем управления и радиоэлектроники (ТУСУР)

На правах рукописи

Исхаков Андрей Юнусович

МЕТОДИЧЕСКОЕ И ПРОГРАММНО-АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОЦЕССА ИДЕНТИФИКАЦИИ ПОСЕТИТЕЛЕЙ В МЕСТАХ МАССОВОГО ПРЕБЫВАНИЯ ЛЮДЕЙ

05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель
доктор технических наук,
профессор Р.В. Мещеряков

Томск – 2016

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
ИАФ	Идентификация и аутентификация
ИД	Идентификатор доступа
КПП	Контрольно-пропускной пункт
КПР	Контрольно-пропускной режим
КУД	Контроль и управление доступом
ММПЛ	Места массового пребывания людей
ОС	Операционная система
ПИАФ	Подсистема идентификации и аутентификации
ПО	Программное обеспечение
СЗИ	Система защиты информации
СКУД	Система контроля и управления доступом
СУ	Средства управления
ТСОБ	Технические средства обеспечения безопасности
УВИП	Устройства ввода идентификационных признаков
УИ	Устройства исполнительные
УПУ	Устройства преграждающие управляемые
УС	Устройства считывающие (считыватели)

ВВЕДЕНИЕ

Актуальность темы. В современном мире одной из наиболее значимых угроз безопасности населения является международный терроризм. Особенность террористических актов последних десятилетий заключается в стремлении преступников распространить среди мирного населения панику, страх и сомнение в силах государственных структур. Для этого в качестве объектов посягательств террористами выбираются места массового пребывания людей. Число жертв, размеры и характер разрушений, вызванные терактами начала XXI века, сопоставимы с последствиями вооруженных конфликтов и локальных войн [1, 2].

В условиях сложившейся геополитической обстановки и крайней степени актуальности угрозы терроризма спецслужбы всего мира предпринимают различные действия по усилению мер безопасности [3–8] в местах массового пребывания людей (ММПЛ) [6, 9]. В законодательстве Российской Федерации на данный момент отсутствует строгое определение ММПЛ, хотя некоторые нормативно-правовые акты подразумеваеют категорирование подобных мест по количественному показателю [10, 11]. В общем случае под ММПЛ понимаются общественные места с высокой плотностью человеческих потоков и вероятностью возникновения неуправляемой толпы.

Подобными свойствами, например, обладают объекты транспортной инфраструктуры: вокзалы, метрополитены, крупные пункты пересадки пассажиров наземного городского транспорта и т.д. Такие места не только обладают внутренними подразделениями, отвечающими за обеспечение физической безопасности граждан, но и в соответствии с [9] подлежат обязательной охране полицией. Усиление мер безопасности на объектах подобного рода достигается путем ужесточения действующего пропускного и внутриобъектового режимов.

Тем не менее нерассмотренными остаются вопросы обеспечения безопасности в ММПЛ, особенности функционирования которых не позволяют внедрить полноценный пропускной режим. К подобным местам можно отнести крупные офисные центры (площади которых арендуются множеством различных компаний), выставочные комплексы (экспоцентры), кинозалы, театры и т.д. Такие места не относятся к перечню объектов [9], подлежащих обязательной охране силовыми структурами.

В рамках данной работы под ММПЛ будем понимать не подлежащие обязательной охране полицией объекты массового пребывания людей, особенности функционирования которых не позволяют внедрить полноценный пропускной режим. Стоит отметить, что речь не идет о полном отсутствии мер по обеспечению физической безопасности в ММПЛ. Зачастую администрация таких объектов, руководствуясь требованиями [11–13] и других законодательных актов, добросовестно относится к реализации комплекса инженерных, технических и организационных мероприятий по обеспечению мер безопасности для своих посетителей (субъектов доступа). К данным мероприятиям относятся выборочный контроль посетителей ММПЛ сотрудниками службы охраны, использование металлодетекторов на пунктах прохода, установка систем пультовой охраны, средств видеонаблюдения и т.д.

Однако постоянный поток «случайных» посетителей и отсутствие возможности регистрации пользователей (заблаговременного уведомления администрации ММПЛ субъектом доступа о намерении посещения объекта), не позволяют проводить процедуру идентификации [14, 15] личности посетителей. Этот факт упрощает беспрепятственный проход на объект злоумышленников, позволяет им без каких-либо усилий слиться с толпой мирных граждан. Кроме того, отсутствие идентифицирующих сведений о посетителях ММПЛ значительно затрудняет расследование преступлений и различных инцидентов правоохранительными структурами.

Политика тотальной проверки и регистрации паспортных данных посетителей неприменима в ММПЛ ввиду ее негативного влияния на протекающие бизнес-процессы. Это вызвано длительностью процедур идентификации посетителей и регистрации соответствующих событий. Зачастую выполнение администрацией ММПЛ подобных мер невозможно ввиду необходимости большой численности контролирующего персонала.

В целом задача идентификации личности весьма многогранна и имеет множество решений применительно к различным предметным областям. Анализ литературы показал, что данная проблема в разных аспектах нашла отражение в работах А.А. Малкова, В.В. Волхонского, А.Г. Сабанова, В.А. Вороны, В.А. Тихонова, Р.В. Мещерякова, А.А Малюка, Г.А. Остапенко, А.А. Шелупанова, B. Schneier, N. Skandhakumar, A. Dmitrienko, J. Brainard, S. Schechter, S. Egelman, R.W. Reeder, а также ряда других отечественных и зарубежных ученых.

Развитие отрасли технических средств защиты невозможно без внедрения наукоемких решений. Учеными всего мира проводятся исследования, направленные на разработку новых способов идентификации пользователей и технологий передачи идентификационных данных, моделирование действий злоумышленника, улучшение помехоустойчивости оборудования и других мер противодействия угрозам информационной безопасности. Например, А.Г. Африн в своей диссертации [16] предложил метод адаптивной организации систем и высокопроизводительных средств биометрического контроля доступа. В работе А.А. Грушо [17] рассматриваются вопросы определения необходимых и достаточных условий существования безопасных структур распределенных систем. Работа В.В. Меньших [18] посвящена созданию модели действий злоумышленника на охраняемом объекте с учетом возможных реакций системы защиты.

Кроме того, исследования в этом направлении отражены в ряде диссертационных работ [19–21], в которых представлены модели и средства

выявления угроз нарушения информационной безопасности. В диссертации Д.А. Якоба [22] разработана методика исследования особенностей функционирования контрольно-пропускных систем, в том числе для объектов с большими потоками посетителей.

Однако, известные модели и методы идентификации пользователей в основном разрабатываются применительно к различным областям информационных технологий. Научные работы, объектом исследования которых являются системы контроля и управления доступом (СКУД), в основном затрагивают вопросы моделирования поведения потока посетителей массовых мероприятий, а также проектирования контрольно-пропускных систем с целью поиска эффективных решений по организации безопасной эвакуации. Вопросы организации процесса идентификации в СКУД ММПЛ проработаны недостаточно.

Использование СКУД [23–26] позволяет автоматизировать процесс идентификации посетителей, однако для этого требуется предварительная регистрация всех пользователей в базе данных (БД) вне зависимости от используемого набора идентификационных признаков. Наиболее распространенным способом регистрации посетителей является непосредственное обращение в подразделение ММПЛ, осуществляющее функции контроля за соблюдением пропускного режима. При этом предполагается предъявление человеком документа, удостоверяющего личность.

Учитывая, что ММПЛ характеризуются высокой плотностью потоков посетителей, применение такого способа регистрации зачастую приводит к увеличению временных затрат и, как следствие, замедлению бизнес-процессов. Такой подход обусловливает проблему подтверждения личности человека (верификации). Например, в некоторых ММПЛ в качестве документа, удостоверяющего личность, может использоваться не только паспорт гражданина РФ, но и другие, менее защищенные документы. Кроме

того, в случае посещения подобных объектов иностранными гражданами и предъявления ими паспортов других государств актуальной становится проблема проверки подлинности документов.

Одним из распространенных подходов к автоматизации процесса регистрации пользователей является применение различных вариантов удаленной регистрации, например, онлайн-сервисов, позволяющих посетителю самостоятельно внести сведения для регистрации в системе. Однако данный подход не решает проблему верификации пользователей, так как в большинстве случаев отсутствует возможность убедиться в достоверности представленной информации.

Можно сделать вывод, что в настоящее время организация процесса идентификации посетителей ММПЛ осложнена следующими проблемами:

– существующие технические средства идентификации и аутентификации (ИАФ) [27] СКУД не позволяют организовать идентификацию посетителей ММПЛ без нарушения протекающих в них бизнес-процессов;

– отсутствие представленных в литературе подходов и методик, которые бы позволяли организовать верификацию личности пользователей при удаленной регистрации в СКУД.

Особенности функционирования ММПЛ и наличие проблем с организацией контрольно-пропускного режима (КПР) на их территории обусловливают актуальность задачи по разработке методических рекомендаций, технических и технологических решений, которые позволили бы организовать удаленную регистрацию и идентификацию посетителей на подобных объектах без нарушения протекающих бизнес-процессов.

Цель исследования состоит в повышении эффективности процесса идентификации посетителей в местах массового пребывания людей за счет применения современных идентификационных признаков.

Объектом исследования являются подсистемы идентификации и аутентификации СКУД в местах массового пребывания людей.

Предметом исследования является процесс идентификации посетителей.

Достижение поставленной цели сводится к разработке нового научно обоснованного технического решения в области идентификации личности, имеющего существенное значение для усовершенствования системы обеспечения общественной безопасности страны. В связи с этим был определен следующий перечень задач:

1. Провести анализ существующих технических решений, применяемых в задаче идентификации посетителей, на предмет оценки возможности их применения в местах массового пребывания людей.
2. Разработать модель процесса идентификации посетителей в СКУД для мест массового пребывания людей.
3. Разработать методику верификации личности субъектов доступа при удаленной регистрации.
4. Разработать подход к идентификации и аутентификации посетителей в местах массового пребывания людей.
5. Разработать алгоритмическое и программное обеспечение процесса идентификации посетителей мест массового пребывания людей.

Методы исследования. Для решения поставленных задач в диссертационной работе использовались методы математического и функционального моделирования, теории множеств и теории защиты информации.

Научная новизна проведенных исследований и полученных в работе результатов заключается в следующем:

1. Разработана модель процесса идентификации в СКУД, отличающаяся необходимостью проведения верификации на этапе удаленной

регистрации и позволяющая организовать идентификацию личности посетителей мест массового пребывания людей.

2. Создана методика верификации субъекта доступа с помощью механизма доверенных лиц, позволяющая организовать подтверждение личности субъекта доступа другими зарегистрированными пользователями при удаленной регистрации.

3. Предложен подход к идентификации и аутентификации в СКУД, основанный на использовании мобильных устройств в качестве идентификаторов, отличающийся возможностью варьирования набора идентификационных данных и технологий их передачи в соответствии с требуемым уровнем защищенности объекта и позволяющий автоматизировать пропускной режим в местах массового пребывания людей.

Практическая значимость результатов. Предложенное автором методическое и программно-алгоритмическое обеспечение позволяет расширить круг достоверно идентифицируемых лиц без усложнения аппаратного обеспечения СКУД. Разработанный комплекс программ позволяет применять мобильные устройства для идентификации посетителей в СКУД мест массового пребывания людей.

Положения, выносимые на защиту:

1. Разработанная модель процесса идентификации в СКУД учитывает особенности функционирования мест массового пребывания людей и позволяет организовать идентификацию личности посетителей.

Соответствует пункту 8 паспорта специальности: Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

2. Методика верификации субъекта доступа позволяет организовать подтверждение личности субъекта доступа на этапе удаленной регистрации и обеспечить массовость применения данной процедуры.

Соответствует пункту 6 паспорта специальности: Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

3. Авторский подход к идентификации и аутентификации в СКУД позволяет автоматизировать пропускной режим в местах массового пребывания людей.

Соответствует пункту 11 паспорта специальности: Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.

Достоверность результатов подтверждается их внутренней непротиворечивостью, а также положительным эффектом от внедрения научных исследований в работу действующих предприятий.

Внедрение результатов. Результаты диссертационной работы были внедрены в деятельность ООО «Удостоверяющий центр Сибири», АО «ОЭЗ ТВТ «Томск», а также в учебный процесс ТУСУРа по дисциплинам «Основы информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности». Результаты диссертационной работы использовались при выполнении следующих проектов:

– проект «Методы и алгоритмы идентификации моделей поведения объектов информационных инфраструктур для обеспечения безопасности государства, общества и личности», поддержанный грантом РФФИ № 16-47-700350;

– проект «Разработка технологии повышения защищенности сервисов аутентификации и электронной подписи для сервис-провайдеров, предоставляющих услуги дистанционно в электронной форме, с использованием ресурсов инфокоммуникационных систем операторов подвижной связи», выполняемый в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического

комплекса России на 2014–2020 годы» по Соглашению о предоставлении субсидии № 14.577.21.0172;

– проект «Разработка и исследование методов построения информационно-безопасных систем», выполняемый в рамках базовой части государственного задания ТУСУР на 2015–2016 гг. (проект № 3657).

Личный вклад. В диссертационной работе представлены результаты, в достижении которых автору принадлежит определяющая роль. Часть опубликованных работ написана в соавторстве с сотрудниками научной группы. Диссертант принимал непосредственное участие в разработке и внедрении комплекса программ «TFAS» и «I-mob» в электронных проходных ООО «Удостоверяющий центр Сибири» и АО «ОЭЗ ТВТ «Томск». Автором предложены модель процесса идентификации, методика верификации субъекта доступа и подход к идентификации и аутентификации в СКУД мест массового пребывания людей. Постановка задачи исследования осуществлялась научным руководителем – доктором технических наук, профессором Р.В. Мещеряковым.

Апробация работы. Основные научные и практические результаты диссертационной работы докладывались и обсуждались на следующих конференциях и семинарах:

1. Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых «Научная сессия ТУСУР», г. Томск, 2013 г.
2. Томские IEEE-семинары «Интеллектуальные системы моделирования, проектирования и управления», г. Томск, 2013–2016 гг.
3. Proceedings of 2014 International Conference on Network Security and Communication Engineering (NSCE 2014), Hong Kong.
4. Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO», г. Томск, 2013 г.
5. Международный форум по практическим вопросам информационной безопасности «Positive Hack Days», г. Москва, 2013 г.

6. Межвузовская научно-практическая конференция «Актуальные проблемы инфосферы. Инфокоммуникации. Геоинформационные технологии. Информационная безопасность», г. Санкт-Петербург, 2013 г.

7. Всероссийская научно-практическая конференция «Проблемы информационной безопасности государства, общества и личности», г. Иркутск, 2014 г.

8. XIX Международный форум Международной академии связи «Формирование инфокоммуникаций нового поколения в интересах устойчивого развития», г. Москва, 2015 г.

Публикации по теме диссертации. Результаты диссертационной работы отражены в 10 публикациях, в том числе 5 публикаций в рецензируемых журналах из перечня ВАК, 5 публикаций в сборниках трудов конференций.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка использованных источников и литературы из 109 наименований. Общий объем работы составляет 140 страниц, в том числе 33 рисунка и 21 таблицу.

1 ИДЕНТИФИКАЦИЯ ПОСЕТИТЕЛЕЙ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Неотъемлемым элементом современных систем защиты объектов различного уровня являются СКУД. Применение подобных комплексов не только позволяет предотвратить несанкционированный доступ, но и предоставляет инструментарий для контроля за поведением людей на охраняемом объекте. Интеграция СКУД с другими техническими средствами защиты позволяет организовать эвакуацию в случае чрезвычайных ситуаций.

Основной задачей СКУД является идентификация субъектов доступа, посещающих защищаемые объекты. На сегодняшний день технические возможности таких систем позволяют автоматизировать процесс идентификации, однако в большинстве случае для решения задачи подтверждения личности требуется привлечение человеческих ресурсов.

Настоящее исследование посвящено разработке методического и программно-алгоритмического обеспечения, которое позволит идентифицировать посетителей ММПЛ без нарушения бизнес-процессов защищаемого объекта.

Данная глава посвящена исследованию вопросов функционирования СКУД. Представлен анализ технических решений, применяемых на сегодняшний день в задачах идентификации личности, и дана оценка возможности применения их в ММПЛ. Рассмотрена структура и примеры реализации СКУД. При моделировании основных процессов особое внимание уделено вопросам идентификации.

В ходе анализа работы ММПЛ выделены характерные особенности их функционирования и сформулированы актуальные проблемы идентификации посетителей на объектах подобного класса.

1.1 Системы контроля и управления доступом

1.1.1 Назначение и классификация систем контроля и управления доступом

Согласно [28], комплексное обеспечение безопасности объекта определяется как деятельность по созданию условий и обеспечению ресурсами для предотвращения и уменьшения последствий от угроз различного характера. Для формирования комплексной системы защиты объекта в первую очередь необходимо разработать концепцию безопасности. В [29] подробно рассмотрены вопросы разработки и реализации концепции безопасности и показано, что в общем случае система защиты объекта должна включать в себя следующие элементы:

– физическую охрану;

– организационные мероприятия;

– технические средства обеспечения безопасности (ТСОБ).

Физическая охрана обеспечивается наличием стационарных и мобильных постов, пунктов диспетчерского наблюдения, групп оперативного реагирования.

К организационным мероприятиям в первую очередь относятся действия, направленные на обеспечение контрольно-пропускного режима (КПР), который необходим для обеспечения упорядоченного доступа сотрудников, посетителей и транспорта на территорию охраняемого объекта. Под КПР понимается комплекс организационно-правовых ограничений и правил, инженерно-технических решений, устанавливающих порядок прохода посетителей через контрольно-пропускные пункты [30].

Структура и количественный состав комплекса ТСОБ могут варьироваться в зависимости от условий функционирования объекта и количества рубежей защиты. Важным элементом каждого рубежа являются СКУД, которые позволяют обеспечивать безопасность персонала и

посетителей, а также сохранность материальных и информационных ресурсов предприятия посредством организации КПР. Подобные системы успешно применяются как на промышленных объектах, так и в жилых помещениях, офисных центрах, магазинах, на автостоянках и т.д. При этом наличие СКУД не только позволяет повысить уровень безопасности путем предотвращения несанкционированного доступа на охраняемую территорию, но и оперативно реагировать на поведение персонала и посетителей.

В соответствии с [26, 31] основными задачами СКУД являются:

– предотвращение несанкционированного доступа в контролируемые зоны с ограниченным доступом, в том числе регистрация таких событий;

– организация возможности беспрепятственного прохода (проезда) в зоны со свободным доступом;

– контроль и учет доступа посетителей на объект;

– обеспечение условий для соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта;

– интеграция с иными системами безопасности (например, автоматическая разблокировка замков на дверях при срабатывании пожарной сигнализации).

СКУД представляет собой совокупность программно-аппаратных средств, обладающих технической, информационной, программной и эксплуатационной совместимостью. Входящие в состав подобных систем устройства можно разделить на следующие группы:

– устройства считывающие (УС): считыватели карт доступа, биометрические сканеры, устройства распознавания автомобильных номеров, кодонаборные устройства и др.;

– средства обнаружения различных материалов: металлодетекторы, обнаружители взрывчатых веществ и радиационных материалов;

– устройства обработки информации: контроллеры, панели управления;

– устройства исполнительные (УИ): турникеты, калитки, шлагбаумы, электромеханические, электромагнитные и механические замки и др.;

– вспомогательные устройства: модули связи между компонентами СКУД, инжекторы питания, адаптеры и др.

Пример реализации современной СКУД представлен на рис. 1.1.

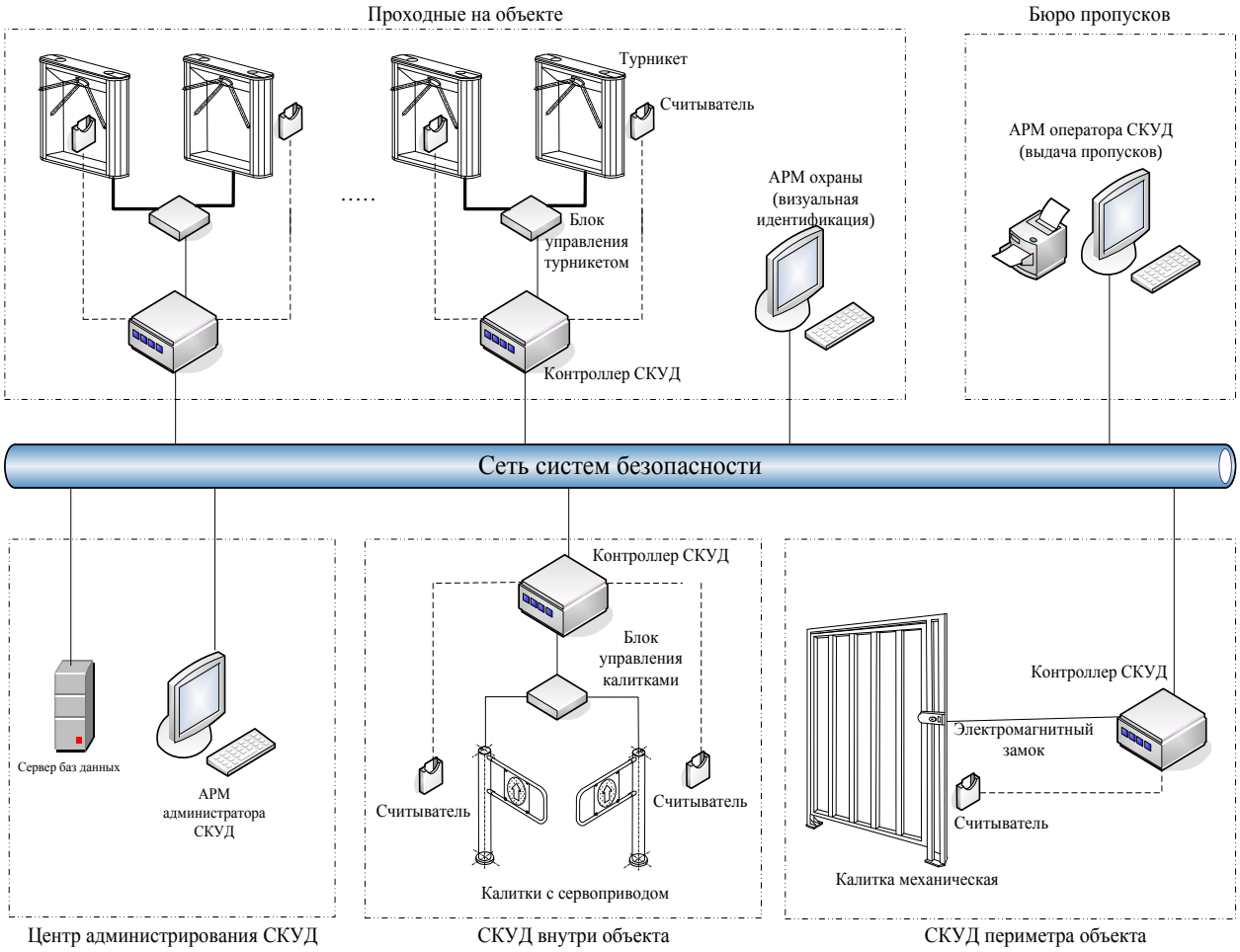

Рисунок 1.1 – Пример реализации современной СКУД

Как было сказано ранее, СКУД может быть реализована различными способами в зависимости от условий функционирования конкретного объекта и решаемых задач. В некоторых случаях могут применяться автономные СКУД для каждой точки прохода. В последнее время наиболее популярны распределенные системы, поддерживающие масштабирование при расширении контролируемой зоны. В таких случаях контроллеры доступа являются самостоятельными устройствами, осуществляющими

процесс управления с использованием специализированных удаленных интерфейсных модулей.

Деление средств и систем КУД на классы может выполняться на основе сравнительного анализа ряда функциональных возможностей. В ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом» [23] наряду с общими техническими требованиями и методами испытаний представлена классификация подобных систем по:

– способу управления;

– числу контролируемых точек доступа;

– функциональным характеристикам;

– виду объектов контроля;

– уровню защищенности системы от несанкционированного доступа.

На рис. 1.2 представлены основные способы классификации СКУД.

Рисунок 1.2 – Классификация СКУД

Автономные системы используются на объектах, где отсутствует необходимость постоянного мониторинга происходящих событий и удаленного управления ИУ. Централизованные (сетевые) СКУД применяются в случае, когда необходимо контролировать время прохода посетителей и управлять конфигурацией любой частью системы с центрального пульта. Термин «универсальные СКУД» характеризует сетевые системы, способные переходить в режим автономной работы при возникновении отказов управляющих компьютеров, сетевого оборудования или обрыве связи с контроллером. Стоит отметить, что функционал возможности автономной работы при сбоях в соединении с центральным пультом уже давно является базовым для любой сетевой СКУД. При построении универсальных СКУД выделяют централизованную, распределенную и смешанную архитектуру.

Централизованная архитектура подразумевает использование центрального контроллера, осуществляющего процесс управления с использованием специализированных интерфейсных модулей. Контроллер в системах с централизованной архитектурой хранит всю базу идентификаторов и событий, произошедших в системе. Таким образом, разделение функции принятия решений и непосредственного управления повышает уровень безопасности СКУД, поскольку сам контроллер установлен на значительном удалении от управляемого им управляемого преграждающего устройства (УПУ). При нарушении связи контроллера с управляющим компьютером система продолжает работать в автономном режиме.

Системы, построенные на базе распределенной архитектуры, содержат БД идентификаторов и событий не в одном, а в нескольких контроллерах. Они выполняют функции управления внешними устройствами и охранными шлейфами через расположенные на плате реле. Особенность типичного расположения контроллеров при распределенной архитектуре непосредственно внутри защищаемых ими

помещений не способствует снижению вероятности несанкционированного доступа (НСД) к ним. Однако при таком подходе менее критично нарушение связи между контроллером и интерфейсным модулем. Выведение из строя одного контроллера не повлияет на работу остальных, а в случае обрыва линии связи между контроллерами и компьютером система продолжает выполнять основные функции управления процессом доступа в автономном режиме.

Наиболее распространенным является подход к построению сетевых СКУД по смешанной архитектуре, подразумевающей использование специализированных считывателей с собственным буфером памяти идентификаторов и событий – «интеллектуальных» интерфейсных модулей. В основе лежит централизованная архитектура, поэтому при повреждении линии связи между центральным контроллером и интерфейсными модулями управления оконечными устройствами активируется автономный режим управления доступом с применением встроенной буферной памяти на каждом из проблемных участков. Системы, построенные с использованием данного технического решения, характеризуются высоким уровнем безопасности и надежности.

СКУД устанавливаются на объектах различных масштабов: от небольших офисов до заводов и технопарков из нескольких зданий. Широкое распространение таких систем приводит к стремительному развитию используемых в их составе технологий. Выбор и настройка систем безопасности на каждом объекте носит индивидуальный характер, так как зависит от множества различных факторов. Этим обусловлено стремление производителей СКУД к унификации используемых технологий.

1.1.2 Средства контроля и управления доступом

В соответствии с [32], средства КУД классифицируются по функциональному назначению устройств, функциональным характеристикам

и устойчивости к НСД. В табл. 1.1 представлена классификация средств КУД.

Таблица 1.1 – Классификация средств КУД

<table>
<tr><th rowspan="2">По функциональному назначению</th><th colspan="2" rowspan="2">По функциональным характеристикам</th><th colspan="2">Устойчивость к НСД (нормальная, повышенная, высокая)</th></tr>
<tr><th>К разрушающим воздействиям</th><th>К неразрушающим воздействиям *</th></tr>
<tr><td rowspan="4">Устройства преграждающие управляемые (УПУ)</td><td rowspan="4">По виду перекрытия проема прохода</td><td>С частичным перекрытием (шлагбаум, турникет)</td><td rowspan="4">Устойчивость ко взлому, взрыву и пулестойкости (только для УПУ со сплошным перекрытием проема)</td><td>Устойчивость к вскрытию</td></tr>
<tr><td>С полным перекрытием (ворота, полноростовый турникет)</td><td rowspan="3">Устойчивость к манипулированию</td></tr>
<tr><td>Со сплошным перекрытием проема (сплошная дверь)</td></tr>
<tr><td>С блокированием объекта в проеме (шлюзовая кабина)</td></tr>
<tr><td rowspan="4">Устройства исполнительные (УИ)</td><td rowspan="4">По способу запирания</td><td>Электромеханические замки</td><td rowspan="4">В зависимости от конструкции по ГОСТ Р 52582, ГОСТ Р 51053, ГОСТ 19091, ГОСТ 5089</td><td>Устойчивость к вскрытию</td></tr>
<tr><td>Электромагнитные замки</td><td rowspan="3">Устойчивость к манипулированию</td></tr>
<tr><td>Электромагнитные защелки</td></tr>
<tr><td>Механизмы привода дверей, ворот</td></tr>
<tr><td rowspan="5">Устройства считывающие (УС)</td><td rowspan="4">По способу считывания (УС)</td><td>С ручным вводом</td><td rowspan="9">–</td><td rowspan="4">Устойчивость к наблюдению для считывателей ввода запоминаемого кода</td></tr>
<tr><td>Контактные</td></tr>
<tr><td>Бесконтактные</td></tr>
<tr><td>Комбинированные</td></tr>
<tr><td rowspan="5">По виду используемых идентификационных признаков (общее для УС и ИД)</td><td>Механические</td><td rowspan="4">Устойчивость к манипулированию</td></tr>
<tr><td>Магнитные</td></tr>
<tr><td>Оптические</td></tr>
<tr><td>Электронные контактные</td></tr>
<tr><td rowspan="4">Идентификаторы (ИД)</td><td>Электронные радиочастотные</td><td rowspan="2">Устойчивость к копированию</td></tr>
<tr><td>Акустические</td></tr>
<tr><td>Биометрические</td><td rowspan="2">Устойчивость к манипулированию</td></tr>
<tr><td>Комбинированные</td></tr>
</table>

Окончание табл. 1.1

По функциональному назначению	По функциональным характеристикам	Устойчивость к НСД (нормальная, повышенная, высокая)	
		К разрушающим воздействиям	К неразрушающим воздействиям *
Средства управления (СУ) в составе аппаратных устройств и программных средств	Аппаратные средства (устройства)	–	Устойчивость защиты СВТ от НСД к информации
	Программные средства (ПО)		Устойчивость к манипулированию

*Примечание. Классификация по устойчивости к неразрушающим воздействиям: вскрытие, манипулирование, наблюдение, копирование устанавливается в стандартах и нормативных документах на средства КУД конкретного типа.

Для обеспечения полноценного функционирования и бесперебойной работы СКУД в состав подобных систем может быть включен широкий набор дополнительных средств:

- источники электропитания (в том числе резервного);
- устройства для передачи данных по различным каналам;
- преобразователи интерфейсов сетей связи;
- компьютерное оборудование и программное обеспечение (ПО);
- извещатели;
- устройства звуковой и световой сигнализации;
- доводчики и кнопки ручного управления УПУ и т.д.

На сегодняшний день нормативная база, определяющая требования, классификацию, порядок и методы испытаний систем и средств подобного класса, представлена как отечественными (ГОСТ Р 51241-2008, ГОСТ Р 50009-2000, ГОСТ 26342-89), так и международными стандартами (ISO 9000, BSI, UL, VDS, EN 50065, VDSG 29023, VDEO833 и др.).

В основе работы любой СКУД лежит принцип сравнения идентификационных признаков [33], принадлежащих или присущих конкретному физическому лицу (субъекту доступа) или объекту (предмету, транспортному средству), с информацией, хранящейся в БД системы.

В рамках данного исследования рассматриваются вопросы функционирования средств КУД, используемых для проведения идентификации субъектов доступа. Несмотря на то что в каждой конкретной СКУД перечень подобных средств различен, в общем случае они могут быть объединены в единую функциональную подсистему. Для ее обозначения введем понятие «подсистема идентификации и аутентификации» (ПИАФ).

На рис. 1.3 представлена структурная схема, отражающая взаимодействие основных элементов СКУД.

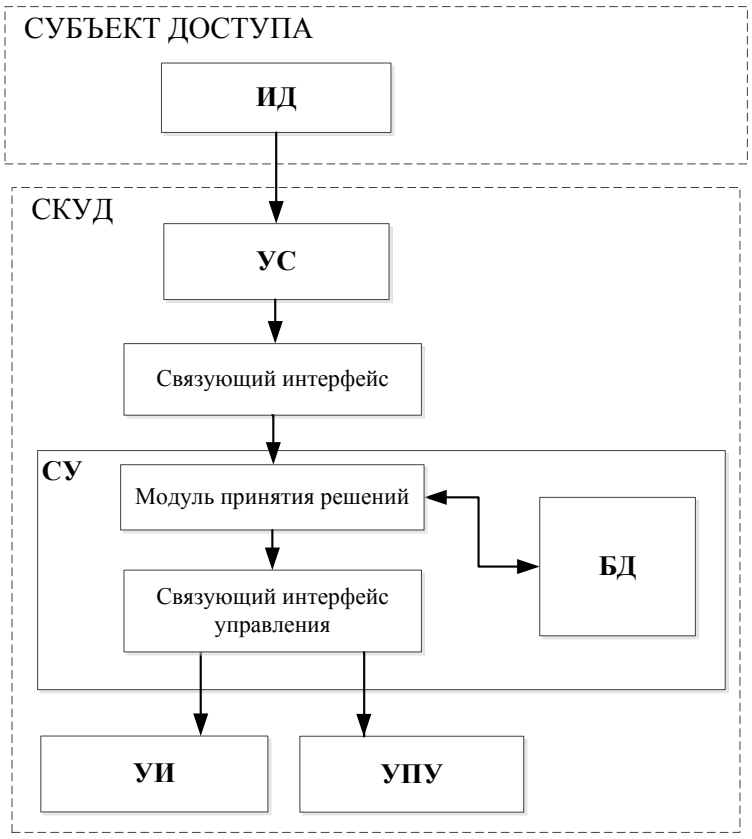

Рисунок 1.3 – Структурная схема взаимодействия элементов СКУД

Контролируемые объекты охраняемой территории, используемые для организации пунктов прохода посетителей, определяются как точки доступа и оборудуются УС, УИ, УПУ и другими необходимыми средствами. Задачи настоящего диссертационного исследования связаны с вопросами идентификации, поэтому из множества средств КУД для дальнейшего рассмотрения были выбраны УС и ИД.

1.1.3 Устройства идентификации в СКУД

Устройства идентификации предназначены для считывания и раскодирования информации, записанной на пользовательских идентификаторах разного типа, и устанавливают права людей и транспорта на перемещение в охраняемой зоне (объекте).

В рекомендациях МВД России [34] выделяются три основных принципа идентификации:

– идентификация по запоминаемому коду, вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств;

– идентификация по вещественному коду, записанному на физическом носителе (идентификаторе), в качестве которого применяются различные ключи, карты, брелоки и т.д.;

– биометрическая идентификация, основанная на определении индивидуальных физических признаков человека.

УС в общем случае должны выполнять следующие функции:

1) ввод запоминаемого кода / считывание идентификационного признака с идентификатора / считывание биометрических характеристик;

2) преобразование полученной информации в электрический сигнал;

3) передача информации в СУ (контроллер СКУД).

В табл. 1.2 приведена классификация идентификаторов доступа по виду используемых идентификационных признаков.

Таблица 1.2 – Классификация идентификаторов доступа

Вид используемых идентификационных признаков	Элемент, лежащий в основе принципа использования	Примеры идентификаторов	Примеры считывающих устройств
Механические	Элементы конструкции идентификаторов	Механические ключи с перфорационными отверстиями	Abloy SL905, Mottura 54.793
Магнитные	Намагниченные участки поверхности или магнитные элементы идентификатора	Карты с магнитной полосой, карты Виганда	Cipher MSR210U-33, Posiflex MR-2106U

Окончание табл. 1.2

Вид используемых идентификационных признаков	Элемент, лежащий в основе принципа использования	Примеры идентификаторов	Примеры считывающих устройств
Оптические	Метки, нанесенные на поверхность или расположенные внутри идентификатора, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении	Карты со штриховым кодом, топографические метки	AP-IRC, СБН–4_КМКС
Электронные контактные	Электронный код, записанный в электронной микросхеме идентификатора	Электронные ключи	ACR38U-I1, OMNIKEY® 3121
Электронные радиочастотные	Радиоканал, используемый для передачи данных	Бесконтактные карты доступа	Болид PROXY–3A, Matrix II IronLogic
Акустические	Кодированный акустический сигнал	Устройства генерации акустических сигналов	Stelberry M-70, Invensense NMP621
Биометрические	Индивидуальные физические признаки человека	Отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи	Smartec ST-FR030EMW, BioSmart PV-TS
Комбинированные	Несколько идентификационных признаков	Бесконтактная карта доступа и отпечатки пальцев	Smartec ST-FR031EM, ACR83

1.2 Процессы идентификации и регистрации в системах контроля и управления доступом

1.2.1 Формализованное описание задачи идентификации

Идентификационный признак – свойство, значение которого определенным образом характеризует субъекта доступа.

Идентификатор – это уникальный набор значений идентификационных признаков субъекта доступа, используемый для идентификации в СКУД.

В качестве идентификатора могут применяться:

– значение имени пользователя (логин);

– идентификационный номер пользователя в системе;

– номер документа установленного образца;

– учетный номер карты-идентификатора или иного устройства.

Процедура идентификации представляет собой процесс опознавания пользователя по присущим или присвоенным идентификационным признакам. При этом выполняется сравнение предъявляемого пользователем идентификатора с содержимым БД СКУД. Для осуществления данной процедуры субъект должен предварительно зарегистрироваться в системе.

Регистрация субъекта доступа подразумевает создание в БД СКУД образа его идентификатора, который в дальнейшем будет выступать эталоном для проведения идентификации.

Процедура аутентификации в общем случае представляет собой проверку подлинности идентификатора, предъявленного субъектом доступа. Проверка производится на основании аутентификатора (секрета) с использованием определенного механизма аутентификации [35, 36].

В зависимости от используемого механизма различают:

– аутентификацию на основе знания некоторой закрытой информации, которой должен обладать только легитимный субъект. Такую информацию часто называют паролем. Пароль может представлять собой текст, персональный идентификационный номер (PIN) [37], комбинацию для замка и т.д.;

– аутентификацию на основе обладания некоторым уникальным предметом – устройством аутентификации, в качестве которого могут выступать механический ключ, смарт-карта, личная печать, электронный USB-ключ и др.;

– аутентификацию на основе биометрических характеристик – уникальных физиологических признаков, например, параметров сетчатки глаза, отпечатков пальца или ладони, голоса и др.

Процедуру прохода в СКУД, построенного на базе классических электронных пропусков, можно рассматривать с разных сторон. С одной стороны, предъявление уникального пропуска можно расценивать как аутентификацию на основе обладания. С другой стороны, в данном случае электронный пропуск предъявляется в качестве идентификатора субъекта доступа, а проверка подлинности (факта легального предъявления пропуска) возлагается на контролирующий персонал.

В дальнейшем проход субъекта доступа через пропускной пункт СКУД будем рассматривать исключительно как процедуру идентификации пользователя. Вопросы аутентификации будут отражены в главе 3. Рассмотрим подробнее задачу идентификации.

Пусть в ПИАФ зарегистрировано *n* субъектов доступа. При этом в момент регистрации *i*-го субъекта доступа в БД СКУД создается образ его идентификатора p_i, который представляет собой набор эталонных значений идентификационных признаков. Тогда все зарегистрированные образы можно представить в виде множества $P = \{ p_1, p_2, \ldots, p_n \}$.

Будем полагать, что ПИАФ позволяет анализировать (распознавать) *k* идентификационных признаков субъекта доступа. Множество $Z = \{ z_1, z_2, ..., z_k \}$ включает признаки, по которым осуществляется процесс идентификации в рамках конкретной СКУД. Элементами множества *Z* могут выступать серия, номер пропуска, рабочая частота используемой технологии передачи данных, PIN-код и т.д. В случае биометрической идентификации могут применяться различные способы распознавания человека по физиологическим или поведенческим признакам. Например, идентификация может осуществляться по рисунку радужной оболочки глаза или по минуциям (уникальный для каждого отпечатка пальца признак, определяющий пункты изменения структуры папиллярных линий: окончание, раздвоение, разрыв и т.д.).

Необходимо отметить, что множество Z формируется для каждой СКУД, исходя из особенностей объекта. Образу p_i при $i = \overline{1..n}$ соответствует набор диапазонов значений идентификационных признаков z_j, $j = \overline{1..k}$, полученных на этапе регистрации i-го субъекта доступа. Обозначим такой набор как вектор $D_i = (d_{i1}, d_{i2}, \ldots, d_{ik})$, определяющий диапазоны, в которые должны попадать значения соответствующих признаков для того, чтобы i-ый субъект был идентифицирован системой.

Каждый элемент d_{ij} для j-го идентификационного признака i-го субъекта доступа представляет собой диапазон $[d_{ij_{\min}}; d_{ij_{\max}}]$. Тогда набор всех известных диапазонов может быть записан в виде матрицы D следующего вида:

$$D = \begin{pmatrix} d_{11} & d_{12} & \ldots & d_{1k} \\ d_{21} & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ d_{n1} & \ldots & \ldots & d_{nk} \end{pmatrix}.$$

В зависимости от архитектуры СКУД и типа используемой ПИАФ вектор D_i может определять не диапазоны, а конкретные эталонные значения идентификационных признаков.

На этапе идентификации субъект доступа предъявляет свой идентификатор, УС создает его образ, который используется для сравнения с образами, хранящимися в БД СКУД. Если в БД СКУД существует единственный образ, полностью соответствующий предъявленному, то субъект доступа считается идентифицированным.

Для формулирования задачи идентификации введем обозначения:

$\hat{p}$ – образ, который необходимо идентифицировать;

$\hat{z}$ – вектор считанных значений идентификационных признаков множества Z, принадлежащих образу $\hat{p}$;

$\hat{z}_j$ – считанное системой значение признака $z_j \in Z$; $j = \overline{1..k}$.

Таким образом, задача идентификации состоит в том, чтобы ответить на вопрос: соответствует ли предъявленный образ $\hat{p}$, обладающий значениями идентификационных признаков $\hat{z}$, строго одному элементу множества P.

Использование вышеприведенных определений позволяет моделировать работу любой современной СКУД независимо от типа и количества используемых идентификаторов.

1.2.2 Модель процесса идентификации в системах контроля и управления доступом

Для достижения цели диссертационного исследования необходимо разработать модель процесса идентификации в СКУД с учетом формулировки задачи, рассмотренной в п. 1.2.1. Основной целью моделирования является определение действий, требуемых для идентификации посетителя в СКУД. В п. 1.1 рассмотрены структура и принципы функционирования подобных комплексов и установлено, что их основными элементами являются субъект доступа, объект доступа (охраняемый объект), идентификатор, БД, УС, СУ, УИ, УПУ.

Для построения модели процесса идентификации был применен структурный подход, который позволяет отразить взаимодействие всех элементов исследуемого процесса путем декомпозиции. В качестве графической нотации использовалась методология IDEF0 [38]. Построение модели осуществлялось с помощью программного средства BPwin 4.0. На рис. 1.4 представлена контекстная диаграмма процедуры идентификации.

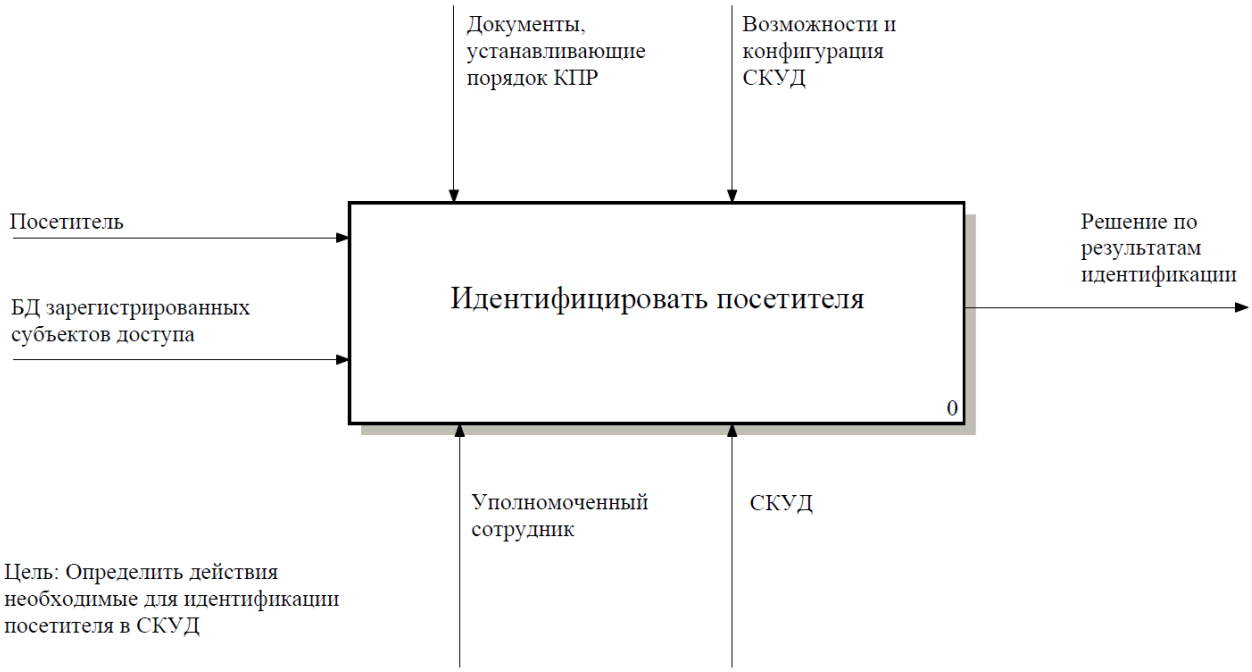

Рисунок 1.4 – IDEF0 диаграмма процесса идентификации посетителя в СКУД (уровень A-0)

Согласно диаграмме (рис. 1.4), входными данными модели являются посетитель и БД зарегистрированных субъектов доступа. В качестве основных механизмов выступают СКУД, а также уполномоченный сотрудник предприятия (оператор), в должностные обязанности которого входит обеспечение КПР. По итогам проведенной процедуры принимается решение об идентификации посетителя.

На рис. 1.5 представлена декомпозиция контекстной диаграммы, раскрывающая основные этапы процедуры идентификации посетителя в СКУД. Анализ предметной области позволил определить, что первым этапом исследуемого процесса является проверка необходимости регистрации субъекта доступа в системе (рис. 1.6).

Затем происходит предъявление пропуска, представляющего собой идентификатор пользователя. В соответствии с конфигурацией СКУД и правилами осуществления КПР с предъявленного идентификатора выделяется набор идентификационных признаков, который проходит проверку на наличие сходств с перечнем образов P.

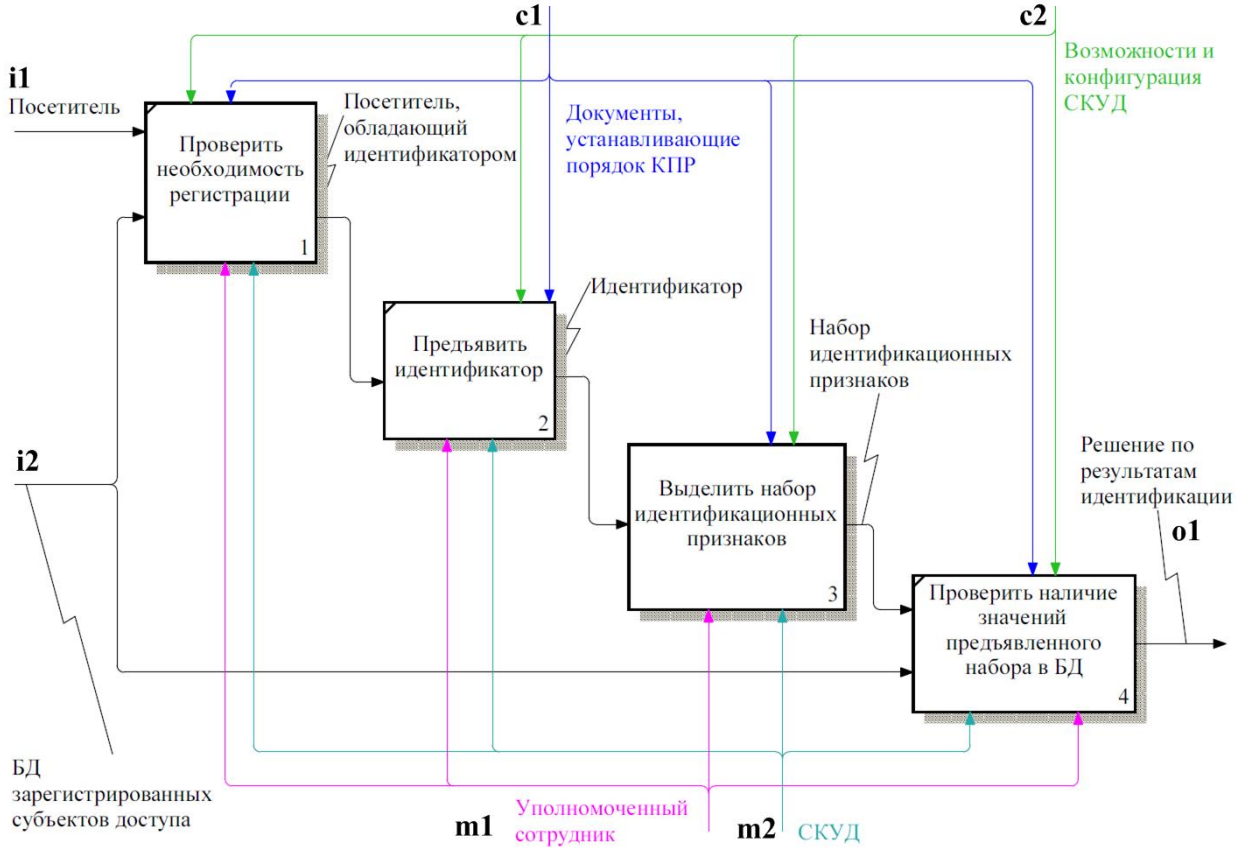

Рисунок 1.5 – Декомпозиция первого уровня IDEF0-диаграммы

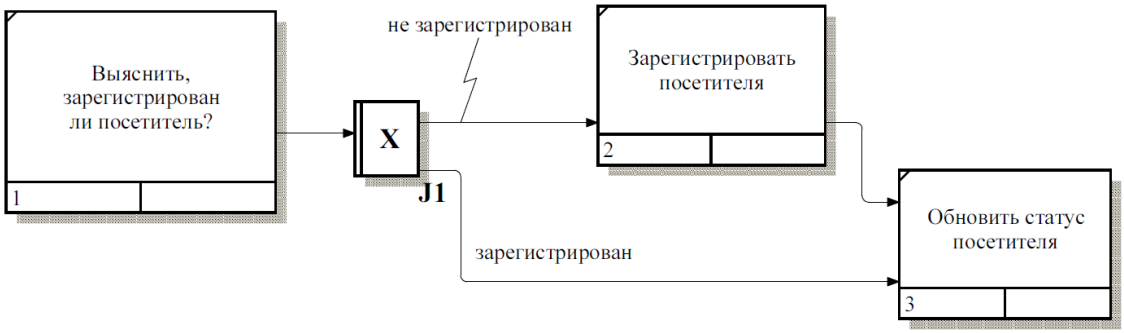

Рисунок 1.6 – Декомпозиция блока «Проверить необходимость регистрации» в виде IDEF3-диаграммы

Граничная ICOM-метка *i2* [39] на рис. 1.5 представляет собой БД зарегистрированных субъектов доступа, то есть множество *P*. Учитывая, что данное множество является частью входных данных для предложенной модели, актуальным представляется вопрос его формирования. Ранее было

определено, что образы идентификаторов p_i добавляются в БД на этапе регистрации пользователя. Более подробно данная процедура будет рассмотрена далее.

Для проведения процедуры идентификации субъект доступа должен предъявить УС образ $\hat{p}$. При этом $\hat{p}$ должен быть представлен значением как минимум одного из идентификационных признаков $z_j \in Z$. Другими словами, для идентификации необходим хотя бы один из тех параметров, которые субъект доступа может передать, а УС может принять в рамках конкретной СКУД.

Как упоминалось ранее, УС – это устройство, которое принимает и обрабатывает переданные ему образы для идентификации, а затем преобразует их в определенный формат, который может быть обработан СУ (контроллером). Тогда работу УС можно представить в виде выражения:

$$\hat{p}_k = F(\hat{p}), \tag{1.1}$$

где $\hat{p}_k$ – образ, предъявленный субъектом доступа, преобразованный в формат, используемый контроллером; F – функция преобразования образа в формат, используемый контроллером.

После выполнения преобразований УС передает контроллеру значение $\hat{p}_k$. Именно контроллер является одним из основных инструментов, позволяющих решить задачу идентификации, сформулированную в п. 1.2.2.

Для решения данной задачи введем понятие меры близости:

$Q(\hat{p}_k, p_i)$ – мера близости между образами $\hat{p}_k$ и p_i, $p_i \in P$, $i = \overline{1..n}$; (1.2)

Функцию вычисления $Q(\hat{p}_k, p_i)$ представим в виде аналитического выражения $\Phi(\hat{z}, D_i)$, позволяющего рассчитать числовую оценку критерия сравнения двух образов как оценку близости или различимости вектора считанных значений идентификационных признаков $\hat{z}$ и вектора диапазонов значений этих признаков для некоторого известного образа D_i.

Выбор вида $\Phi(\hat{z}, D_i)$ зависит от особенностей используемой системы идентификации. Например, мера сравнения может быть рассчитана с использованием расстояния Хэмминга, коэффициента парной корреляции, вероятностных оценок метода Байеса и других метрик. В ходе анализа переданного УС образа $\hat{p}_k$ контроллер проверяет, существует ли в БД соответствующий образ p_i. В случае если такой образ существует, причем в единственном экземпляре, принимается положительный результат идентификации посетителя, в противном случае субъект доступа не будет идентифицирован.

Тогда процедуру идентификации в СКУД можно представить следующим образом [40]:

$$Q(\hat{p}, p_i) = \Phi(\hat{z}, D_i),\ i = \overline{1..n}, \tag{1.3}$$

$$\hat{p} = p_i : \Phi\left(\hat{z}, D_i\right) \equiv \begin{cases} \min\left(\Phi\left(\hat{z}, D_i\right)\right), \text{если } \Phi - \text{метрика близости}, \\ \max\left(\Phi\left(\hat{z}, D_i\right)\right), \text{если } \Phi - \text{метрика различимости}, \end{cases} \tag{1.4}$$

где $p_i \in P,\ D_i \in D,\ i = \overline{1..n}$

Выражение (1.4) описывает правило, при котором отнесение $\hat{p}$ к конкретному образу p_i производится по мажоритарной оценке значения функции $\Phi(\hat{z}, D_i)$.

При этом обязательным ограничивающим условием выступают выражения (1.5) и (1.6), согласно которым идентификация представленного образа в текущей системе невозможна, в случае если в зависимости от выбранной метрики оценки значение $\Phi(\hat{z}, D_i)$ превышает (или не достигает) некоторого заданного порога λ.

$$\hat{p} \notin P : \Phi\left(\hat{z}, D_i\right) \le \lambda,\ p_i \in P,\ D_i \in D,\ i = \overline{1..n}, \tag{1.5}$$

$$\hat{p} \notin P : \Phi\left(\hat{z}, D_i\right) > \lambda,\ p_i \in P,\ D_i \in D,\ i = \overline{1..n}. \tag{1.6}$$

Условие (1.5) необходимо применять в случае использования метрики близости, а выражение (1.6) – при использовании метрики различимости.

В случае успешной идентификации пользователя и отсутствия требований выполнения процедур аутентификации осуществляется передача управляющего воздействия на УИ или УПУ. Если же политикой безопасности объекта и ПИАФ предусмотрена процедура обязательной аутентификации, то проводятся дополнительные проверки, в ходе которых проверяется подлинность предъявленного идентификатора.

На рис. 1.7 представлена схема процесса идентификации в СКУД.

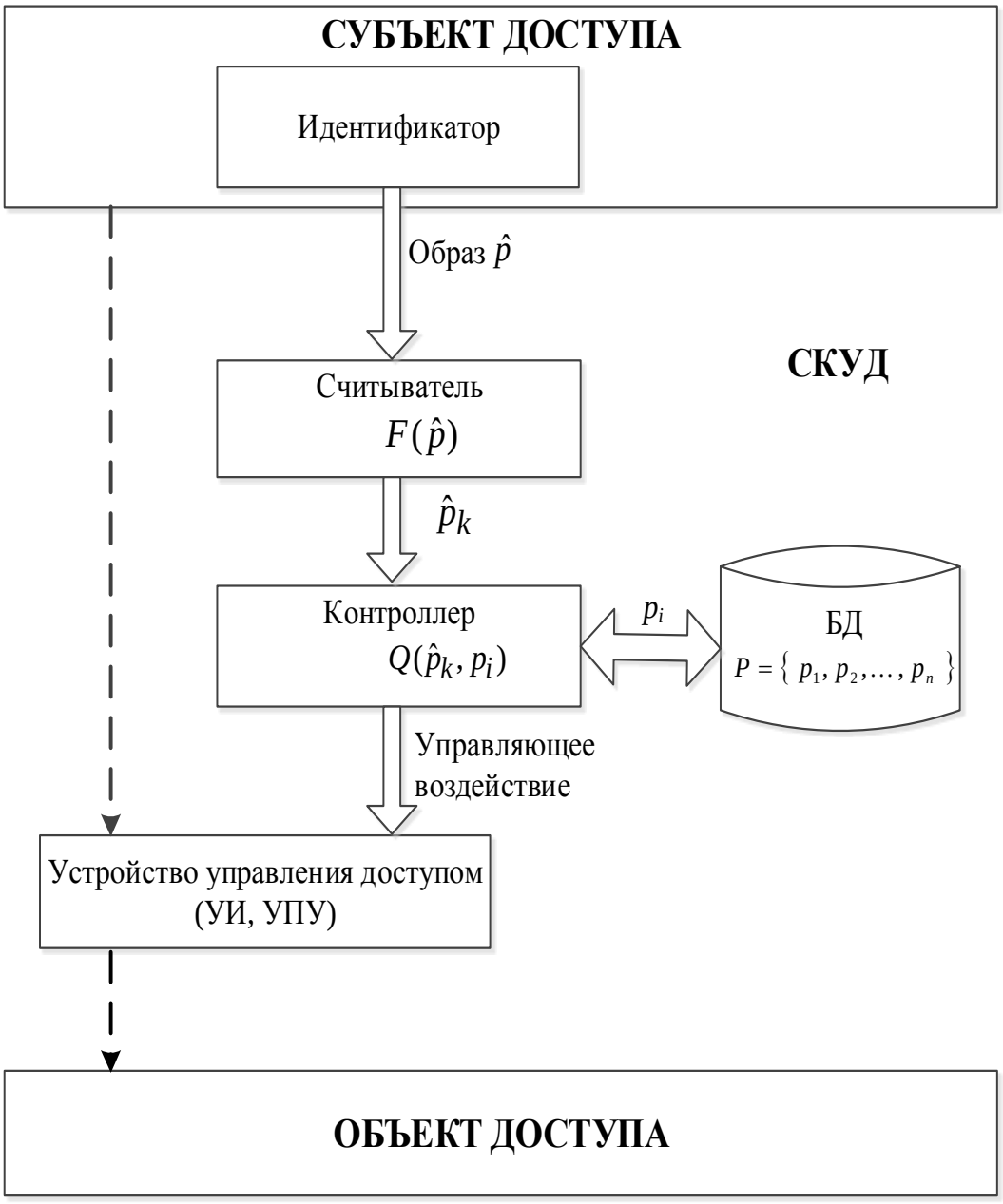

Рисунок 1.7 – Схема процесса идентификации в СКУД

Ранее было определено ранее, что регистрация пользователя в ПИАФ является неотъемлемой частью процесса идентификации. Рассмотрим декомпозицию блока «Зарегистрировать посетителя» (рис. 1.6) в виде IDEF0-диаграммы, представленной на рис.1.8. Входными данными для процедуры регистрации являются посетитель и БД зарегистрированных субъектов доступа, а в качестве основных механизмов выступают СКУД и уполномоченный сотрудник предприятия (оператор).

Оператор, выбрав параметры по которым он может идентифицировать регистрируемого, оформляет заявку на регистрацию. Получив сведения, подтверждающие личность посетителя, оператор верифицирует его (например, сравнивает внешность регистрируемого с фотографией в предъявленном паспорте) и получает значения идентификационных признаков (например, записывает в форму регистрации паспортные данные). Полученные значения проверяются на отсутствие коллизий и записываются в БД СКУД, после этого генерируется идентификатор доступа. Завершающим этапом является выдача субъекту доступа уникального идентификатора (электронной карты, RFID-метки, персонифицированного пропуска с нанесением штрих-кода и т.д.). При использования биометрических систем идентификации последний шаг отсутствует.

Одним из важнейших этапов регистрации субъекта доступа в СКУД является верификация личности (проверка указанных пользователем идентификационных данных). Как правило, эта процедура проводится уполномоченным лицом, ответственным за соблюдение КПР в организации, путем проверки документов удостоверения личности. Более подробно данная процедура рассмотрена в главе 2.

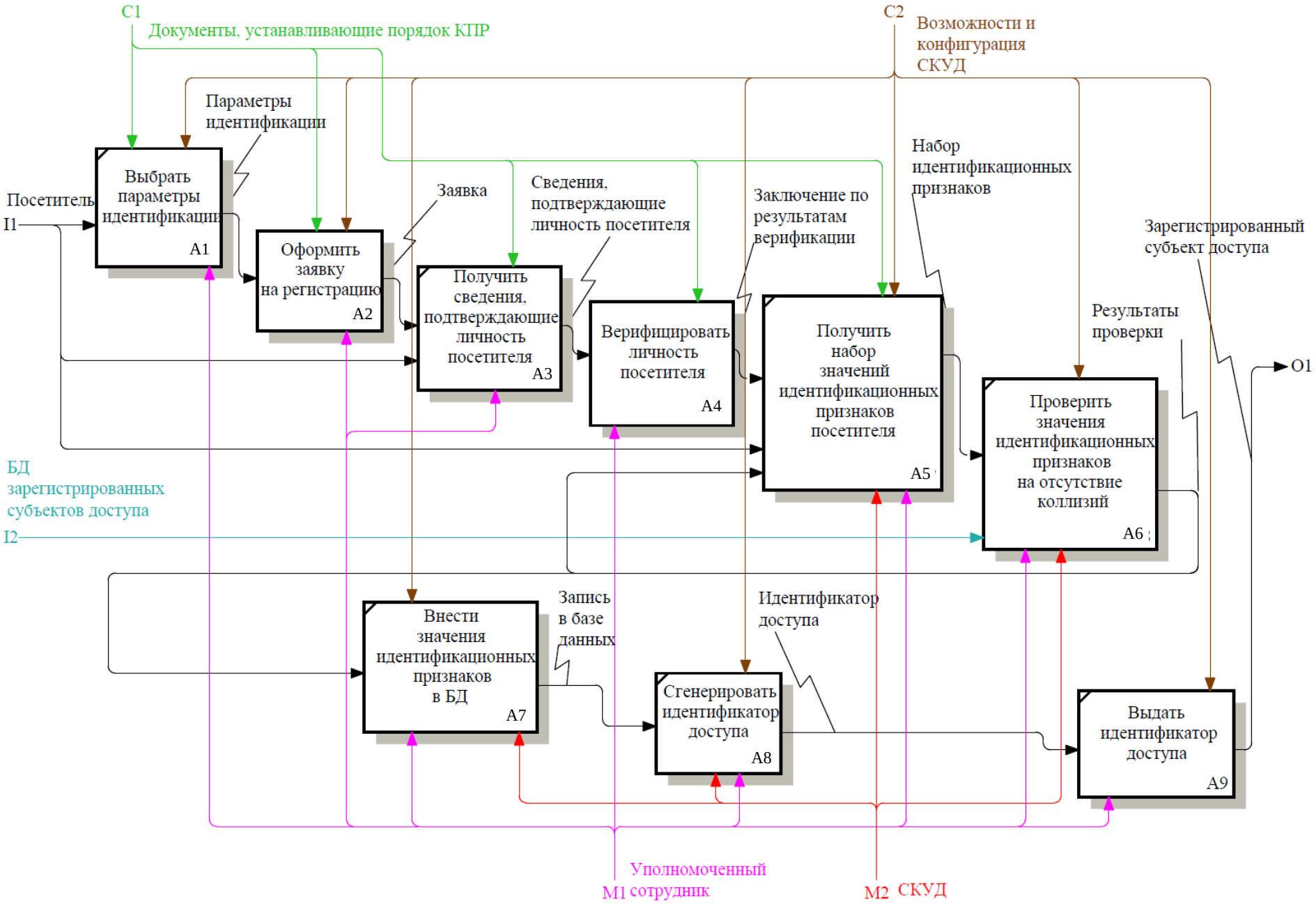

Рисунок 1.8 – Декомпозиция блока «Зарегистрировать посетителя» в виде IDEF0-диаграммы

1.3 Идентификация посетителей в местах массового пребывания людей

1.3.1 Особенности функционирования

Ранее было определено, что под ММПЛ в настоящей работе понимаются общественные места, не подлежащие обязательной охране полицией и характеризующиеся высокой плотностью человеческих потоков с вероятностью возникновения неуправляемой толпы. К подобным объектам можно отнести крупные офисные центры (площади которых арендуются множеством различных компаний), выставочные комплексы (экспоцентры), особые экономические зоны, музеи, кинозалы, театры, развлекательные комплексы, объекты гостиничной сферы и т.д.

В целях установления дифференцированных требований к обеспечению безопасности объекты подобного рода категорируются по числу одновременно находящихся людей [9]. Исходя из этого, в случае возможности одновременного пребывания более 50 человек объект (территория) относится к некоторому классу ММПЛ (рис. 1.9).

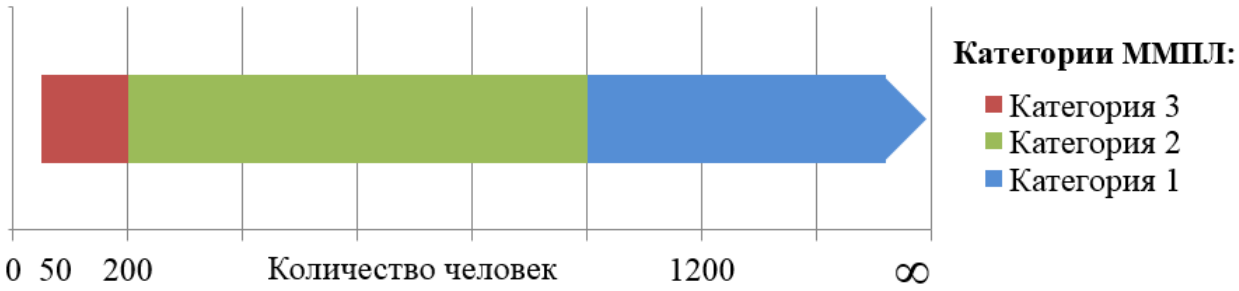

Рисунок 1.9 – Категорирование ММПЛ

Для мониторинга одновременного пребывания и (или) передвижения людей на территории ММПЛ могут применяться средства фото- и видеофиксации, фотоэлектронные световые барьеры, радарные установки, акустические сенсорные напольные панели, аэрофотосъемка, турникеты и

другие технические устройства. Мониторинг посетителей должен проводиться не только в рабочие, но и выходные (праздничные) дни.

В соответствии с требованиями законодательства на собственника ММПЛ возлагается обязанность по составлению паспорта безопасности, предназначенного для оперативного использования органами государственной власти, местного самоуправления муниципальных образований и иными субъектами, осуществляющими противодействие терроризму. Данный документ необходим для проведения мероприятий по предупреждению и ликвидации последствий актов терроризма, оказанию необходимой помощи пострадавшим и содержит данные о наличии на объекте специальных средств и сил, которые необходимы для защиты людей и материально-технической базы при наступлении акта терроризма.

Как правило, безопасность вышеперечисленных объектов обеспечивается сотрудниками частных охранных предприятий, предоставляющих услуги физической охраны. Однако отсутствие требований по обязательной идентификации личности посетителей ММПЛ значительно упрощает для злоумышленников возможности мимикрирования и беспрепятственного прохода через пункты досмотра. Кроме того, отсутствие персонифицированных сведений о посетителях подобных объектов значительно затрудняет расследование преступлений и различных инцидентов органами безопасности. Между тем, наличие вышеперечисленных данных позволило бы повысить эффективность работы силовых ведомств путем внедрения в ММПЛ средств автоматизированной проверки сведений о посетителях по БД розыска.

Каждое из ММПЛ уникально, имеет сложившиеся бизнес-процессы и характерную систему защиты объекта. Тем не менее в ходе анализа работы различных ММПЛ, а также публикаций в тематических журналах [36, 41–45], автором были выделены особенности функционирования подобных объектов. В качестве примера представлены особенности внедрения СКУД в крупных офисных центрах.

В современном офисном центре может насчитываться несколько десятков компаний-арендаторов [46]. Довольно часто крупные корпорации соглашаются арендовать необходимые им площади только при условии установки на их территории СКУД определенной марки. Это может быть обусловлено требованиями единой политики безопасности корпорации. Однако в связи с наличием других арендаторов такой подход не отменяет для администрации ММПЛ задачу по организации КПР на входе в здание [47]. Если СКУД компании-арендатора не может быть интегрирована в общую систему безопасности ММПЛ, то субъектам доступа придется пользоваться несколькими идентификаторами.

Конечно, в большинстве случаев арендаторы соглашаются на использование той СКУД, которую им предложила управляющая компания. При таком подходе актуальным становится вопрос финансирования затрат на выпуск и обслуживание идентификаторов. Учитывая большой поток посетителей ММПЛ и, как следствие, значительный оборот используемых пропусков, арендодателю в большинстве случаев приходится возлагать эти затраты на арендаторов, что отражается на общей стоимости аренды.

Стоит отметить, что в крупных бизнес-центрах в течение рабочего дня контролирующий персонал ежеминутно испытывают серьезную нагрузку при обработке информации о посетителях, временных сотрудниках, сменах авторизаций постоянных пользователей и т.д. Большой поток посетителей ММПЛ не позволяет охраннику-контролеру максимально полно сконцентрироваться на его прямых задачах, не отвлекаясь на посторонние воздействия.

Очевидно, что рассматриваемые в данном исследовании ММПЛ как класс объектов характеризуются рядом особенностей функционирования, накладывающих значительные ограничения на применение традиционных подходов по интеграции СКУД.

1.3.2 Проблемы идентификации посетителей

Несмотря на то, что на сегодняшний день существует множество способов и механизмов идентификации пользователей в сети Интернет, в большинстве случаев установить реальную личность не представляется возможным. Это приводит к затруднениям в расследовании правонарушений, а учитывая сложившуюся геополитическую обстановку, может быть использовано злоумышленниками для дестабилизации общества и создания угроз общественной безопасности.

В июле 2016 г. были внесены изменения в федеральный закон № 35-ФЗ «О противодействии терроризму» [12] и отдельные законодательные акты Российской Федерации в части установления дополнительных мер по обеспечению общественной безопасности. Правительству и ФСБ России даны поручения, касающиеся проработки и утверждения следующих вопросов:

– порядок сертификации средств шифрования при передаче сообщений в сети Интернет, а также установление норм ответственности за использование на сетях связи несертифицированных средств кодирования (шифрования);

– порядок передачи ключей шифрования в адрес уполномоченного органа в области обеспечения безопасности РФ;

– применение норм федерального закона № 35-ФЗ «О противодействии терроризму» и отдельных законодательных актов о прекращении оказания услуг связи в случае неподтверждения соответствия персональных данных фактических пользователей услуг связи сведениям, указанным в абонентских договорах.

Подобные меры еще раз подчеркивают направленность политики государства на деанонимизацию пользователей сети Интернет. Газета «Известия» опубликовала [48] высказывание заместителя главы комитета Государственной думы РФ по информационной политике Вадима Деньгина: «Мы должны идти к тому, чтобы верификация пользователей была

повсеместной. В повседневной жизни есть паспорт, и человек показывает его почти везде, и в Интернете должно быть так же. Тут нечего бояться. Это правильный шаг».

Между тем, в обычной жизни задача идентификации людей не менее актуальна, чем «виртуальном мире» интернет-ресурсов. Особенно это касается ММПЛ. Подобные объекты должны быть обеспечены системами безопасности, в том числе СКУД, позволяющими идентифицировать личность каждого посетителя.

На протяжении вот уже нескольких десятков лет основным средством идентификации в СКУД является пропуск в виде пластиковой карты. Это контактные и бесконтактные карты различных форматов и стандартов, QR- (двухмерные) и штрих-коды на физических и электронных носителях. Широкое распространение подобного рода идентификаторов объясняется главным образом их низкой стоимостью, а также универсальностью – карты доступа легко добавлять в любую уже существующую СКУД. Кроме того, smart-карты (например, класс MIFARE) [49], благодаря наличию встроенной памяти, используются для сторонних приложений: муниципальных транспортных систем, программ лояльности и пр. Однако карты доступа имеют ряд существенных недостатков, которые в значительной мере снижают эффективность контроля и учета потоков посетителей и сотрудников. Ниже представлены недостатки наиболее распространенных технических решений для идентификации в СКУД.

Потеря / передача карты доступа

Применение электронных карт доступа или другого вида физических идентификаторов при большом потоке посетителей, характерном для ММПЛ, порождает проблему проверки фактов нелегального предъявления идентификатора. Обычно эта задача возлагается на охранников-контролеров. Зачастую контролирующий персонал либо игнорирует подобные нарушения, либо физически не может отслеживать факты использования зарегистрированных пропусков сторонними (неавторизованными)

посетителями. С одной стороны, пользователь может целенаправленно передать свой идентификатор сторонним лицам. С другой стороны, пользователь может потерять карту доступа. При этом существует большая вероятность того, что нашедший ее злоумышленник сможет определить, куда и когда данный пропуск предоставляет доступ.

Клонирование карты

Серьезной проблемой карточных идентификаторов является техническая возможность их клонирования. Самый распространенный в нашей стране стандарт бесконтактных карт EM-Marine [50] (по оценкам экспертов, от 60 до 70% всех СКУД задействуют именно его для идентификации) вообще не имеет защиты от несанкционированного считывания и последующего клонирования.

Также популярным является семейство карт MIFARE на базе чипов производства NXP Semiconductor. Для шифрования данных в них используются лицензионные проприетарные криптоалгоритмы. Примерами подобных ИД являются MIFARE Plus или MIFARE DESfire EV1. Однако на практике системы безопасности, реализованные с использованием карт этих стандартов, встречаются в основном на крупных предприятиях по причине их высокой стоимости. Стандарт MIFARE Classic более популярен, в том числе и благодаря возможности производить карты на базе неоригинального чипа, совместимого с протоколами NXP. Стоимость таких продуктов близка к EM-Marine. Стоит отметить, что защита этих карт была взломана при помощи реверс-инжиниринга в 2008 г. Поэтому, имея технические средства, злоумышленник сможет на небольшом расстоянии считать данные карты и восстановить их на другой карте.

Недостатки биометрических систем

Большинство недостатков СКУД, построенных с использованием карт доступа, могут быть устранены посредством применения биометрических терминалов. Пользователь не имеет возможности сознательно передать свой

биометрический идентификатор третьему лицу или потерять его. Кроме того, задача дублирования и воспроизведения биометрических признаков на другом носителе является сложно реализуемой. Но сам принцип работы биометрических терминалов создает ряд сложностей, препятствующих их повсеместному распространению. Удельный вес биометрических систем в общей массе установленных и эксплуатируемых СКУД остается незначительным. Особенно это касается исследуемой предметной области – объектов ММПЛ. Устройства, в основе которых лежит распознавание биометрических признаков (дактилоскопия, геометрия руки, лица, венозного рисунка, радужной оболочки глаза и др.) в несколько раз превышает стоимость считывателей карт доступа [51]. Большинство заказчиков предпочитают работать с карточными ИД, несмотря на все их недостатки.

В СКУД, использующих карты доступа, сопоставлением предъявленного идентификатора и БД образов занимается контроллер. Считыватель лишь транслирует полученный номер карты для обработки. В подавляющем большинстве биометрических систем мэтчинг (процесс сравнения) выполняется самим считывателем или терминалом. После успешной процедуры мэтчинга возможен один из двух вариантов:

1) терминал сам принимает решение относительно допуска / задержания пользователя и таким образом выполняет функцию контроллера (управление замком может происходить через встроенное реле);

2) терминал формирует пакет данных и отправляет его на сторонний контроллер СКУД для обработки.

Первый вариант является очень популярным: большинство терминалов имеет возможность сетевого подключения и реле управления замками. Все, что необходимо для получения законченной СКУД, – это ПО для добавления и удаления пользователей и настройки правил и алгоритмов доступа. Практически все производители терминалов предлагают собственный программный продукт, но, как правило, он обладает весьма скромным функционалом и подходит исключительно для внесения новых

пользователей в БД или организации доступа в небольшом офисе. Полноценную СКУД на его базе построить невозможно, не говоря уже об интеграции в нее сторонних комплексов, например, видеонаблюдения или охранной сигнализации. В связи с этим, подобные решения подходят исключительно для небольших систем с ограниченным числом пользователей, что не удовлетворяет общим принципам функционирования ММПЛ.

Эксплуатация биометрических средств идентификации в составе СКУД однозначно предполагает второй вариант. В этом случае биометрический терминал выступает в роли контроллера СКУД как обычный считыватель, выдающий информацию об идентификаторе (большинство современных терминалов работают по протоколу Wiegand). Однако, стоит отметить, что процедура мэтчинга производится самим считывателем. Другими словами, оператору системы необходимо добавлять / удалять биометрические ИД во все считыватели посредством ПО терминалов, а выполнять повседневные задачи, связанные с контролем доступа, – с помощью ПО СКУД. Можно предположить, что для объектов с минимальной текучкой кадров и отсутствием сторонних посетителей этот вариант приемлем. Но применять подобную схему в ММПЛ, характеризующихся необходимостью регулярного изменения БД пользователей, невозможно.

Кроме того, актуальным является вопрос обеспечения безопасности биометрических персональных данных. Потенциальные пользователи подобных систем могут негативно относиться к процедуре сбора отпечатков пальцев или других параметров для идентификации. Нужно четко разграничивать криминалистическую биометрию и электронные системы доступа, основанные на распознавании биометрических характеристик. В последнем случае система, как правило, не хранит шаблон (например, дактилоскопический отпечаток) в чистом виде. В процессе добавления пользователя в систему сканер действительно получает изображение того

или иного признака. В зависимости от терминала это рисунок дуг, завитков и петель на коже пальца, структура сетки вен, геометрия ладони с расставленными пальцами и т.д. Однако в дальнейшем происходит процесс извлечения из него опорных данных, таких как расстояние между определенными точками на отпечатке пальца, которые после оцифровывания не имеют ничего общего с оригиналом. Какие именно опорные данные служат для создания виртуального образа идентификатора – информация обычно закрытая и используется каждым конкретным производителем как часть проприетарного алгоритма. Восстановить оригинальный рисунок, даже получив доступ к цифровому шаблону, невозможно. И хотя каждый производитель терминалов прилагает много усилий для объяснения этих тонкостей, сознание того, что кто-то может завладеть личными данными, часто отталкивает заказчика от выбора в пользу биометрии.

Также серьезным недостатком биометрических терминалов является аспект гигиены. Существует большое количество техник бесконтактного сканирования биометрических параметров, но все же подавляющее большинство систем реализовано на контактном дактилоскопическом принципе (ввиду широкого распространения и невысокой стоимости применения данной технологии).

Верификация пользователя при регистрации

Вне зависимости от используемого набора идентификационных признаков, любая СКУД требует предварительной регистрации субъектов доступа в БД. Традиционным способом регистрации является непосредственное обращение потенциального посетителя в подразделение, осуществляющее функции контроля за КПР. При этом предполагается проведение процедур проверки личности регистрируемого по документам. На рис. 1.10 представлен порядок регистрации учетной записи субъекта доступа в СКУД третьим лицом – уполномоченным сотрудником контролируемого объекта.

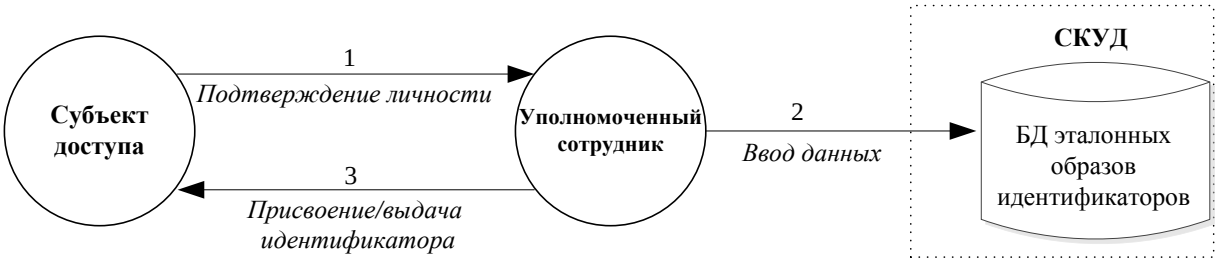

Рисунок 1.10 – Последовательность действий при регистрации субъекта доступа уполномоченным сотрудником контролируемого объекта

Приведенная на рис. 1.10 традиционная схема регистрации относит СКУД к классу систем с неполной степенью автоматизации [52], выраженной в необходимости очного посещения субъектом доступа подразделения, отвечающего за организацию КПР. Анализ предметной области позволяет утверждать, что применение подобного подхода к регистрации пользователей неприменимо для ММПЛ.

1.3.3 Адаптация модели процесса идентификации в СКУД для мест массового пребывания людей

Рассмотренные ранее особенности функционирования ММПЛ обусловливают наличие проблем с организацией КПР на их территории при использовании СКУД. Ниже рассмотрены предложения автора, позволяющие адаптировать представленную в п. 1.2.2 модель для ее применения в ММПЛ.

Применение традиционной процедуры регистрации и выдачи пропуска требует необходимости предварительного посещения объекта. Многие ММПЛ подразумевают наличие большого потока людей, заинтересованных в однократном посещении объекта. Очевидно, что для таких посетителей нецелесообразно требовать отдельного прибытия на объект с целью получения одноразового пропуска, поэтому зачастую данная

процедура проводится непосредственно в момент посещения объекта. В то же время, основной отличительной характеристикой ММПЛ является наличие больших человеческих потоков, что значительно затрудняет процесс регистрации и выдачи пропуска непосредственно на проходной и приводит к замедлению бизнес-процессов. В связи с этим администрация объекта становится перед выбором – увеличивать штатную численность персонала либо принимать во внимание высокую вероятность ошибок при регистрации посетителей, связанных с человеческим фактором. В большинстве ММПЛ отсутствует возможность обеспечения КПП необходимым количеством сотрудников для осуществления регистрации и выдачи пропусков. Таким образом, процедура регистрации субъектов доступа в ММПЛ должна быть предельно автоматизирована в целях оптимизации необходимого объёма привлекаемых человеческих ресурсов. В качестве решения данной проблемы автором предлагается предусмотреть возможность использования удаленной регистрации субъектов доступа. Такой подход повлечет за собой исключение механизма «M1» из диаграммы, представленной на рис. 1.8. Другими словами, все действия на этапе регистрации должны проводиться удаленно и без привлечения оператора.

Использование удаленной регистрации в СКУД порождает проблему проверки личности посетителя. На сегодняшний день некоторые объекты, например, современные выставочные комплексы, оборудованы СКУД, предоставляющими возможность удаленной регистрации. Однако, такие системы не предусматривают процедуру верификации (блок «A4» на рис. 1.8). В приложении 4 приведена IDEF0-диаграмма процедуры удаленной регистрации без подтверждения личности. Учитывая, что исключение верификации ставит под сомнение эффективность дальнейшей идентификации, то использование удаленной регистрации в ММПЛ возможно только при условии сохранения процедуры подтверждения личности.

Также было отмечено, что использование СКУД в ММПЛ обусловливает проблему оперативного управления и обслуживания идентификаторов. В случае выхода из строя бесконтактных карт доступа, широко применяемых в СКУД, пользователям необходимо посетить объект для перевыпуска пропуска. Очевидно, что особенности функционирования ММПЛ требуют упрощения данной процедуры. Кроме того, для ММПЛ актуальным является вопрос финансирования затрат на выдачу пропусков и обеспечения безопасности в целом (затраты на эмиссию карт, оплату труда охранников-контролеров и т.д.). Поэтому автором предлагается адаптировать модель процесса идентификации путем разработки требований к блоку «A8» диаграммы, представленной на рис. 1.8. Требования заключаются в обеспечении возможности генерации идентификаторов, которые можно было бы использовать без необходимости выдачи субъекту доступа отдельного физического носителя (предмета). Это позволит обеспечить оперативную модификацию и блокировку пропусков. Такая возможность может быть реализована за счет использования информационных технологий, позволяющих снизить финансовые затраты на выдачу пропусков путем применения идентификационных признаков уже присущих современному человеку.

Высокая вероятность компрометации пропуска в ММПЛ (утери либо передачи его другому лицу) связана с трудностями в установлении норм ответственности за подделку, нелегальное использование пропусков и нарушение КПР. Например, зачастую договор, регламентирующий порядок использования пропусков, заключается с юридическим лицом, а фактически пропусками пользуются физические лица, с которыми у администрации ММПЛ нет никаких соглашений. Поэтому используемые технологии транспорта идентификационных данных должны предусматривать

проведение аутентификации для обеспечения необходимого уровня защищенности ММПЛ.

Таким образом, модель процесса идентификации в СКУД ММПЛ должна обеспечивать выполнение следующих требований:

1) использование удаленной регистрации субъектов доступа как решение проблемы предварительной выдачи пропусков;

2) наличие механизмов проверки личности с минимальным привлечением контролирующего персонала ММПЛ на этапе удаленной регистрации;

3) отсутствие необходимости выдачи физических идентификаторов как решение проблемы оперативного управления и обслуживания ИД;

4) использование современных информационных технологий, позволяющих снизить финансовые затраты на выдачу пропусков путем применения идентификационных признаков уже присущих современному человеку;

5) использование технологий транспорта идентификационных данных, предусматривающих проведение аутентификации для обеспечения необходимого уровня защищенности ММПЛ.

Учет данных положений позволяет адаптировать модель процесса идентификации в СКУД для применения в ММПЛ, путем исключения механизма оператора из диаграммы процедуры регистрации (рис. 1.11).

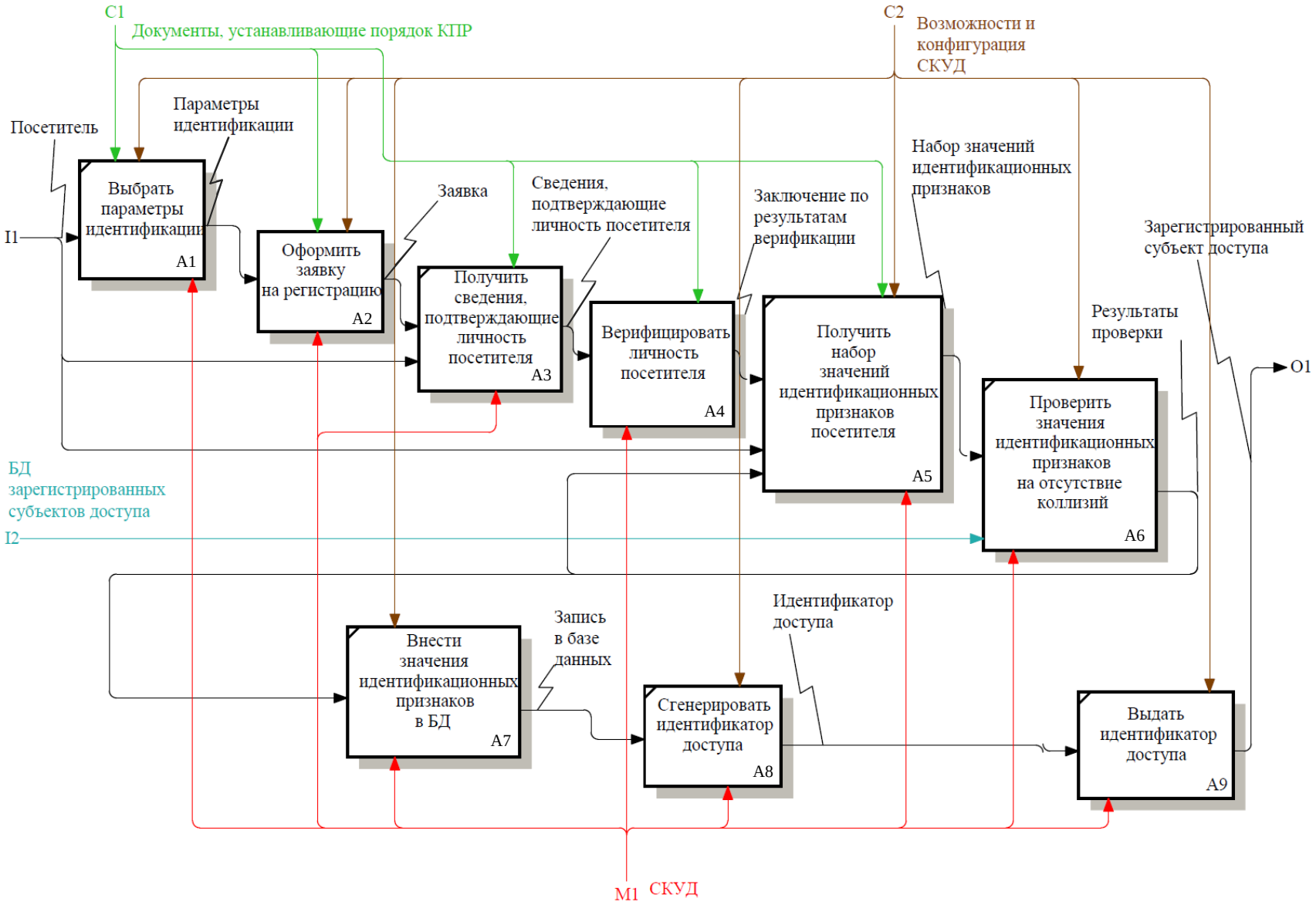

Рисунок 1.11 – Декомпозиция блока «Зарегистрировать посетителя» в виде IDEF0-диаграммы

1.4 Выводы

Данная глава посвящена исследованию вопросов функционирования СКУД и особенностей их применения на объектах, для которых характерно большое количество посетителей. Представлена классификация идентификаторов доступа и проведена оценка возможности применения их в исследуемой предметной области. Определено место СКУД в комплексной системе защиты объекта, рассмотрена архитектура подобных комплексов и примеры реализации.

Автором дано формальное описание задачи идентификации разработана модель данного процесса для СКУД. Моделирование основных процессов СКУД позволило установить, что информация, хранящаяся в БД, является входными данными для процедуры идентификации. В связи с этим подлежит рассмотрению вопрос формования БД СКУД, а именно регистрации субъектов доступа в системе. Таким образом, актуальной является задача разработки методических рекомендаций, технических и технологических решений, которые позволили бы автоматизировать процесс регистрации посетителей.

В ходе исследования были сформулированы основные проблемы современных технических решений идентификации посетителей на объектах подобного класса. Автором была проведена адаптация модели процесса идентификации в СКУД для возможности ее применения в ММПЛ.

Рассмотренные особенности функционирования ММПЛ и наличие проблем с организацией КПР на их территории обусловливают актуальность задачи выявления современных идентификационных признаков, которые бы позволили решить задачу идентификации посетителей на подобных объектах без нарушения протекающих бизнес-процессов.

В следующей главе рассматриваются вопросы разработки методического обеспечения процесса верификации личности регистрируемого пользователя.

2 МЕТОДИКА ВЕРИФИКАЦИИ СУБЪЕКТА ДОСТУПА НА ОСНОВЕ МЕХАНИЗМА ДОВЕРЕННЫХ ЛИЦ

В предыдущей главе были рассмотрены особенности функционирования ММПЛ. Установлено, что внедрение в таких объектах СКУД зачастую приводит к увеличению длительности процедуры регистрации посетителей. Причиной этого является сложность соблюдения всех требований КПР при высокой плотности потока посетителей. Процедура регистрации в СКУД подразумевает проверку документов, удостоверяющих личность, и внесение идентификационных данных в БД. Традиционно регистрация выполняется оператором подразделения, отвечающего за соблюдение КПР.

Для решения такой проблемы целесообразно применять удаленную регистрацию, предоставив посетителям возможность самостоятельно и заблаговременно оформлять заявку и получать идентификатор доступа в ММПЛ. В то же время исследования показали, что удаленная регистрация обусловливает актуальность проблемы верификации личности. В результате была поставлена задача исследовать существующие на сегодняшний день механизмы верификации, а также провести анализ их применимости в СКУД ММПЛ. По результатам анализа автором было принято решение разработать методическое обеспечение процедуры удаленной регистрации пользователей СКУД, предусматривающее возможность верификации личности без предварительного посещения объекта.

В данной главе предложена методика верификации субъекта доступа, являющаяся частью разрабатываемого методического обеспечения.

2.1 Механизмы установления личности в автоматизированных системах

В первой главе было установлено, что традиционные способы регистрации и идентификации посетителей в СКУД не могут быть применены в исследуемых объектах. Рассмотренная в п.1.3.3 модель процесса идентификации в СКУД ММПЛ определяет ряд требований к организации процедуры регистрации. Во-первых, необходимо предусмотреть возможность полностью удаленной регистрации субъекта доступа (без необходимости предварительного посещения объекта). Во-вторых, обязательным требованием является проведение процедуры верификации личности регистрируемого.

Примером реализации процедур удаленной регистрации и выдачи пропусков могут служить онлайн-системы, позволяющие зарегистрироваться на конференцию, мастер-класс, выставку и т.д. Как правило, в таких случаях идентификатором выступает сгенерированный системой и распечатанный самим пользователем билет или пропуск. Стоит отметить, что при таком подходе в большинстве случаев отсутствует возможность убедиться в достоверности представленной информации и, как следствие, подтвердить личность регистрируемого пользователя. В настоящее время существует ряд способов установления сведений о личности пользователя, используемых при удаленной регистрации в автоматизированной системе (АС).

Косвенная верификация. Данный способ верификации предполагает сбор информации об автоматизированном рабочем месте (АРМ) посетителя ресурса. Например, IP-адрес [53], переменные окружения, «Browser Fingerprint» [54], «HTTP-referer» [55] и т.д. Подобные сведения могут использоваться для установления личности регистрируемого в дальнейшем.

На рис. 2.1 представлена схема, предполагающая самостоятельную регистрацию пользователя в АС.

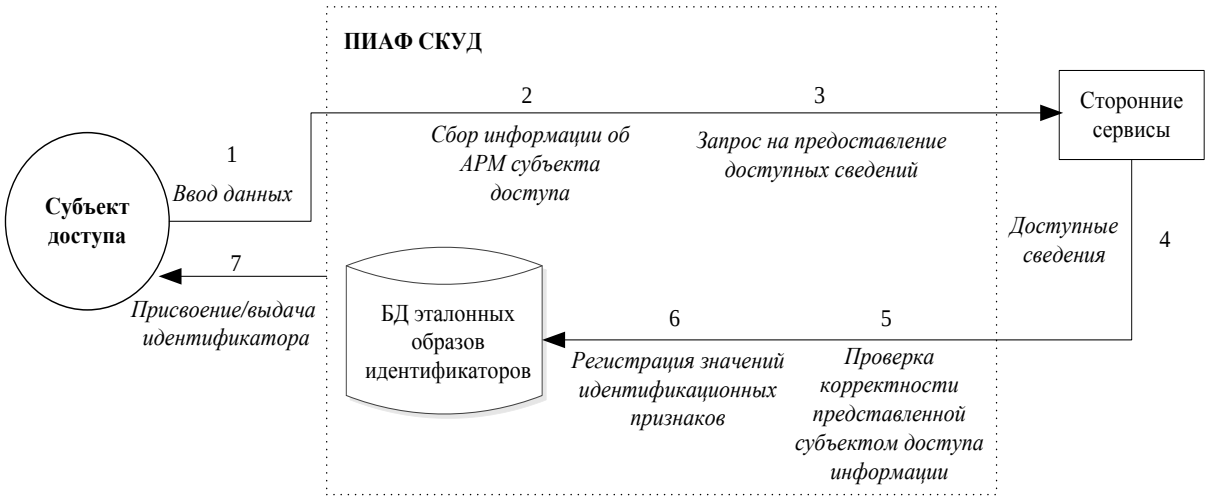

Рисунок 2.1 – Схема регистрации субъекта доступа

Для исключения ошибок и защиты от автоматических регистраций данные, указанные пользователем в регистрационной форме, подвергаются автоматизированной проверке на корректность посредством различных алгоритмов, например:

– проверка размерности введенных сведений;

– проверка контрольных значений (ИНН, ОКПО, ОКАТО и т.д.);

– тест Тьюринга (механизм CAPTCHA) [56], предназначенный для блокировки автоматических регистраций «ботами».

Если характеристики АРМ, примеры которых приведены выше, носят справочный и аналитический характер, то данные о профилях регистрируемого в социальных сетях, полученные посредством API-функций, могут быть использованы для верификации фамилии и имени пользователя. Кроме того, IP-адрес может быть использован правоохранительными органами при расследовании правонарушений и инцидентов.

На рис. 2.2 представлен обобщенный алгоритм регистрации пользователя в АС, предусматривающий косвенную верификации личности.

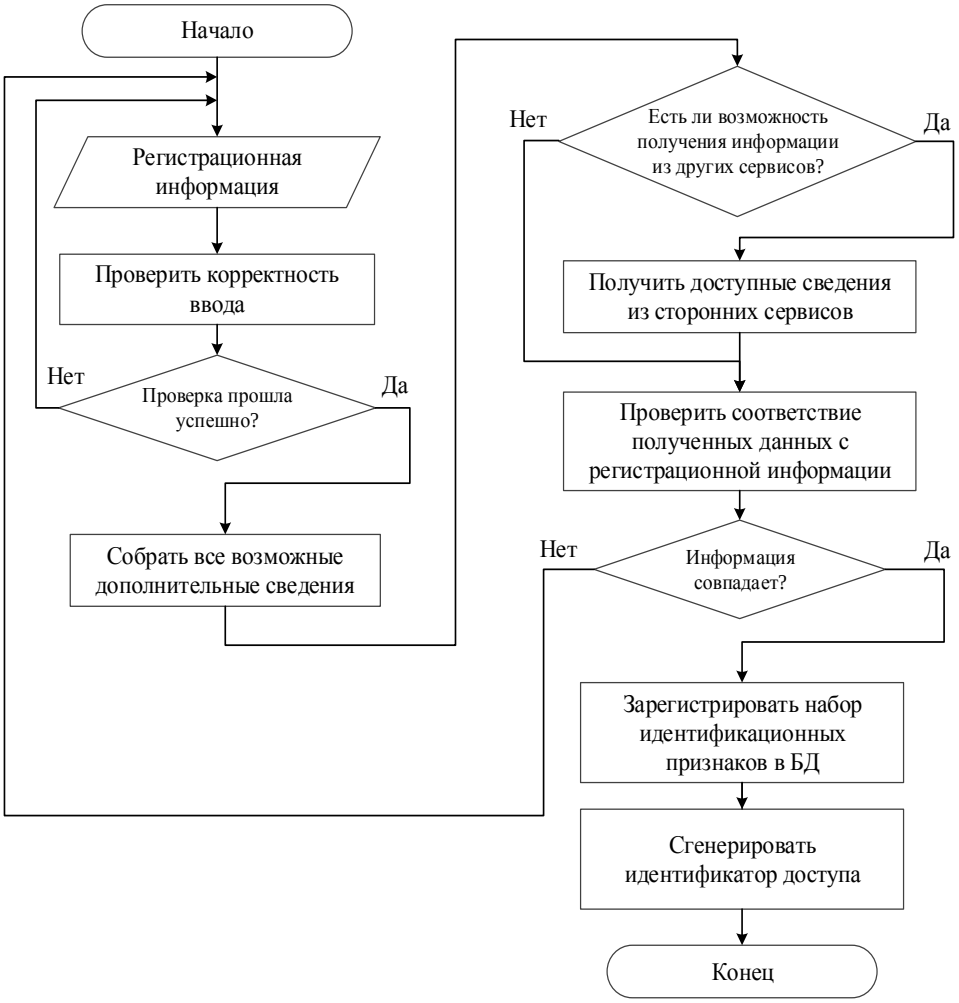

Рисунок 2.2 – Алгоритм регистрации субъекта доступа, использующий косвенную верификацию личности

Верификация с использованием доверенных систем. Одним из способов верификации является «привязка» регистрируемой учетной записи к номеру мобильного телефона путем отправки одноразового кода в виде SMS-сообщения. Такой подход нередко используется в системах многофакторной аутентификации [57] для проведения финансовых операций через системы онлайн-банков, а также для получения государственных услуг в электронной форме.

В случае с банком или государственной услугой «привязка» номера телефона как дополнительного фактора аутентификации осуществляется заблаговременно, непосредственно при посещении клиентом офиса и

предъявлении документа, удостоверяющего личность. Другими словами, процесс регистрации не является удаленным.

Необходимо отметить, что удаленная регистрация подразумевает необходимость полной отмены предварительного посещения ММПЛ. Поскольку номер телефона может быть зарегистрирован на другого человека и определить данный факт невозможно без привлечения правоохранительных органов, то применение только SMS-сообщений не является достаточным для верификации. Данное обстоятельство, вероятно, стало одной из причин поправок, внесенных в стандарт Digital Authentication Guideline [58], в части рекомендаций недопущения применения SMS-сообщений в качестве одного из элементов многофакторной аутентификации.

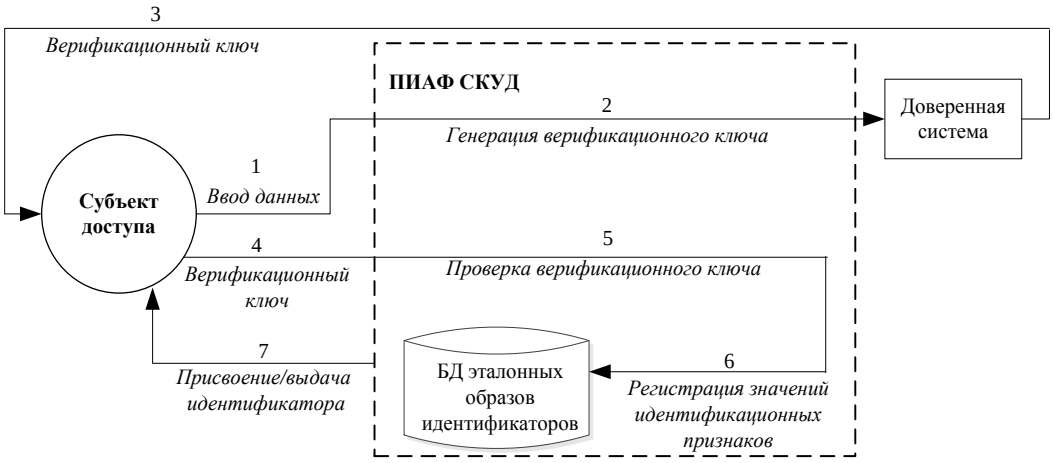

Рисунок 2.3 – Схема регистрации субъекта доступа с верификацией посредством доверенной системы (среды)

Представленная на рис. 2.3 схема регистрации широко применяется в современных электронных сервисах сети Интернет. В качестве доверенной системы зачастую выступают службы электронной почты, на которые присылается ссылка для активации аккаунта. Однако подобный подход не позволяет достоверно проверить подлинность факта принадлежности введенных сведений конкретному субъекту доступа. На рис. 2.4 представлен алгоритм регистрации, предполагающий верификацию с использованием доверенной системы (среды).

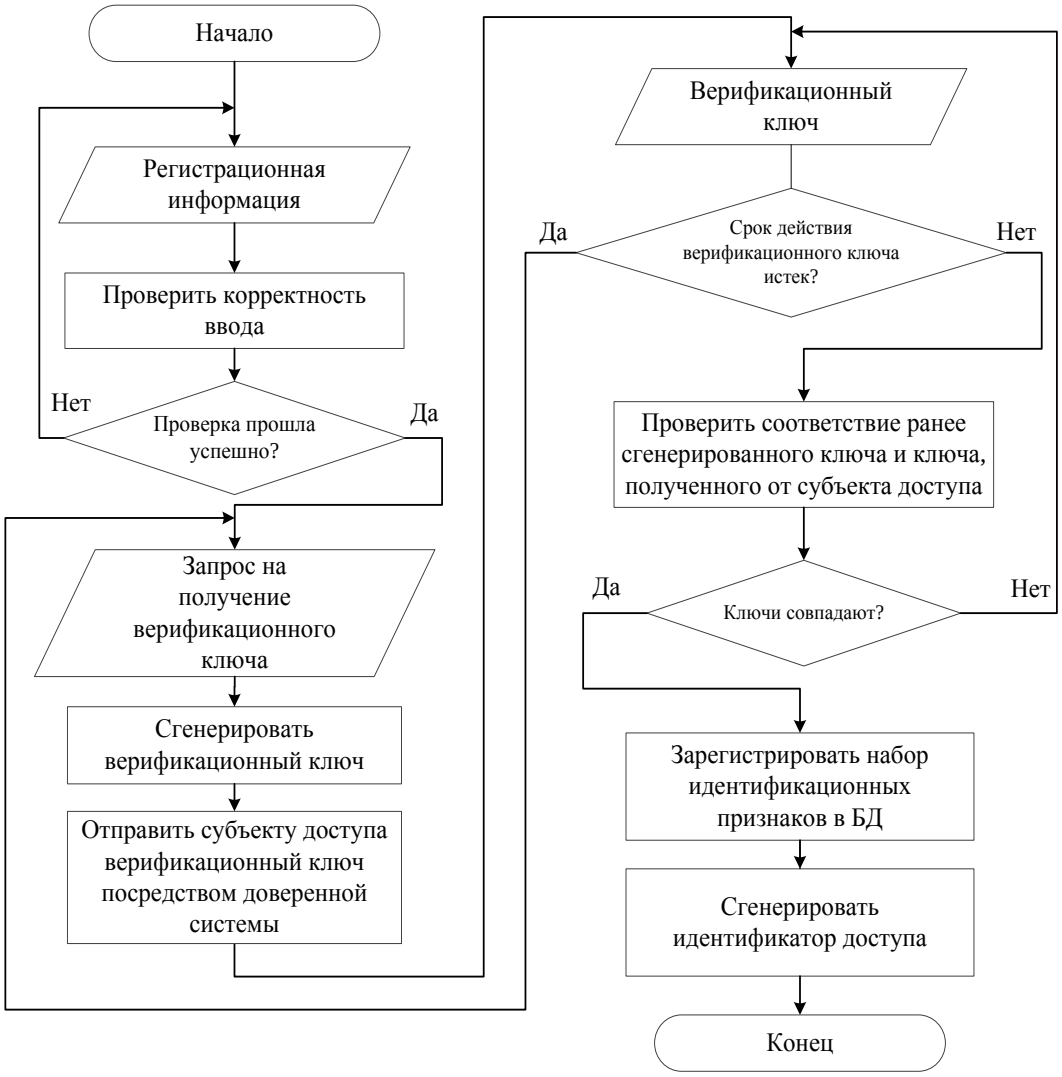

Рисунок 2.4 – Алгоритм регистрации субъекта доступа с верификацией посредством доверенной системы (среды)

Верификация с использованием провайдера единого входа. Существует возможность полной передачи функционала по верификации субъекта доступа в адрес доверенной третьей стороны – провайдера единого входа (Federated Identity [59]).

В общем случае провайдеры единого входа, использующие протоколы OpenID [59] или oAuth [60], удостоверяют не физическое лицо, а лишь связь некоторых авторизационных данных интернет-пользователя с OpenID / oAuth идентификатором (URL). Таким образом, подобные сервисы зачастую не

отменяют анонимности: при регистрации на сервере провайдера пользователь может ввести недостоверные данные.

На рис. 2.5 представлена схема регистрации субъекта в СКУД, согласно которой выдача идентификатора возможна после авторизации субъекта у провайдера единого входа.

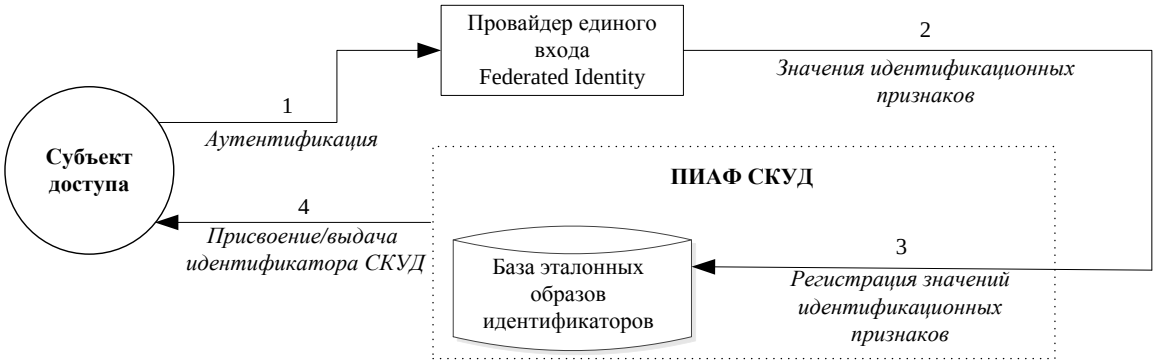

Рисунок 2.5 – Использование регистрационных сведений, предоставляемых провайдерами единого входа

На рис. 2.6 приведен алгоритм регистрации, предполагающий использование провайдера единого входа в качестве способа верификации.

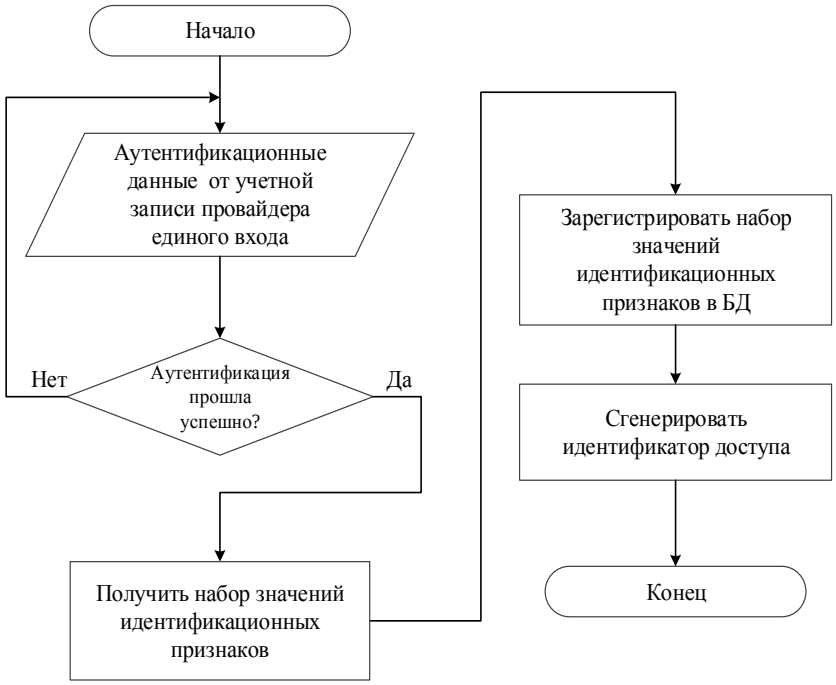

Рисунок 2.6 – Алгоритм регистрации субъекта доступа с верификацией провайдером единого входа

Примером провайдера единого входа, подразумевающим проведение верификации пользователей, является Федеральная государственная информационная система «Единая система идентификации и аутентификации» (ФГИС ЕСИА) [61]. Данная система разработана Минкомсвязи России в рамках проекта инфраструктуры электронного правительства. Цель ФГИС ЕСИА заключается в упорядочивании и централизации процессов регистрации, идентификации, аутентификации и авторизации пользователей. Одной из основных задач системы является обработка идентификационных данных: регистров физических, юридических лиц, органов и организаций, должностных лиц органов, организаций и информационных систем.

С целью обеспечения указанного функционала в ФГИС ЕСИА реализовано два альтернативных механизма интеграции:

- механизм, основанный на стандарте SAML версии 2.0 [62];
- механизм, основанный на модели OpenID Connect 1.0 [62].

Данный провайдер единого входа предусматривает три основных типа учетных записей (рис.2.7) [61]:

− упрощенная учетная запись (для ее регистрации требуется указать имя и фамилию, один из возможных каналов коммуникации), позволяющая получить доступ к ограниченному перечню государственных услуг и возможностей информационных систем;

− стандартная учетная запись (данные пользователя прошли проверку в базовых государственных информационных системах – Пенсионном фонде РФ и Главном управлении по вопросам миграции Министерства внутренних дел РФ), позволяющая получить доступ к расширенному перечню государственных услуг;

− подтвержденная учетная запись (данные пользователя прошли проверку, а его личность подтверждена одним из доступных способов), позволяющая получить доступ к полному перечню государственных услуг.

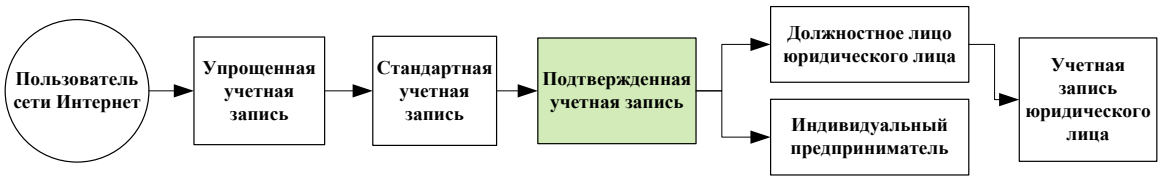

Рисунок 2.7 – Типы учетных записей и роли пользователей ФГИС ЕСИА

Для верификации пользователя (перехода к типу «подтвержденная учетная запись») требуются наличие и активация стандартной учетной записи посредством подтверждения личности пользователя одним из следующих способов:

– обратиться лично в один из центров обслуживания;

– получить код подтверждения личности заказным письмом через отделение Почты России;

– воспользоваться имеющейся универсальной электронной картой [63] или квалифицированной электронной подписью (ЭП) [64].

В соответствии с отчетом центра аналитики Минкомсвязи [65] на 22.01.2016 г., в данной системе были зарегистрированы 22,5 млн пользователей, причем только 56,5% из них имеют учетную запись, подтвержденную личным визитом в уполномоченную организацию.

Таким образом, использование функционала ФГИС ЕСИА в процедурах регистрации субъектов доступа СКУД ММПЛ является перспективным методом проверки личности пользователя в случае использования «подтвержденных учетных записей». Однако процесс верификации в ФГИС ЕСИА, т.е. получения статуса «подтвержденной учетной записи», требует длительного времени регистрации.

Существует единственный юридически значимый способ подтверждения личности субъекта доступа на этапе удаленной регистрации – удостоверять электронное заявление на регистрацию в системе с помощью ЭП. Ввиду присущего ЭП свойства неотказуемости, подкрепленного на

законодательном уровне, данный шаг будет являться гарантом достоверности всех предъявленных идентификационных данных.

Принимая во внимание, что на сегодняшний день активному использованию ЭП большинством хозяйствующих субъектов препятствуют ее цена и условия получения, можно с уверенностью утверждать, что данный способ – определенный задел на будущее, когда каждый гражданин будет иметь УЭК с квалифицированным сертификатом ключа проверки ЭП [64].

Автором проведен сравнительный анализ вышеперечисленных способов на предмет возможности их применения в ММПЛ. В качестве критериев при сравнении были выделены:

- возможность установления личности;
- возможность фальсификации сведений злоумышленником;
- возможность удаленного проведения процедуры;
- возможность использования способа нерезидентами РФ;
- массовость применения.

Перечисленный набор критериев, по мнению автора, в полной мере охватывает спектр вопросов, которые необходимо учесть при организации КПР в ММПЛ.

Под возможностью установления личности понимается способность администратора (оператора) СКУД получить паспортные данные зарегистрировавшегося человека.

Очевидно, что возможность фальсификации сведений в ходе процедуры верификации существует для любого механизма. Однако ее сложность изменяется в зависимости от используемых верификационных признаков, компетентности персонала (при наличии), проводящего процедуру, и других факторов. Сложность фальсификации оценивалась автором по шкале от 1 до 5, где:

1 – для фальсификации процедуры не требуется специальное обеспечение или знания, для передачи ложных данных используются свободные для доступа средства;

2 – фальсификация процедуры подразумевает необходимость глубоких знаний в области технологий обработки и передачи данных, используемого программного обеспечения.

3 – для фальсификации необходимо использование специализированного программного или программно-аппаратного обеспечения, глубокие знания в области технологий обработки и передачи данных.

4 – для фальсификации необходима кража данных, носителей информации, ключей доступа, а также использование специализированного программного или программно-аппаратного обеспечения, глубокие знания в области технологий обработки и передачи данных.

5 – о возможности фальсификации на сегодняшний день не имеется сведений.

Было принято, что при наличии возможности удаленной верификации пользователь не имеет необходимости предварительно посещать объект для регистрации, при отсутствии такой возможности посещение необходимо.

Так как посещение многих ММПЛ не ограничено для иностранных граждан, важно учитывать возможность использования способов регистрации, доступных для нерезидентов РФ.

Массовость способа представляет собой его доступность на сегодняшний день для использования населением независимо от места проживания, возраста, профессии, социального статуса и т.д. Чаще всего она зависит от необходимости наличия дополнительных устройств, доступа к специальным ресурсам или материальных затрат для их получения. В табл. 2.1 представлен сравнительный обзор современных решений используемых в ПИАФ АС для установления сведений о личности, на основе выделенных критериев.

Таблица 2.1 – Решения подтверждения личности при регистрации

Способ	Критерии сравнения				
	Сложность фальсификации	Установление личности	Удаленная верификация	Использование нерезидентами РФ	Массовость
Личная проверка документов, удостоверяющих личность	4 – использование чужого паспорта (изменение внешнего вида). Человеческий фактор при проверке фотографии	Да	Нет	Да	Да
Отправка кода активации на мобильный телефон	1 – использование чужих SIM-карт, услуги сервисов анонимных мобильных номеров	Да	Да	Да	Да
Отправка кода активации на указанный e-mail	2 – использование фальшивых аккаунтов в почтовых службах	Нет	Да	Да	Да
Привязка к аккаунту соц. сети	1 – использование фальшивых аккаунтов в соц. сетях	Нет	Да	Да	Нет
Запись IP-адреса	3 – использование анонимайзеров (proxy-серверы, VPN-туннели, Tor, I2P)	Нет	Да	Да	Да
Сбор «browser Fingerprint», «HTTP-referer» и прочих характеристик клиента	2 – настройка анонимизации в браузерах	Нет	Да	Да	Да
Верификация посредством платежных систем	3 – использование чужих виртуальных кошельков	Нет	Да	Да	Нет
Использование Federated Identity провайдеров (OpenID, oAuth)	2 – использование фальшивых аккаунтов у Federated Identity провайдеров	Нет	Да	Да	Нет
Использование «подтвержденных учетных записей» ФГИС ЕСИА	4 – кража аутентификационных данных от учетной записи. Кража носителя сертификата ключа проверки электронной подписи и PIN-кода	Да	Да	Да. *Множество ограничений*	Да
Применение технологий электронной подписи	4 – кража носителя сертификата ключа проверки электронной подписи и PIN-кода	Да	Да	Да. *Множество ограничений*	Нет

Использование подтвержденных учетных записей ФГИС ЕСИА, а также применение технологий ЭП удовлетворяют критериям, выдвинутым к требуемой методике установления личности регистрируемого в ММПЛ. Однако для получения возможности пользоваться этими способами

существует серьезный ограничивающий фактор – необходимость предварительного посещения уполномоченного учреждения (удостоверяющего центра, почтового отделения и т.д.).

Таким образом, возникает необходимость создания дополнительного способа, который бы наравне с указанными обеспечивал возможность верификации личности и при этом удовлетворял выдвинутым требованиям.

2.2 Механизм доверенных лиц

Автором предлагается в процедуре регистрации учетной записи пользователя в ПИАФ СКУД ММПЛ использовать подход к организации процесса верификации личности, в основу которого положен механизм доверенных лиц [66]. Подход предполагает подтверждение личности регистрируемого другими пользователями, которые лично удостоверились в правомерности совершения запрашиваемой операции и одновременно с этим наделены соответствующими привилегиями.

Одной из первых аутентификацию с использованием подобного механизма предложила исследовательская группа Джона Брэйнарда [67]. Исследователями была реализована и испытана система, использующая в своем составе социальную аутентификацию, в процессе которой личность пользователя удостоверяется другими людьми.

Успешным примером внедрения подобного механизма является действующая по настоящее время система восстановления доступа к аккаунту «Trusted Contacts», используемая в социальной сети Facebook с 2013 г. [68]. У пользователя сети есть возможность указать несколько друзей, которые могли бы подтвердить его личность с помощью специального ключа в случае блокировки аккаунта. Предполагается, что указанные пользователем лица имеют возможность позвонить или встретиться с ним лично, чтобы подтвердить легитимность запроса на восстановление доступа. По мнению администрации социальной сети, такой механизм является наиболее надежным и безопасным для восстановления доступа.

Позднее в своей диссертации А.А. Малков предложил алгоритм работы автоматизированной системы восстановления доступа к учетной записи, основанный на технологии социальной аутентификации с помощью доверенных лиц [69]. Согласно данной технологии решение о восстановлении доступа принимается на основании оценок так называемых поручителей. При этом А.А. Малков предложил дополнить механизм доверенных лиц проверкой доверенных каналов связи на этапе формирования списка поручителей и анализом активности пользователя за период времени, предшествующий обращению к системе, путем вычисления времени премодерации.

Как в случае с сетью Facebook, так и в технологии А.А. Малкова механизм доверенных лиц применяется в задачах восстановления доступа к уже существующим учетным записям. Автором же рассматривается задача верификации личности до момента создания учетной записи. Для этого предлагается провести адаптацию технологии социальной аутентификации с целью решения задачи верификации субъекта доступа при регистрации в СКУД ММПЛ.

При оценке возможности использования подхода, основанного на применении доверенных лиц, для решения поставленной задачи автор исходил из следующих положений. Во-первых, данный механизм обеспечивает возможность удаленной верификации, что позволяет провести весь процесс регистрации субъекта доступа без предварительного посещения объекта. Во-вторых, наличие контактов между посетителями и поручителями (доверенными лицами) по альтернативным каналам связи позволяет регулировать данный процесс для достижения требуемого уровня проверки достоверности данных.

В литературе на сегодняшний день не представлено методическое обеспечение, которое бы затрагивало вопросы применения данного

механизма в различных случаях. Также отсутствует методическое обеспечение, регламентирующее процесс верификации личности при удаленной регистрации пользователей в СКУД.

В связи с этим автор предпринял попытку разработать методику верификации личности субъектов доступа СКУД [70]. В ходе проводимого исследования были сформулированы основные потребности потенциальных пользователей такой методики – должностных лиц, ответственных за организацию КПР. Используемый механизм верификации должен обеспечивать:

1) возможность полностью удаленного применения без необходимости предварительного посещения объекта;

2) возможность субъектам доступа самостоятельно передавать в СКУД свои идентификационные данные в момент регистрации;

3) возможность самостоятельно задавать степень достоверности верификации в соответствии с требуемым уровнем защищенности объекта;

4) соответствие современному развитию СКУД и возможность интеграции в них.

2.3 Описание методики верификации субъекта доступа

Назначение методики

Организация процесса подтверждения личности субъекта на этапе удаленной регистрации в СКУД.

Вход: заявка на регистрацию субъекта.

Выход: решение по результатам верификации.

Термины и обозначения, используемые в описании методики

S – множество субъектов доступа;

S_1 – множество субъектов доступа, желающих получить пропуск для СКУД ММПЛ);

S_2 – множество зарегистрированных субъектов доступа;

S_3 – множество зарегистрированных субъектов доступа, наделенных привилегиями выступать гарантом при подтверждении личности некоторого $\hat{s} \in S_1$.

При этом выполняются следующие соотношения:

$$S_1, S_2, S_3 \subset S;$$

$$S_1 \cap S_2 = \varnothing;$$

$$S_3 \subset S_2.$$

VS – система верификации личности;

$\hat{s}$ – субъект доступа, личность которого подлежит верификации, $\hat{s} \in S_1$;

s – зарегистрированный пользователь, наделенный привилегиями выступать гарантом при подтверждении личности некоторого $\hat{s}$, так что $s \in S_3$, $\hat{s} \in S_1$;

S' – множество потенциальных поручителей, указанных субъектом $\hat{s}$ при регистрации, при этом $S' \subset S_3$;

Q – множество вопросов, на которые должен ответить $s \in S'$ для верификации личности $\hat{s}$, причем $Q = \{q_1, q_2, \ldots, q_n\}$, $|Q| = n$;

q_1 – вопрос о подтверждении личности субъекта $\hat{s}$;

q_i – вопрос, характеризующий компетенцию субъекта s для подтверждения личности $\hat{s}$, при чем $i = 2..n$;

d_k – оценка компетенции субъекта $s_k \in \acute{S}$ для подтверждения личности $\hat{s}$;

δ_{ij} – нормированная в диапазоне [0; 1] оценка j-го варианта ответа на вопрос $q_i \in Q$, причем $\sum_{j=1}^{Bi} \delta_{ij} = 1$, где B_i – количество вариантов ответа на вопрос q_i;

y_{ki} – оценка, соответствующая ответу субъекта $s_k \in \acute{S}$ на вопрос $q_i \in Q$;

r_k – интегральная оценка результатов ответов субъекта $s_k \in \acute{S}$;

l_1 – пороговое значение оценки d_k;

l_2 – пороговое значение, определяющее точность верификации (соответствующее одной из градаций по используемой порядковой шкале);

$g\ (R,l_2)$ – функция принятия решения о верификации субъекта доступа.

k – одноразовый верификационный ключ;

c_1 – основной канал передачи данных;

c_2 – дополнительный канал передачи данных.

Описание методики

1. В *VS* размещается заявка на верификацию личности субъекта доступа $\hat{s}$. В составе заявки содержатся значения идентификационных признаков, подлежащие проверке. Заявка может быть подана как самим субъектом доступа $\hat{s}$, так и некоторым зарегистрированным пользователем s.

2. *VS* генерирует k и передает его $\hat{s}$, используя при этом c_1.

3. $\hat{s}$, используя c_2, подтверждает получение k.

4. Если заявка была подана пользователем s – считаем верификацию успешной. Иначе организовать верификацию $\hat{s}$:

4.1 *VS* запрашивает у $\hat{s}$ список пользователей S', которые потенциально могут подтвердить личность $\hat{s}$.

4.2 *VS* отправляет в адрес $s \in S'$, указанных $\hat{s}$ на шаге 4.1, уведомления о необходимости верифицировать личность $\hat{s}$.

4.3 $s \in S'$ подтверждают личность субъекта доступа путем заполнения опросника Q.

4.4 *VS* оценивает количественное значение ответа $\hat{y}_{k1}$ по шкале Харрингтона:

$$y_{k1} = f_{\text{Harrington}}\ (\hat{y}_{k1}), \qquad (2.1)$$

где $\hat{y}_{k1}$ – ответ субъекта $s_k \in S'$ на вопрос q_1 = «Подтверждаете ли Вы личность данного субъекта доступа?»; $f_{\text{Harrington}}(x)$ – функция, преобразующая градацию порядковой шкалы Харрингтона в числовое значение (на основе табл. 2.2):

$$f_{\text{Harrington}}(x) = \begin{cases} 0{,}1, \text{ если } \lambda = 1; \\ 0{,}285, \text{ если } \lambda = 2; \\ 0{,}5, \text{ если } \lambda = 3; \\ 0{,}715, \text{ если } \lambda = 4; \\ 0{,}9, \text{ если } \lambda = 5. \end{cases} \quad (2.2)$$

4.5 *VS* оценивает компетенцию d_k субъекта $s_k \in S'$, используя нормированные оценки ответов δ_{ij} (пример оценок приведен в табл. 2.3):

Если субъект $s_k \in S'$ выбирает j-й вариант ответа на i-й вопрос, то $y_{ki} = \delta_{ij}$, $i = 2..n$, $j = 1..B_i$.

Компетенция d_k рассчитывается по формуле:

$$d_k = \frac{\sum_{i=2}^{n} y_{ki}}{\sum_{i=1}^{n} \max_j(\delta_{ij})}. \quad (2.3)$$

4.6 *VS* рассчитывает интегральную оценку r_k субъекта s_k (2.4).

$$r_k = \begin{cases} y_{1k} \cdot d_k, \text{ если } d_k \geq l_1; \\ 0, \text{ иначе.} \end{cases} \quad (2.4)$$

Всякий раз после расчета нового значения r_k *VS* проверяет условие (2.5) наличия достаточного количества ответов компетентных доверенных лиц:

$$\exists\ R = \{r_k \mid r_k \neq 0\} \text{ и } |R| \geq l_2. \quad (2.5)$$

В случае выполнения условия – переход к шагу 4.7.

4.7 *VS* принимает решение по результатам процедуры верификации субъекта $\hat{s}$ согласно функции $g(R, l_2)$:

$$g(R, l_2) = \begin{cases} \textit{Истина}, \text{ если } F_{\text{Harrington}}\left[\frac{\sum_{k=1}^{m} r_k}{m}\right] \geq l_2; \\ \textit{Ложь}, \text{ иначе.} \end{cases}, \quad (2.6)$$

где m – число оценок компетентных доверенных лиц, $m = |R|$; $F_{\text{Harrington}}(x)$ – функция, преобразующая числовое значение в одну из градаций порядковой шкалы Харрингтона (на основе табл. 2.2):

$$F_{\text{Harrington}}(x) = \begin{cases} \lambda = 1, \text{ если } x \in [0; 0,2]; \\ \lambda = 2, \text{ если } x \in (0,2; 0,37]; \\ \lambda = 3, \text{ если } x \in (0,37; 0,63]; \\ \lambda = 4, \text{ если } x \in (0,63; 0,8]; \\ \lambda = 5, \text{ если } x \in (0,8; 1]. \end{cases} \quad (2.7)$$

До тех пор, пока g принимает значение *Ложь*, считается, что пользователь не прошел процедуру верификации. При получении значения *Истина* считается, что субъект верифицирован.

На любом шаге методики возможен переход к шагу 1 – для заполнения новой заявки на верификацию.

2.4 Применение методики

Примечания к методике

1) На шаге 4.4 представленной методики для получения и обработки количественными методами качественной информации предлагается использовать вербально-числовую шкалу Харрингтона. В табл. 2.2 представлен предлагаемый состав содержательно описываемых наименований ее градаций, соответствующие им количественные значения и числовые интервалы. Данная шкала находит широкое применение в работах [71–72] и позволяет измерить степень интенсивности критериального свойства, имеющего субъективный характер.

Таблица 2.2 – Рекомендуемая к использованию шкала Харрингтона

Количественное значение	Числовые интервалы	Ответ, данный $s_k \in S'$	Условное значение λ, соответствующее уровню градации ответа
0,1	0–0,2	«Полностью уверен, что не он»	λ = 1
0,285	0,2–0,37	«Кажется, что не он»	λ = 2
0,5	0,37–0,63	«Не знаю»	λ = 3
0,715	0,63–0,8	«Кажется, что он»	λ = 4
0,9	0,8–1	«Полностью уверен, что он»	λ = 5

2) На шаге 4.5 в качестве вопросов, ответов и соответствующих им нормированных оценок, предлагается использовать данные из таблицы 2.3. Данный шаг позволяет количественно оценить компетенцию доверенного лица, т.е. способность объективно верифицировать личность регистрируемого субъекта.

Таблица 2.3 – Возможная таблица вопросов-ответов с нормированными оценками

i	Вопрос q_i	δ_{i1}	δ_{i2}	δ_{i3}	δ_{i4}
2	«Кем вам приходится пользователь?»	«Не знаю его» $\delta_{11} = 0$	«Плохо помню, откуда я его знаю» $\delta_{12} = 1/6$	«Товарищ, знакомый» $\delta_{13} = 2/6$	«Родственник / близкий друг» $\delta_{14} = 3/6$
3	«Каким способом вы убедились в личности пользователя?»	«Я не проверял личность» $\delta_{21} = 0$	«Электронная почта / мессенеджеры» $\delta_{22} = 1/6$	«Телефонный разговор» $\delta_{23} = 2/6$	«Личная встреча» $\delta_{24} = 3/6$

3) На 4.1 этапе методики *VS* предпочтительно запрашивать список по значениям некоторого идентификационного признака, например, по номеру телефона. В данном случае для эффективного поиска по множеству S_3 реализация *VS* должна включать аналитическую обработку различных форматов входных данных.

4) Для автоматизации создания множества S' рекомендуется предоставлять инструменты, позволяющие субъекту $\hat{s}$ импортировать список контактов электронной почты, телефонной книги и т.д.

5) В соответствии с результатами исследований [73] методика подразумевает привлечение не менее 3 пользователей $s \in S_2$ для подтверждения личности $\hat{s}$.

6) Для получения статуса доверенного лица $s \in S_2$ должен пройти дополнительную процедуру верификации. Ее смысл заключается в подтверждении субъектом доступа своего согласия с правилами и нормами ответственности за приобретаемые им права на подтверждение личности других субъектов. Ниже представлены варианты реализаций прохождения дополнительной процедуры верификации ММПЛ:

– письменное согласие (при очном посещении ММПЛ);

– подписание согласия средствами квалифицированной электронной подписи;

– подписание согласия в электронном виде с использованием «подтвержденной учетной записи» ФГИС ЕСИА.

Область применения

Множество рассматриваемых ММПЛ для применения методики следует разделить на 2 группы:

1 группа – объекты, в которых любое посещение должно быть инициировано некоторым заинтересованным представителем ММПЛ, т.е. подразумевается, что каждый посетитель может попасть на охраняемый объект только по приглашению принимающей стороны. Например, если в качестве ММПЛ выступает офисный центр, помещения которого сдаются в аренду, то в качестве инициатора может выступать представитель арендатора, обладающий возможностью верификации личности.

2 группа – объекты, в которых представителям ММПЛ невозможно организовать приглашения субъектов доступа. Бизнес-процессы подобных объектов построены таким образом, что представителям ММПЛ заведомо неизвестно, кто и когда решит их посетить. Примером выступают торговые центры, театры и кинотеатры, и т.д.

Алгоритм использования

На рис. 2.8 представлена блок-схема алгоритма применения предложенной методики.

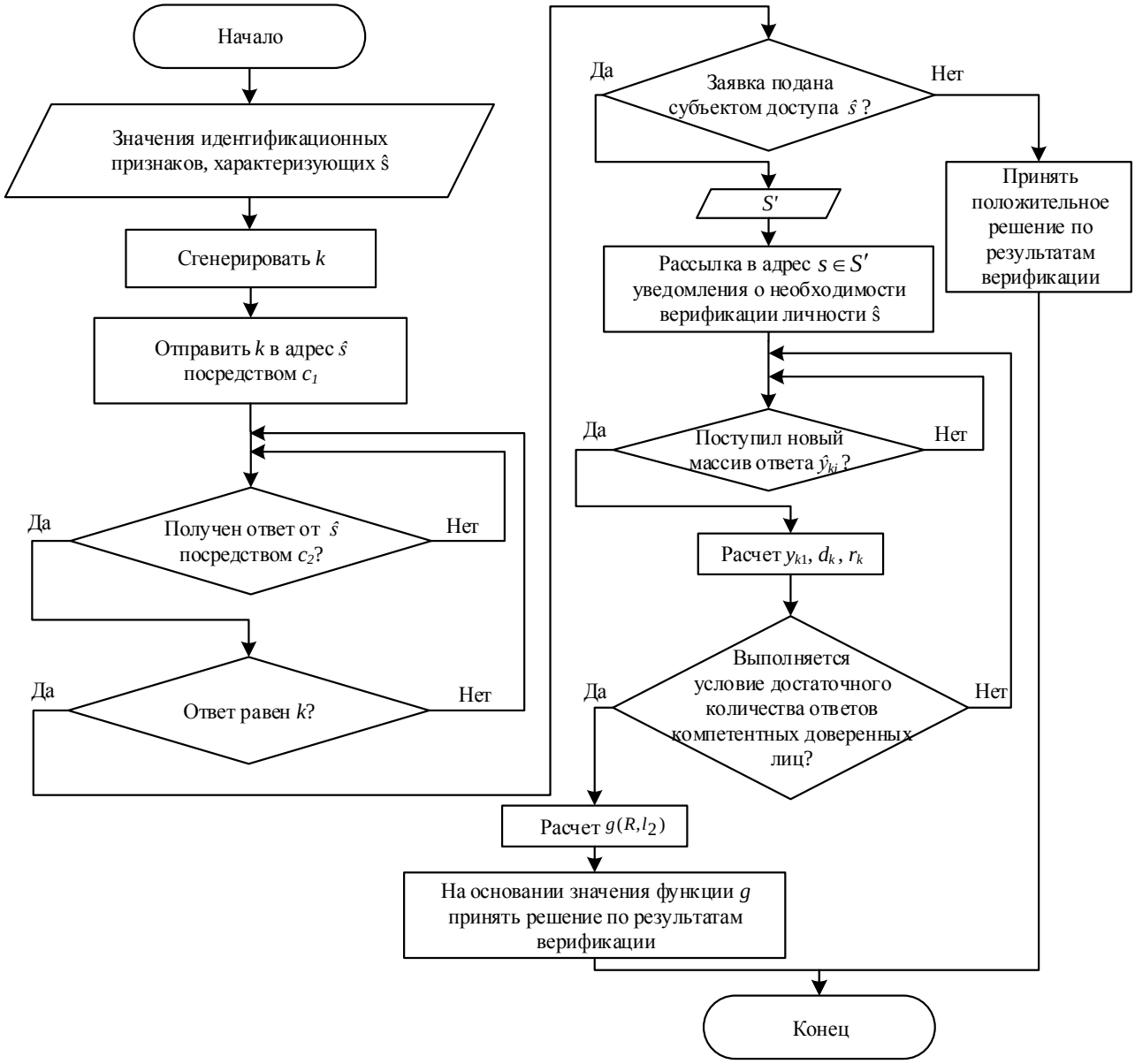

Рисунок 2.8 – Блок-схема применения методики системой *VS*

Апробация методики рассмотрена в главе 3 в ходе эксперимента по внедрению методики в процесс регистрации посетителей ММПЛ.

2.4 Выводы

Проведенный анализ существующих механизмов верификации показал, что использование подтвержденных учетных записей ФГИС ЕСИА и применение технологий ЭП удовлетворяют критериям, выдвинутым к

требуемой методике установления личности при удаленной регистрации в СКУД. Однако возможность внедрения таких механизмов в ММПЛ ограничивается их недостаточной распространенностью на сегодняшний день по ряду причин, в том числе ввиду необходимости посещения пунктов выдачи и материальных затрат. На практике представителям администрации защищаемых объектов приходится искать компромисс между тщательностью проверки идентификационных данных, представленных посетителем, и влиянием данной процедуры на протекание бизнес-процессов.

Автором предложен вариант регистрации, при котором проверка личности осуществлялась бы полностью удаленно, и при этом существовала возможность варьирования требований к процессу верификации в соответствии с уровнем защищенности объекта. Исходя из ранее поставленной задачи и учитывая особенности функционирования ММПЛ, рассмотренные в главе 1, была разработана методика верификации субъекта доступа, основанная на применении механизма доверенных лиц.

Применение предложенной автором методики позволяет организовать процесс верификации полностью удаленно, удовлетворяя при этом всем выдвинутым ранее критериям. Возможность варьирования структуры опросника, минимального количества доверенных лиц и списка каналов передачи данных позволяет адаптировать процесс регистрации пользователей в СКУД к политике безопасности, принятой в конкретном ММПЛ.

Следующая глава посвящена разработке подхода к идентификации и аутентификации в СКУД ММПЛ.

3 ПОДХОД К ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОСЕТИТЕЛЕЙ В МЕСТАХ МАССОВОГО ПРЕБЫВАНИЯ ЛЮДЕЙ

Рассмотренные особенности функционирования ММПЛ и наличие проблем с организацией КПР на их территории обусловливают актуальность задачи выявления современных идентификационных признаков, которые бы позволили решить задачу идентификации посетителей на подобных объектах без нарушения протекающих бизнес-процессов.

Стремительное развитие рынка бытовой электроники и широкое распространение мобильных устройств обусловило наличие у многих людей нескольких личных гаджетов. Появление социальных сетей, мессенджеров, развитие бесконтактных технологий оплаты привело к тому, что люди все чаще ассоциируют конкретные мобильные устройства как неотъемлемый аксессуар, «привязывая» их к различным учетным записям, банковским картам и т.д. Таким образом, человек все тщательнее и бережнее относится к обеспечению сохранности личного мобильного устройства связи, нередко позволяющего идентифицировать его в среде инфокоммуникаций.

Данная глава посвящена исследованию возможных вариантов применения мобильных устройств связи в качестве идентификаторов доступа посетителей. Представлен подход к идентификации и аутентификации, позволяющий автоматизировать пропускной режим в ММПЛ посредством СКУД.

Предложены варианты алгоритмов аутентификации с помощью мобильных устройств связи, которые положены в основу разработанной системы усиленной мобильной аутентификации для СКУД ММПЛ. Представлены результаты апробации предложенного автором методического и программно-алгоритмического обеспечения.

3.1 Использование современных идентификационных признаков в СКУД

3.1.1 Мобильные устройства как способ идентификации

Появление смартфонов – мобильных телефонов, вычислительная мощность которых сегодня сопоставима со стационарными компьютерами, – стало символом одного из важнейших прорывных шагов в развитии инфокоммуникаций, качественно повлиявших на жизнь человека. На базе смартфонов за последние несколько лет появились новые виды электронной техники (планшеты, смарт-браслеты, смарт-часы и прочие гаджеты [74]), которые активно используются практически во всех видах жизнедеятельности человека. При этом в большинстве случаев подобные устройства используются для обеспечения возможности человека быть всегда «на связи» посредством различных технологий (GSM, LTE, Wi-Fi, Bluetooth и т.д. [75]). Данный факт позволяет объединить подобные устройства в единый класс – мобильные устройства связи.

Согласно статистике [76], представленной Международным Союзом Электросвязи (США), на 2016 г. в мире используется около 7 377 млн мобильных устройств связи, учитывая, что население Земли составляет около 7 448 млн человек. При этом, согласно [77], мобильные устройства связи составляют более 50% продаж всей потребительской электроники в мире. Очевидно, что при таком состоянии рынка доступность данного рода гаджетов увеличивается, в том числе из-за снижения их стоимости. На сегодняшний день у многих людей есть несколько подобных устройств, например ноутбук, планшет, смартфон и др.

С одной стороны, при таком положении дел вполне логичным представляется усиление потребительского отношения к мобильным устройствами связи и их значительному понижению в списке материальных благ человека. С другой стороны, несмотря на эффект массовости и усиления

потребительского отношения к гаджетам, в последнее время наблюдается обратный эффект – персонализация гаджетов. Появление социальных сетей, мессенджеров, развитие бесконтактных технологий оплаты приводит к тому, что человеку не хочется часто менять устройство связи. Для него важна возможность постоянной коммуникации. Именно поэтому люди все чаще ассоциируют конкретные мобильные устройства как неотъемлемый аксессуар, «привязывая» их к различным учетным записям, банковским картам и т.д. Потеря или кража гаджетов нередко вызывает у современного человека серьезный дискомфорт, на время «выбивая его из жизненной колеи». Таким образом, в обществе все чаще заметна тенденция – тщательнее и бережнее относиться к обеспечению сохранности личного мобильного устройства связи, нередко позволяющего идентифицировать себя в среде инфокоммуникаций.

Издательство Nature.com опубликовало отчет [78] об исследовании американских и бельгийских ученых, в котором оценивалась возможность идентификации человека в обществе на основе данных о его местонахождении во времени и в пространстве. При этом основным инструментом исследования являлись мобильные устройства связи. На протяжении 15 месяцев накапливалась и анализировалась анонимизированная информация о времени и месте звонков и SMS-сообщений 1,5 млн абонентов. На основе полученных данных строились индивидуальные «следы» (траектории) передвижения людей.

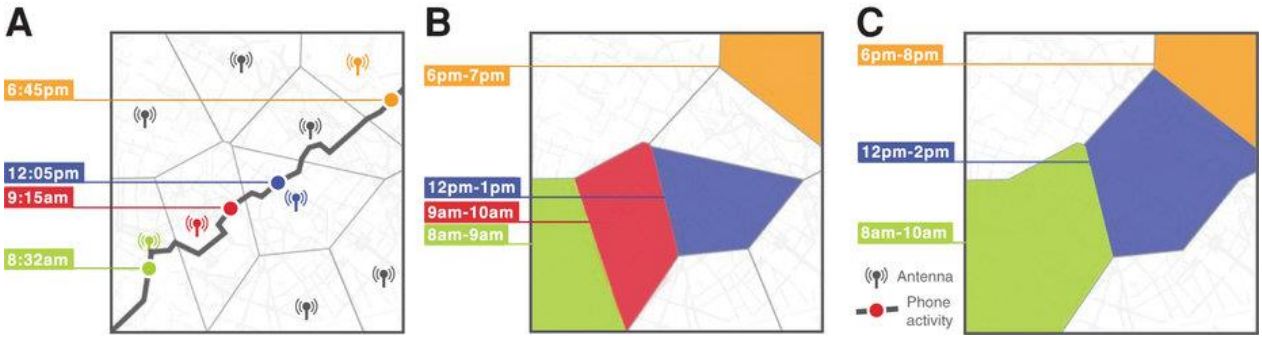

Рисунок 3.1 – Пример вычисления траектории движения анонимного пользователя, построенной путем исследования активности использования мобильного устройства связи в течение дня

Результаты исследования показали, что в 95% случаев достаточно знать всего 4 пространственно-временные точки из открытых источников (Facebook, Twitter, Foursquare, LinkedIn и т.п.) для идентификации и деанонимизации человека среди миллионов других членов общества. Одним из наиболее значимых результатов вышеуказанного исследования является подтверждение факта персонализации мобильных устройств связи в современном мире и возможности рассмотрения их в качестве современных идентификационных признаков.

По мнению автора, данное предположение не является субъективным в связи с наличием множества других подтверждений. Например, одним из направлений развития современных ИТ-компаний является концепция BYOD («Bring your own device») [79]. Принцип, заложенный в эту концепцию, подразумевает, что для доступа к работе с ресурсами компании сотрудники используют личные ноутбуки, планшеты, смартфоны и т.д. Подобная стратегия активно поддерживается такими крупными корпорациями, как Microsoft [80], VMware [81], SAP [82], IBM [83]. Несмотря на то что для подобных компаний затраты на приобретение и сопровождение корпоративных мобильных устройств являются приемлемыми, они охотно поддерживают данную концепцию, предоставляя возможности своим сотрудникам комфортно работать удаленно, вне зависимости от места и времени. При этом современный взгляд на обеспечение безопасности объектов информатизации [84-86] лишь подтверждает приведенные выше слова о персонализации мобильных устройств: в большинстве случаев сотрудники намного тщательнее заботятся о сохранности своего гаджета, чем о безопасности выданного им отдельного физического идентификатора (например, proximity карты доступа).

Все это еще раз подтверждает, что на сегодняшний день мобильные устройства связи настолько прочно вошли в нашу жизнь, что без них сложно представить будни каждого человека.

В настоящее время на рынке систем безопасности наблюдается повышение спроса на СКУД, обладающие функционалом «мобильного доступа». Происхождение этого термина связано с продуктом «Mobile Access» [87], представленным компанией HID Global в 2014 г. и позволяющим смартфонам взаимодействовать со специализированными считывателями iClass SE [88] и multiClass SE [88]. Продукт подразумевает возможность построения инфраструктуры, в которой для получения доступа к материальным или информационным ресурсам в качестве идентификатора используются мобильные устройства.

Широкая вариативность встроенных модулей и предлагаемых функций современных гаджетов на сегодняшний день позволяет организовать взаимодействие со СКУД несколькими способами.

Использование GSM-модуля

Поскольку подавляющее большинство рассматриваемых устройств может быть использовано в качестве сотового телефона, одним из наиболее распространненых подходов является использование GSM-модуля. При этом управляющее воздействие на ИУ или УПУ передается в случае поступления телефонного звонка с определенного номера, закрепленного в БД СКУД за субъектом доступа. Длительность процедуры звонка, а также возможные сбои в работе операторов связи ограничивает область применения подобных систем объектами, характеризующимися невысокой проходимостью посетителей. Примером реализации может выступать шлагбаум, установленный на автомобильной парковке и управляемый по звонку с телефонов субъектов доступа, зарегистрированных в БД. Помимо низкой скорости функционирования подобная схема обеспечивает низкий уровень защищенности, поскольку единственным защитным механизмом выступает «белый список» номеров абонентов.

Использование мобильных приложений

Поскольку современные мобильные устройства функционируют на базе ОС, предоставляющих возможности установки различного ПО, то одним

из вариантов применения их в СКУД является разработка специализированных клиентских приложений, которые позволяют субъекту доступа самостоятельно передавать команды на контроллер. Очевидное преимущество данной схемы заключается в возможности исключения УС и как следствие, упрощении архитектуры СКУД. В то же время необходимо гарантировать наличие связи между смартфоном и контроллером. В целях обеспечения масштабируемости и снижения стоимости системы в подобных решениях зачастую используются облачные сервисы в сети Интернет. Учитывая, что предоставление возможности субъекту доступа самостоятельно передавать команды контроллеру по сути приводит к наделению пользователей правами операторов системы, вышеуказанные преимущества такой схемы взаимодействия обусловливают возникновение целого спектра угроз безопасности для СКУД в целом.

Использование технологий штрих-кодирования

Еще одним вариантом взаимодействия смартфонов и ПИАФ является применение линейных или двумерных штрихкодов, которые отображаются на экране мобильного устройства [89]. Для реализации такой схемы в СКУД должны применяться УС видеозаписывающего класса, способные фиксировать изображение, преобразовывать его и передавать информацию на контроллер в некотором формате. Примером таких СКУД являются системы регистрации билетов. Учитывая, что такие системы характеризуются низкой степенью защищенности ключевой информации, считываемой с экрана мобильного устройства, применение подобных решений весьма ограничено.

Использование технологии Near Field Communication

Появившаяся более 10 лет назад технология беспроводной высокочастотной связи малого радиуса действия NFC (Near Field Communication) [90, 91] является одним из наиболее популярных современных трендов в области использования использования мобильных

устройств в качестве идентификатора. Среди основных характеристик этой технологии следует отметить:

– бесконтактную передача данных;

– минимальное возможное расстояние для передачи данных;

– возможность обмена информацией с другими устройствами или пассивными метками;

– низкую стоимость решения;

– низкое энергопотребление.

Подробные технические характеристики приведены в Приложении 3 [91, 92]. Спецификация интерфейса NFC не предоставляет практических сценариев использования. В отличие, например, от Bluetooth, NFC является только базой, а непосредственные решения обеспечиваются дополнительным ПО. С одной стороны, это открывает широкие возможности для разработчиков, а с другой – является для них же проблемой при обеспечении взаимодействия разных приложений и устройств. Существенным недостатком, ограничивающим массовое применение данной технологии, является отсутствие соответствующего модуля у большого количества существующих смартфонов.

Использование Bluetooth Low Energy

Bluetooth с низким энергопотреблением (Bluetooth Smart, BLE) [93] представляет собой спецификацию ядра популярной беспроводной технологии, наиболее существенными достоинствами которой при использовании в СКУД являются:

– сверхмалое энергопотребление (среднее, пиковое и в режиме простоя);

– отсутствие необходимости предварительного сопряжения устройств;

– использование алгоритма шифрования данных AES [94] с ключом размером в 128 бит, что является достоинством при использовании в СКУД.

Подробные технические характеристики приведены в приложении 3 [95]. Кроме того, в отличие от NFC, BLE полноценно поддерживается как в мобильных ОС Android (с версии 4.4), так и Apple iOS.

Представленный выше анализ существующих решений и подходов по использованию мобильных средств связи в качестве идентификаторов доступа позволяет сделать вывод, что существенными недостатками предлагаемых на рынке продуктов являются:

– необходимость применения конкретного оборудования, поддерживающего фиксированный набор технологий передачи данных;

– отсутствие в их составе документации, регламентирующей организацию ПИАФ в СКУД ММПЛ;

– проприетарность алгоритмов и используемого ПО.

Другими словами, в настоящее время отсутствует методическое обеспечение, которое позволяло бы организовывать процедуры идентификации и аутентификации в ММПЛ, исходя из требований политики безопасности объекта, а не из особенностей применения конкретного оборудования.

Автором предлагается подход, который заключается в использовании мобильных устройств в качестве идентификаторов для ПИАФ электронных проходных. При этом отличительной особенностью подхода является отсутствие зависимости от конкретных протоколов и технологий передачи данных.

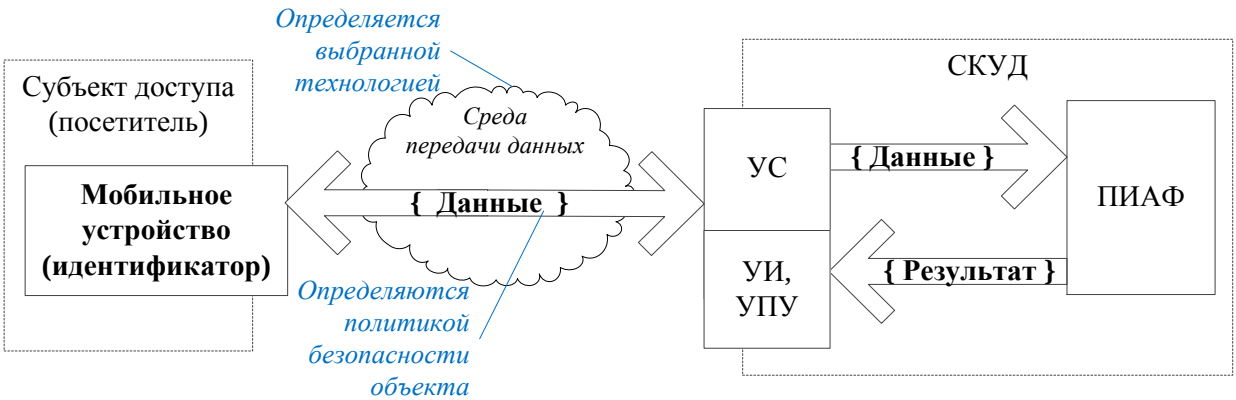

Рисунок 3.2 – Концепция предлагаемого подхода

Концепция подхода (рис. 3.2) предполагает использование мобильных устройств в качестве идентификаторов доступа. При этом владельцу объекта предоставляется возможность самостоятельного определения набора идентификационных данных, а также технологии их передачи в СКУД, что обеспечивает гибкость подхода и возможность масштабирования ПИАФ.

В соответствии с этапами, представленными на рис. 3.3, для организации ПИАФ в СКУД ММПЛ необходимо проанализировать бизнес-процессы и ТСОБ, уже имеющиеся на объекте. На основе полученных сведений следует определить механизмы аутентификации (если они требуются), технологии передачи данных и алгоритмы шифрования. Полученные данные представляют собой техническое задание, которое используется для построения (реализации) ПИАФ.

Рисунок 3.3 – Использование подхода

Как упоминалось ранее, большинство современных смартфонов характеризуются существенными вычислительными возможностями и оборудованы высокоскоростными модулями связи для работы в сети Интернет. Мобильные ОС предоставляют широкий спектр инструментов для разработки и установки специализированных прикладных программ, а также возможность использования различных средств шифрования. Благодаря этому современное мобильное устройство связи может содержать в себе несколько идентификаторов («виртуальных пропусков»), используемых для доступа на различные объекты.

Данные факты являлись предпосылками теоретических изысканий автора и легли в основу вышеизложенного подхода к идентификации и аутентификации в СКУД ММПЛ. Ниже перечислены основные преимущества применения мобильных устройств в качестве идентификаторов доступа.

Во-первых, в современном мире мобильные устройства связи нередко рассматриваются в качестве идентификационных признаков, поэтому вероятность обнаружения субъектом доступа потери или кражи такого идентификатора значительно выше, чем в случае с классическими электронными пропусками. Также вероятность возникновения случаев передачи смартфона другим лицам для прохода на объект значительно ниже, чем в случае с картами доступа. Кроме того, современные телефоны нередко обладают функционалом по информированию владельца о координатах устройства.

Во-вторых, одно мобильное устройство может быть использовано в качестве идентификатора для нескольких объектов. Многие организации имеют офисы по всему миру, в которых могут использоваться различные СКУД. В случае командирования сотрудников зачастую требуются гостевые пропуска. Применение мобильных устройств, помимо очевидного снижения финансовых затрат на обслуживание идентификаторов, позволяет обеспечить единую политику безопасности на всех объектах компании.

В-третьих, наличие в мобильных устройствах высокоскоростных модулей подключения к сетям передачи данных обусловливает возможность оперативного удаленного управления идентификаторами, включая их выдачу, изменение конфигурации и отзыв в режиме реального времени. Не менее важной является возможность удаленной регистрации субъектов доступа в БД СКУД (без предварительного посещения объекта) с применением механизмов верификации личности.

В-четвертых, используемые в мобильных устройствах технологии транспорта идентификационных данных обеспечивают возможность использования в местах, требующих значительного расстояния между УС и идентификатором. Например, шлагбаум на въезде в паркинг, гараж и т.д. Кроме того, в большинстве случаев возможна скрытая установка УС (без вмешательства в интерьер помещения) для защиты от вандализма.

В-пятых, современные мобильные ОС позволяют использовать алгоритмы шифрования и средства ЭП, что обеспечивает высокий уровень безопасности самого устройства, выступающего в качестве идентификатора. Как правило, приложения работают в изолированной программной среде (Sandbox) [96], исключающей возможность доступа или изменения данных другими программами, а базовые функции автоматической блокировки экрана обеспечивают возможность введения дополнительного фактора аутентификации посредством применения паролей различных видов.

Помимо вышеперечисленных преимуществ предложенный подход обусловливает широкие конвергенционные возможности, поскольку мобильное устройство, применяемое в качестве идентификатора, может быть использовано как для разграничения доступа к физическим объектам, так и для доступа к электронным ресурсам предприятия. Примером может являться аутентификация при доступе к беспроводным сетям связи, VPN [97], корпоративным порталам и т.д.

3.1.2 Применение одноразовых паролей для аутентификации в СКУД

В целях достижения универсальности подхода, а также массовости построенных на его основе систем, автором не выдвигались требования к технологиям транспорта идентификационной информации. Между тем, ранее было отмечено, что далеко не все существующие решения обеспечивают безопасность передаваемых данных. В связи с этим подход предполагает возможность применения механизмов усиленной аутентификации, позволяющих защитить передаваемые данные от возможной компрометации злоумышленником. В качестве примера реализации подобных механизмов автором предлагается использовать технологию одноразовых паролей (One time password, OTP) [57,98]. Преимущество одноразового пароля по сравнению с обычным состоит в ограничении его использования лишь в рамках одного сеанса аутентификации. Таким образом, злоумышленник, перехвативший данные из успешной сессии, не может им воспользоваться повторно. В табл. 3.1 приведены методы реализации данного механизма в системах аутентификации и требования к технологии передачи данных при использовании приведенного подхода.

В случае использования технологии одноразовых паролей автором предлагается использовать следующие компоненты в качестве основы секретного ключа *k*:

– численное значение графического пароля g для запуска приложения. В ПЗУ мобильного устройства хранится хеш значение g_H;

– ключевая пара n (массив «заводских» параметров мобильного устройства, которые буду опрашиваться аппаратом при каждой генерации временного пароля). Привязка к физическим характеристикам является дополнительным рубежом защиты от копирования ПЗУ мобильного устройства;

– случайный набор бит b, который сохраняется в скрытой области памяти мобильного устройства.

Таблица 3.1 – Требования к технологии передачи данных в зависимости от используемого метода аутентификации с помощью OTP

Название метода	Принцип работы	Требования к технологии передачи данных
«Запрос-ответ»	В начале процедуры аутентификации пользователь отправляет на сервер свой идентификатор. В качестве ответа сервер генерирует случайную строку и посылает ее обратно. Полученные данные пользователь шифрует с помощью секретного ключа, после чего возвращает результат отправителю. Сервер находит в БД ключ данного пользователя и с его помощью шифрует исходную строку. Далее проводится сравнение результатов шифрования. При полном совпадении считается, что аутентификация прошла успешно	Использование метода возможно только в случае выбора технологии передачи данных, реализующей возможность двустороннего обмена информацией между мобильным устройством и УС
«Только ответ»	В начале процедуры аутентификации программное или аппаратное обеспечение пользователя самостоятельно генерирует исходные данные, которые будут зашифрованы и отправлены на сервер для сравнения. При этом в процессе создания строки используется значение предыдущего запроса. Сервер тоже обладает этими сведениями. Зная идентификатор, он находит значение предыдущего запроса пользователя и генерирует точно такую же строку. Зашифровав ее с помощью секретного ключа пользователя, сервер получает значение, которое должно полностью совпадать с присланными пользователем данными	Технология передачи данных должна подразумевать возможность получения УС информации от мобильного устройства
«Синхронизация по времени»	В качестве исходной строки выступают текущие показания таймера устройства. При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 с). Эти данные зашифровываются с помощью секретного ключа и отправляются на сервер вместе с идентификатором. Сервер при получении запроса на аутентификацию выполняет аналогичные действия, после чего производит сравнение двух значений: вычисленного и полученного от пользователя	Технология передачи данных должна подразумевать возможность получения УС информации от мобильного устройства
«Синхронизация по событию»	Метод практически идентичен предыдущему, однако в качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей. Это значение подсчитывается обеими сторонами отдельно друг от друга	Технология передачи данных должна подразумевать возможность получения УС информации от мобильного устройства

Далее вычисляется хеш свертка от перечисленных компонентов. Из полученного значения в соответствии с выбранным алгоритмом шифрования формируется секретный ключ. Например, осуществляется выделение *l* символов строки или преобразование к ближайшему простому числу. На рис. 3.4 представлена схема формирования сообщения *M*, предназначенного для передачи УС.

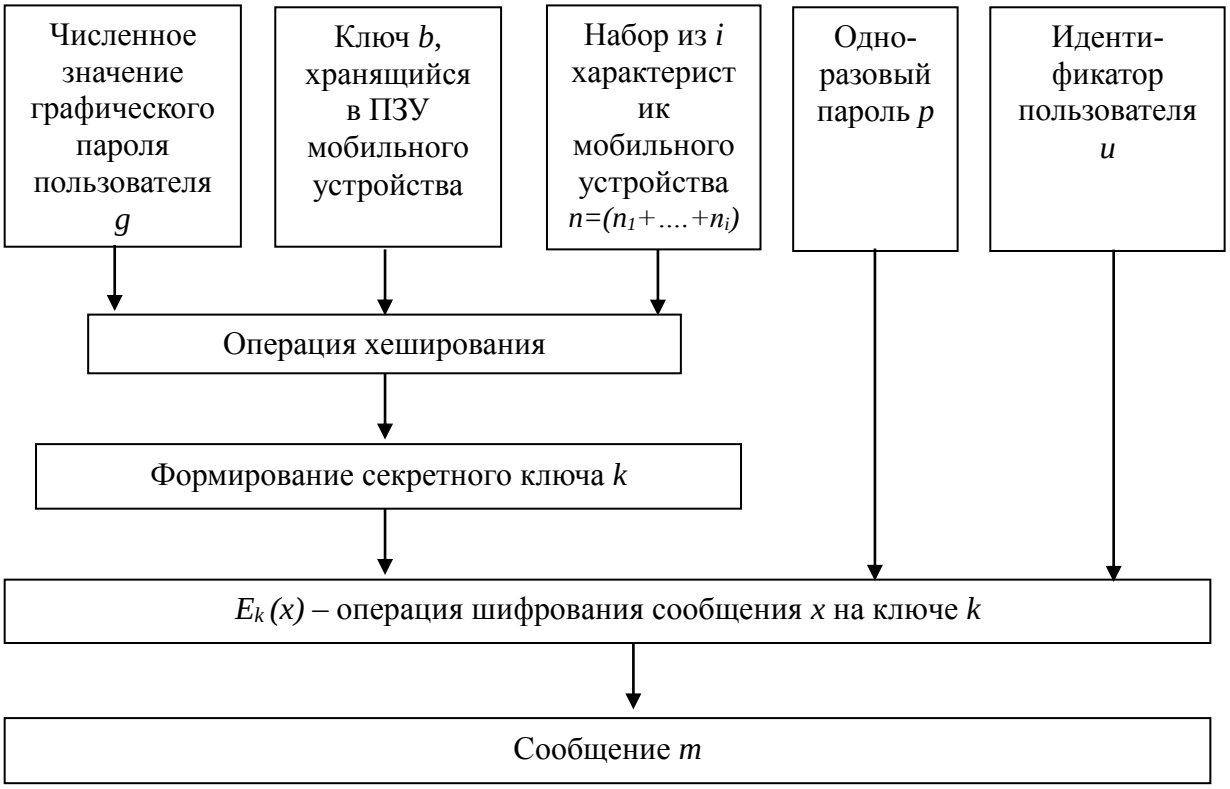

Рисунок 3.4 – Пример схемы формирования сообщения *m*, содержащего одноразовый пароль

Как видно из рис. 3.4, вторым фактором аутентификации выступает защита от несанкционированного доступа к приложению-аутентификатору (в случае потери / кражи мобильного устройства) путем использования современных методов графических паролей. Графический пароль содержит два взаимодополняющих компонента: он включает изображение из пользовательской мультимедиа-библиотеки и набор жестов, рисуемых поверх изображения. Использование личных изображений увеличивает и безопасность, и запоминаемость пароля.

Для полноты предлагаемого подхода автором были предложены алгоритмы аутентификации, в основе которых лежат технологии передачи данных в виде QR-кодов и динамических NFC-меток.

3.1.3 Алгоритм аутентификации на основе применения QR-кодов

Применение метода генерации OTP «запрос-ответ», предполагающего асинхронный режим работы с двусторонним обменом данными между клиентом и сервером, не находит практической реализации в случае использования технологий штрихового кодирования.

Недостатком всех остальных методов, работающих в синхронном режиме, является возможность рассинхронизации OTP-токена [57] и сервера. Несмотря на то что в режиме «синхронизация по времени» используется не дискретное значение, а некоторый допустимый запас времени для процедуры аутентификации, часы программного генератора одноразовых паролей могут уйти вперед или отстать. Это может быть вызвано умышленным изменением времени устройства либо сбросом настроек по причине разряда аккумулятора или сбоя ПО.

Умышленная смена временных параметров является той процедурой, которую пользователи обычно выполняют очень редко, тем более что современные средства связи обладают функционалом синхронизации времени с NTP серверами. В случае полной разрядки телефона внутренние часы мобильного устройства обычно поддерживаются резервным элементом питания.

В режимах «только ответ» или «синхронизация по событию» сбой аутентификации может привести к «отставанию» сервера от мобильного устройства субъекта. В качестве примера можно рассмотреть случай, когда пользователь запустил приложение-аутентификатор, но по каким-то причинам не воспользовался им и завершил работу. В качестве решения подобных проблем можно генерировать варианты OTP сразу для нескольких

событий. Приведенный ниже алгоритм предполагает формирование одноразовых паролей в режиме «синхронизация по времени».

Регистрация мобильного устройства субъекта доступа

Для регистрации идентификатора необходимо перейти в режим синхронизации времени и поднести мобильное устройство к камере-считывателю (в случае удаленной регистрации – к web-камере субъекта доступа). ПО, установленное на мобильном устройстве, отобразит на дисплее QR код с текущим временем. После этого сервер вычислит и сохранит значение смещения между своими часами и временем, переданным мобильным устройством. Как и в случае с синхронизацией времени, процедура согласования ключа b происходит путем считывания строки с дисплея устройства QR кода. В случае использования удаленной регистрации посетителей необходимо обеспечить шифрование передаваемых данных между клиентом и сервером.

Аутентификация

Процедура аутентификации в такой системе будет выполняться согласно схеме, представленной на рис. 3.5 [99].

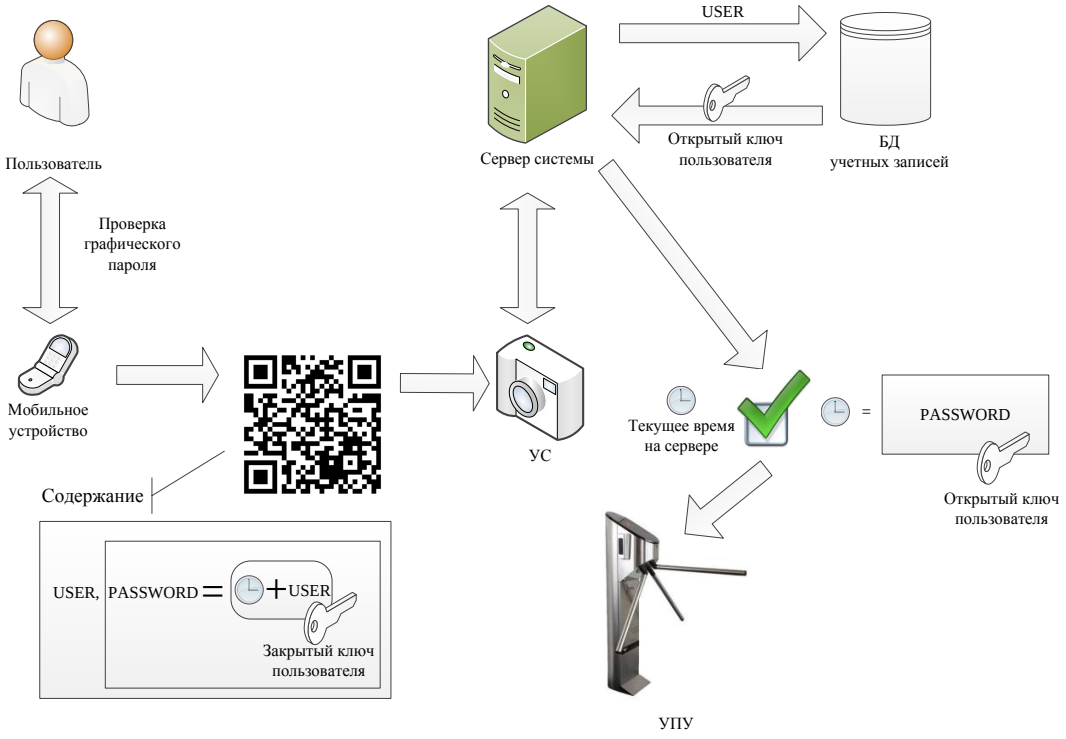

Рисунок 3.5 – Схема аутентификации в режиме передачи QR кодов

Получение одноразового QR кода для аутентификации можно описать выражением *F*:

$$F(u,g,b,n) = Q\left(u \times E_{R[H(g*b*n),l]}(u \oplus t)\right) \quad (3.1)$$

где *u* – идентификатор пользователя; *g* – значение графического пароля; *b* – ключ, хранящийся в ПЗУ мобильного устройства; *n* – набор значений аппаратных характеристик мобильного устройства; *t* – текущая временная метка; *l* – набор требований, предъявляемых к секретному ключу в используемом алгоритме шифрования; ×, *, $\oplus$ – операции конкатенации строк с использованием разделителей; *Q(x)* – операция преобразования сообщения *x* в QR код; $E_k(x)$ – операция шифрования сообщения *x* на ключе *k*; $R(x,y)$ – операция формирования секретного ключа из входной строки *x* в соответствии с набором требований *y*, предъявляемых к секретному ключу используемым алгоритмом шифрования; $H(x)$ – операция хэширования строки *x*.

Алгоритм, определяющий порядок формирования одноразового QR кода для аутентификации, представлен в виде блок-схемы на рис. 3.6.

Перед началом операции формирования нового QR кода счетчик t_{int}, принимает значение 0. В качестве условия, свидетельствующего о необходимости генерации нового QR кода, выступает процедура сравнения счетчика с параметром «временя жизни одноразового пароля $t_{int\text{-}live}$», определяемого оператором системы.

УС системы после считывания QR кода передает его контроллеру для декодирования (операция *Q`*) и дальнейшего разбиения (операция *Array*) на массив *m*, состоящий из двух элементов – идентификатора пользователя *u* и значениея OTP (выражение (3.2)):

$$F`(m`) = Array[Q`(m`)] \quad (3.2)$$

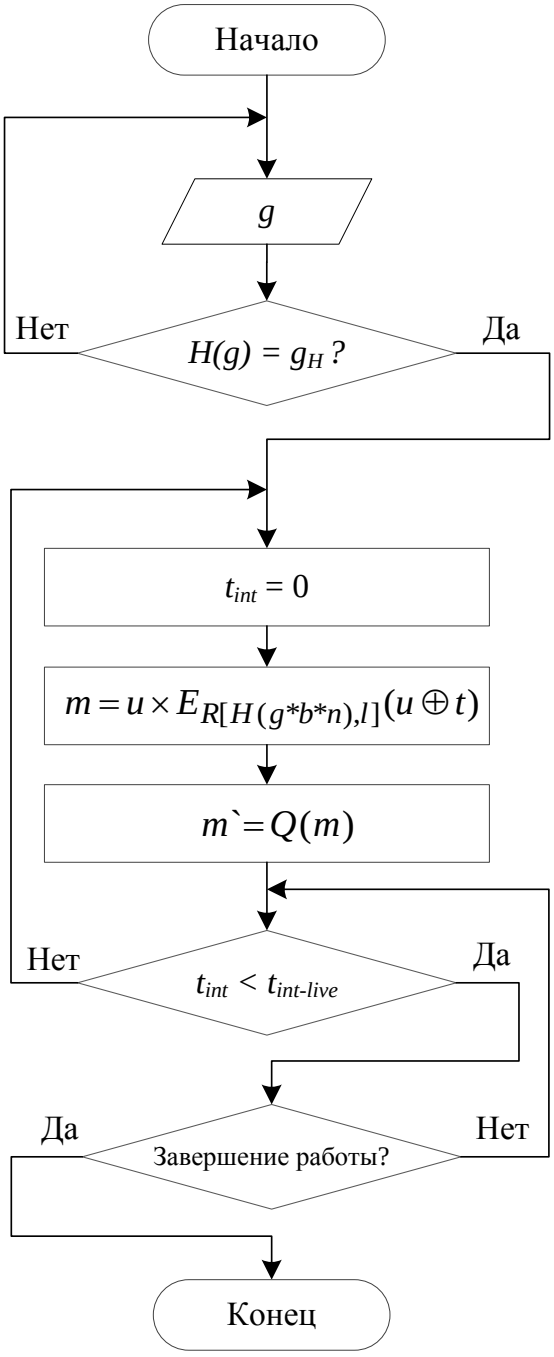

Рисунок 3.6 – Блок-схема формирования QR кода для аутентификации

Далее выполняется процедура расшифрования и последующее выделение значение времени генерации пароля:

$$P\left(D_{S(m[0])}(m[1])\right) = t_2, \tag{3.3}$$

где t_2 – полученное значение времени генерации одноразового пароля; $m[0]$ – идентификатор пользователя; $m[1]$ – значение пароля; $P(x)$ – операция выделения значения времени генерации ОТР; $D_k(x)$ – операция расшифрования сообщения x на ключе k; $S(x)$ – операция получения ключа k по пользовательскому идентификатору x из БД.

В случае успешного расшифрования значения ОТР система сверяет текущее время t со временем генерации одноразового пароля t_2. Если разница не превышает установленную границу $t_{int\text{-}live}$, то в УИ или УПУ передается управляющее воздействие на пропуск субъекта доступа (рисунок 3.7).

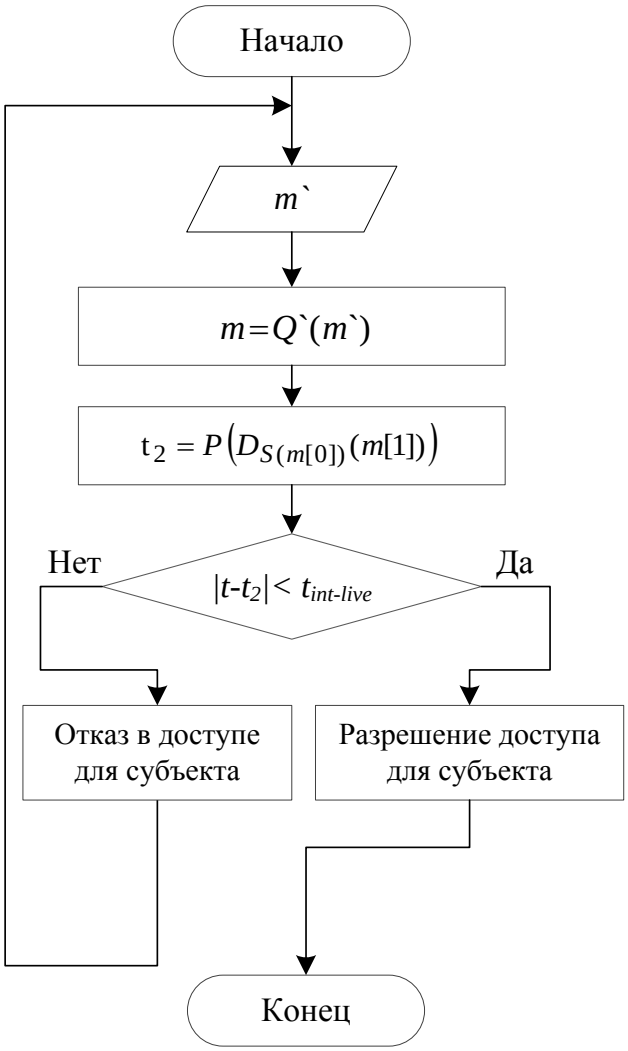

Рисунок 3.7 – Блок-схема выполнения процедуры аутентификации контроллером СКУД

3.1.4 Алгоритм аутентификации на основе применения NFC-меток

Технология NFC предусматривает три режима работы [100]:

1) Card Emulation mode – эмуляция бесконтактной смарт-карты;

2) Peer-to-Peer – пиринговый режим обмена между двумя активными устройствами;

3) Reader-Writer mode – режим чтение / запись.

До 2013 года информацию для осуществления NFC-транзакций в режиме эмуляции бесконтактной карты в мобильных устройствах можно было хранить только на специальном защищенном чипе (Secure element, SE [101]). Данный элемент может быть размещен либо конструктивно в корпусе телефона, либо на специальной карте формата MicroSD, либо в SIM-карте формата (принцип SIM centric NFC [91, 101]). С выпуском мобильной ОС Android 4.4 KitKat [102] компания Google предоставила возможность взаимодействия NFC-контроллера не только с SE, но и с обычным приложением в телефоне. Данное решение под названием Host Card Emulation (HCE) оказалось очень популярным среди приложений для мобильных устройств (карты лояльности, бонусные системы, скидочные купоны и т.д.). Все приведенные в п. 3.1.1 решения по реализации функционала мобильного доступа в СКУД в случае применения технологии NFC основаны на использовании HCE.

В данной работе автором предложен алгоритм для использования технологии NFC в СКУД, использующий альтернативный режим Peer-to-Peer и основанный на применении OTP с методом генерации одноразовых паролей «Запрос-ответ» (рис. 3.8). Применение подобного алгоритма существенно расширяет возможность практической реализации функционала мобильного доступа в СКУД, не требуя от мобильного устройства поддержки технологии HCE.

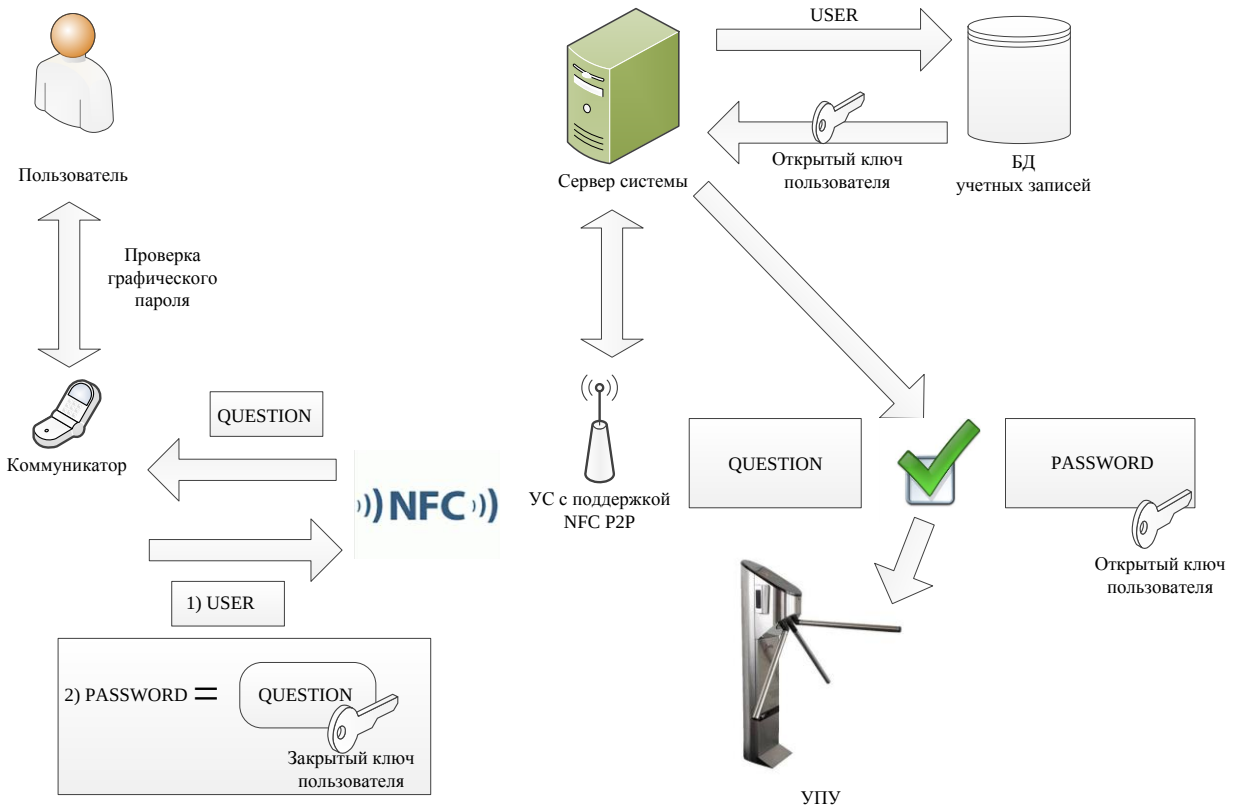

Рисунок 3.8 – Схема аутентификации в режиме NFC

В данной схеме динамическим составляющим является случайный вопрос *a*, который сервер генерирует на каждое обращение пользователя. Именно этот вопрос подвергается шифрованию пользовательским устройством, в дальнейшем позволяя осуществить проверку аутентичности субъекта доступа.

Алгоритм процедуры аутентификации можно представить в виде блок-схем, представленных на рис. 3.9, 3.10.

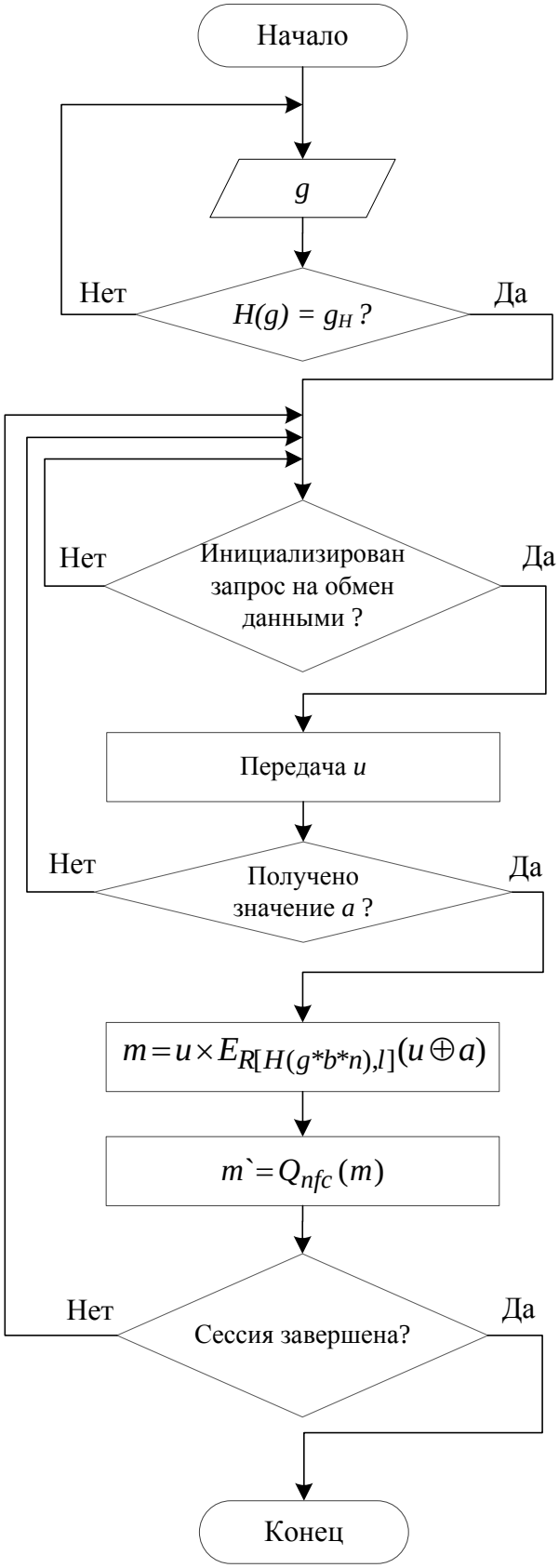

Рисунок 3.9 – Блок-схема алгоритма аутентификации в режиме NFC для мобильного средства субъекта доступа

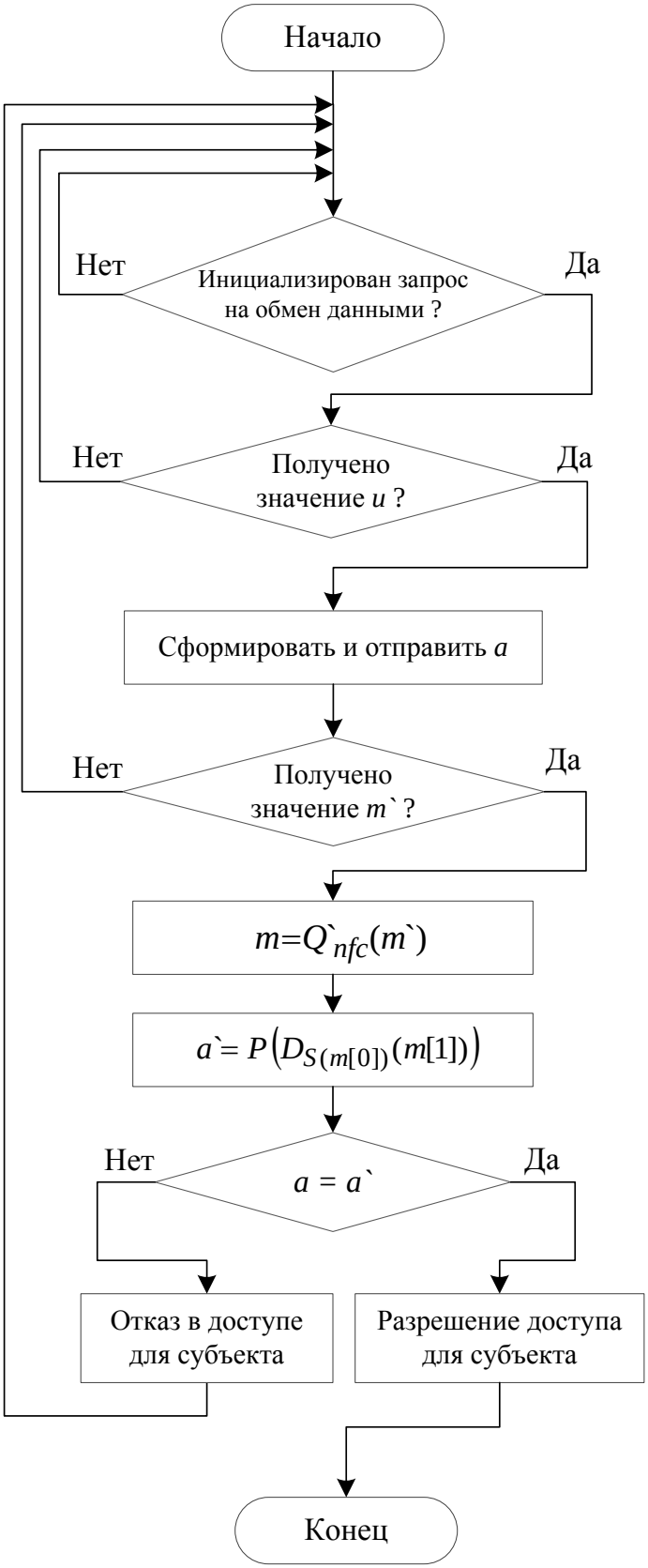

Рисунок 3.10 – Блок-схема алгоритма работы сервера аутентификации в режиме NFC

3.2 Разработка системы усиленной мобильной аутентификации для СКУД ММПЛ

Представленный в п 3.1 анализ СКУД, обладающих функционалом «мобильного доступа», показал, что существующие решения не учитывают особенности функционирования ММПЛ, вследствие чего их применение для организации процесса идентификации посетителей в рассматриваемых объектах не представляется возможным. В связи с этим было принято решение разработать систему идентификации посетителей для СКУД ММПЛ, в основе которой лежит предложенный в п. 3.1 подход.

На основании анализа особенностей объекта внедрения и существующих методов взаимодействия мобильного устройства и УС, представленных в пункте 3.1.1 настоящего исследования, было решено реализовать два режима транспорта данных:

– режим передачи, основанный на использовании технологии штрихового кодирования;

– режим передачи, основанный на использовании технологии NFC.

Одной из составляющих приведенного в п. 3.1 подхода является возможность внедрения механизмов усиленной аутентификации. Между тем, учитывая что системы, базируюшиеся на технологии штрихового кодирования, характеризуются низкой степенью защищенности ключевой информации, было решено реализовать систему усиленной аутентификации («I-mob», Приложение 1).

Структура разработанной системы представлена на рис. 3.11. Функционал программного комплекса реализован в виде трех взаимосвязанных подсистем, каждая из которых состоит из совокупности модулей.

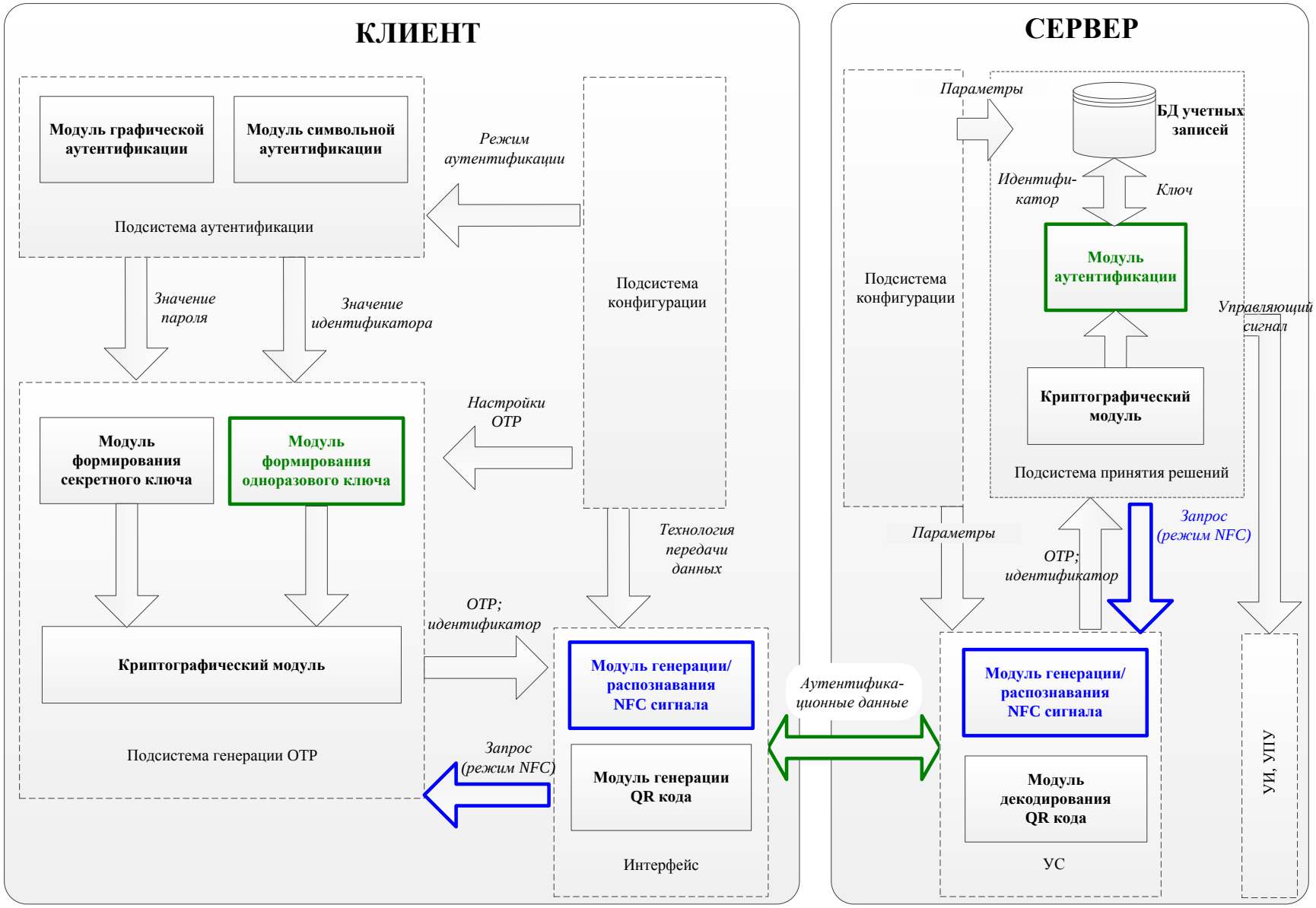

Рисунок 3.11 – Структура системы усиленной аутентификации

Клиентская часть

Мобильное приложение реализовано для наиболее популярных операционных систем Android и Apple iOS. Клиентская версия Android подразумевает два режима транспорта данных:

– NFC-метки (режим P2P и режим эмуляции бесконтактной карты);

– QR-коды.

Для реализации режима эмуляции карты в ОС Android используется технология HCE. На рис. 3.12 представлен скриншот работы программы. Для реализации программного генератора OTP в режиме передачи QR кодов был выбран режим «синхронизация по времени» с использованием интервала проверки в 10 с. Данный метод был выделен после проведенного анализа на частоту возможных проявлений рассинхронизации в практических условиях.

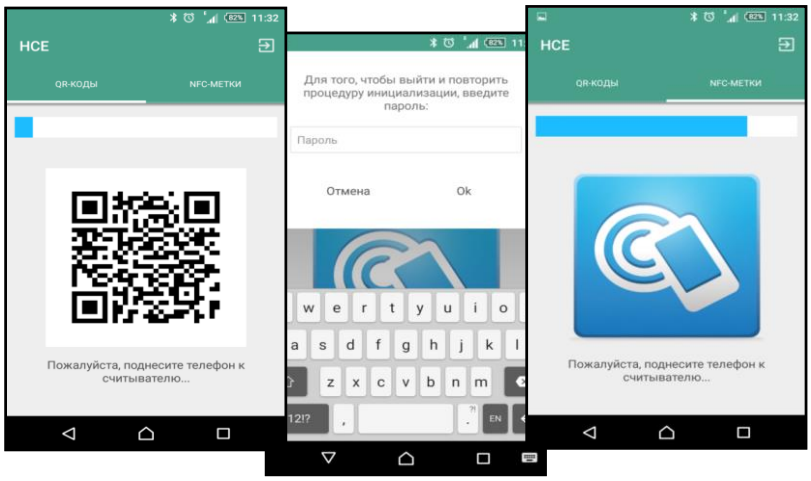

Рисунок 3.12 – Скриншот клиентской версии разработанной системы усиленной аутентификации для ОС Android

В мобильных устройствах, выпускаемых компанией Apple, модули NFC появились лишь с шестой версии смартфонов IPhone. Кроме того, производитель ограничил область применения данного модуля собственной платежной системой Apple Pay [103]. В связи с отсутствием технической возможности реализации технологии NFC для взаимодействия с УС СКУД, разработанная система для версии Apple iOS использует возможность передачи данных только посредством QR-кодов. При разработке клиентского

приложения под мобильную операционную систему Apple iOS была использована среда разработки XCode и свободно распространяемая библиотека QR-Code-Encoder-for-Objective-C [104]. На рис. 3.13 представлен интерфейс разработанного приложения.

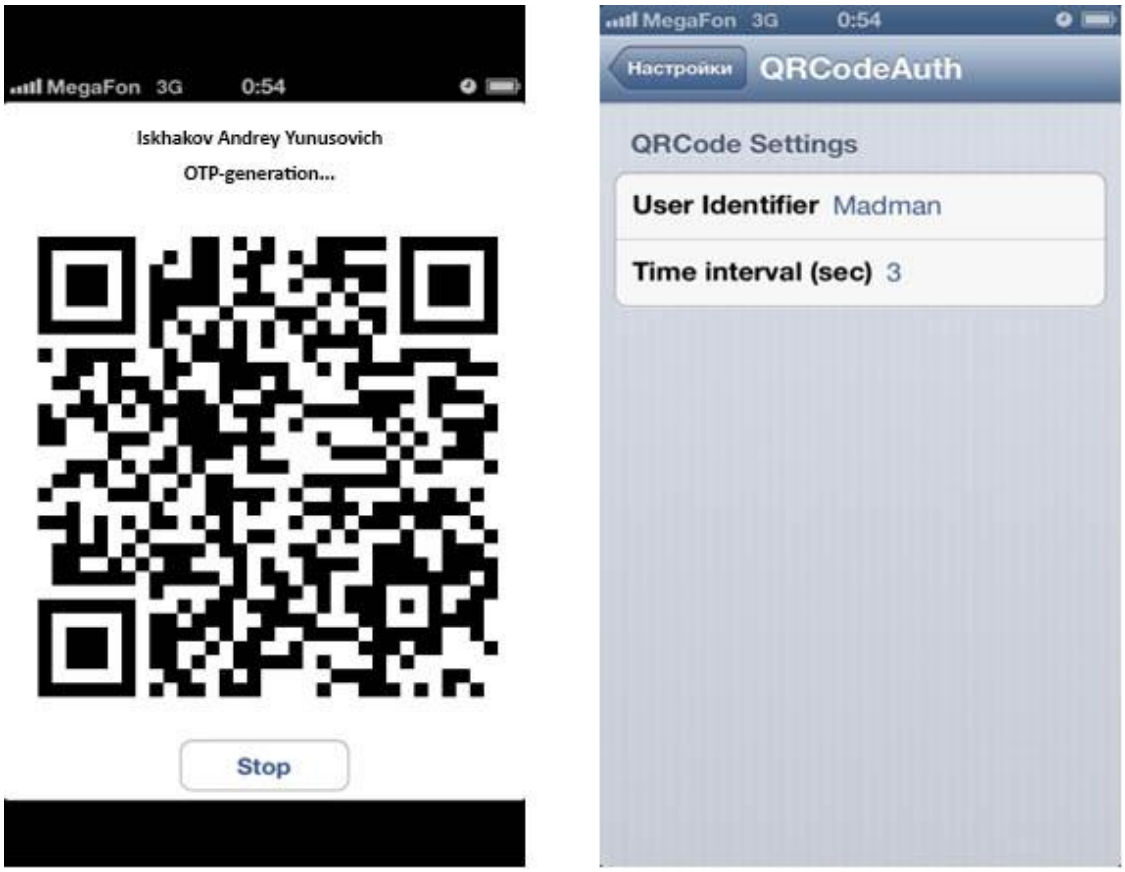

Рисунок 3.13 – Скриншот клиентской версии разработанной системы усиленной аутентификации для ОС Apple iOS.

Серверная часть

На рис. 3.14 представлен интерфейс администратора системы. Ниже перечислены функциональные возможности разработанной системы:

– идентификация пользователей;

– аутентификация пользователей;

– удаленная регистрация и выдача ИД;

– реализация предложенной автором методики удаленной верификации субъекта доступа;

– накопление информации в журналах прохода;

– накопление и графическое представление статистики доступа по точкам прохода.

При разработке системы отдельное внимание было уделено обеспечению безопасности веб-приложения, подробно рассмотренное в [105-107]

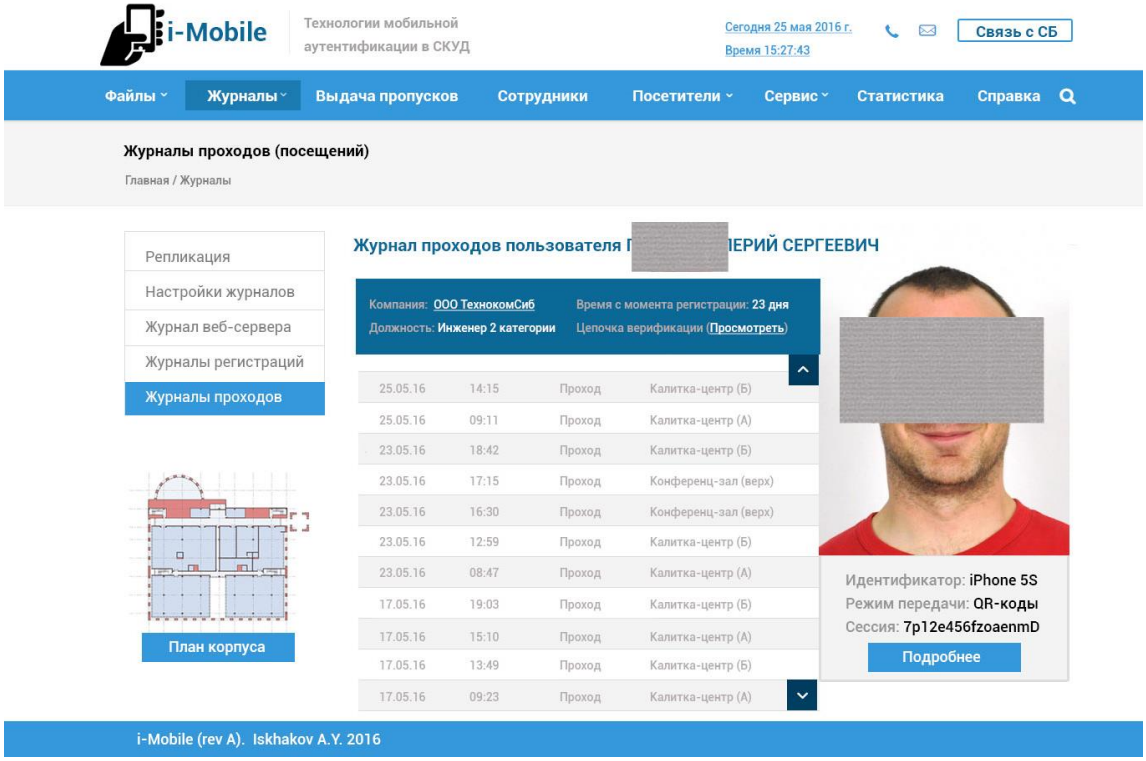

Рисунок 3.13 – Скриншот интерфейса администратора системы

3.3 Экспериментальная апробация результатов работы

Для оценки адекватности и эффективности предложенного методического и программно-алгоритмического обеспечения был проведен ряд экспериментов. Для апробации методики верификации субъекта доступа на основе механизма доверенных лиц был проведен эксперимент, состоящий в моделировании ситуации, где данная методика верификации может быть применена. Было организовано мероприятие с массовым участием, для доступа на которое посетителям необходимо было пройти верификацию с помощью механизма доверенных лиц. Оценка адекватности предложенного

подхода к идентификации и аутентификации в СКУД ММПЛ на основе современных идентификационных признаков осуществлялась на основе сравнения его с аналогами на базе критериев, важных с точки зрения использования подхода на реальных объектах.

3.3.1 Апробация методики верификации на основе доверенных лиц

Эффективность предложенной методики верификации была оценена в сравнении с приведенными в п. 2.2.2 аналогами: верификацией с помощью учетной записи ФГИС ЕСИА и использованием средств ЭП. Апробация предполагала необходимость зарегистрироваться и пройти верификацию для посещения массового мероприятия с помощью одного из предложенных пользователю способов. В качестве пользователей выступали члены трех трудовых коллективов общей численностью 112 человек, которые получили рассылку с приглашением на данное мероприятие с необходимостью регистрации, прохождения процедуры верификации и получения идентификатора. Среди участников присутствовали лица возрастом от 24 до 56 лет.

Для сравнения аналогов были выделены следующие количественные показатели:

1) количество человек, воспользовавшихся механизмом (посчитавших его наиболее удобным для процедуры верификации личности);

2) среднее время, потребовавшееся для регистрации пользователя;

3) среднее время, потребовавшееся для верификации пользователя;

4) доля выявленных ошибочных верификаций от общего количества верифицированных данным механизмом.

Из 112 участников 9 (по 3 в каждой организации) являлись администраторами системы, то есть были зарегистрированы, верифицированы и имели идентификаторы (для функционирования механизма доверенных лиц). 103 человека должны были получить

идентификаторы самостоятельно, при этом не проводилось какое-либо анонсирование и отрыв членов коллектива от рабочего процесса. Таким образом, была предпринята попытка смоделировать ситуацию, когда более 50 человек желают посетить одно мероприятие и получить соответствующий идентификатор для этого. Количество посетителей – 103 – делает невозможным их регистрацию непосредственно при посещении ММПЛ, при учете того факта, что посетители не приходят на мероприятие ранее чем за 30 мин, а на регистрацию 1 посетителя соответствующему персоналу требуется не менее 30 с.

По итогам проведения процедуры не оказалось участников, не справившихся с получением идентификатора. Численные результаты апробации по выделенным показателям приведены в табл. 3.2.

Таблица 3.2. Количественные показатели апробации методики верификации на основе механизма доверенных лиц

Способ верификации	Учетная запись ФГИС ЕСИА	Использование средств ЭП	Механизм доверенных лиц
Количество человек, воспользовавшихся способом	21	4	78
Среднее время регистрации, мин.	7,18	11,10	33,24
Среднее время верификации, мин.	1,21	1,48	24,57
Доля выявленных ошибок верификации, %	0	0	0

Приведенные результаты иллюстрируют тот факт, что длительность процедуры верификации с использованием механизма доверенных лиц значительно превышает соответствующие значения для двух других способов. Однако следует отметить, что в рамках решения поставленной перед пользователями задачи – регистрации на общее мероприятие – средний показатель, равный 33,24 мин, является удовлетворительным и не превышает разумно допустимого временного интервала для использования на практике. Вместе с тем количество пользователей, выбравших способ верификации с помощью механизма доверенных лиц, в 3,7 раза превышает количество

использовавших для этого учетную запись ФГИС ЕСИА, а количество использовавших ЭП – в 19,5 раз.

Таким образом, экспериментальная апробация показала, что эффективность предложенной методики является удовлетворительной с точки зрения общего времени, затрачиваемого на регистрацию с его использованием. С точки зрения массовости применения предложенная методика верификации личности на основе доверенных лиц является в несколько раз более эффективной по сравнению с аналогичными решениями. Адекватность методики, выраженная в достоверности проведения процедуры верификации, доказывается отсутствием ошибочных верификаций, в чем она не уступает аналогам.

3.3.2 Апробация похода к идентификации и аутентификации в СКУД ММПЛ

Оценка адекватности предложенного подхода к идентификации и аутентификации в СКУД ММПЛ и эффективности его применения была произведена посредством сравнения с аналогами:

– наиболее распространенным способом идентификации в СКУД с помощью использования в качестве идентификатор бесконтактной карты;

– идентификацией посетителей на основе проверки их документов, удостоверяющих личность, как единственным аналогом, подходящим для ММПЛ на сегодняшний день.

Сравнение проводилось на основе следующих критериев:

1) время идентификации 1 000 посетителей;
2) количество отказов при считывании 1 000 идентификаторов;
3) возможность применения в ММПЛ;
4) количество ошибок при считывании 1 000 идентификаторов.

Значения критериев для сравниваемых подходов, рассчитанные в ходе экспериментальной апробации, приведены в табл. 3.3

Таблица 3.3 Измеренные значения критериев для сравниваемых подходов

Критерий сравнения	Предложенный подход	Подход на основе бесконтактных карт-идентификаторов	Подход с помощью проверки документа
Время идентификации 1000 посетителей, с	3 115	2 268	45 158
Возможность применения в ММПЛ	Да	Нет	Да
Количество ошибок 1 рода (отказов) на 1 000 считываний	8	47	0
Количество ошибок 2 рода на 1 000 считываний	0	0	3

Для сравнения альтернативных подходов на основе значений нескольких критерий был использован метод анализа иерархий [108, 109], который позволяет произвести многокритериальный выбор наилучшей альтернативы. В основе метода лежит декомпозиция сложной задачи сравнения нескольких альтернатив на множество попарных, более простых сравнений.

Метод предполагает, что критерии могут иметь локальные приоритеты, то есть веса. Для их оценки предлагается использовать оценочную шкалу, приведенную в табл. 3.4. Данная шкала позволяет оценить критерии по принципу их значимости, а также альтернативы – по степени интенсивности проявления критерия.

Таблица 3.4. Шкала относительной важности для оценочного сравнения критериев и альтернатив

Интенсивность относительной важности	Определение	Объяснение
0	Несравнимы	Сравнение невозможно
1	Равная важность	Равный вклад двух видов деятельности в цель
3	Умеренное превосходство одного над другим	Опыт и суждения дают легкое превосходство одному виду деятельности над другим
5	Существенное или сильное превосходство	Опыт и суждения дают сильное превосходство одному виду деятельности над другим

Окончание табл. 3.4

7	Значительное превосходство	Одному из видов деятельности дается настолько сильное превосходство, что оно становится практически значительным
9	Очень сильное превосходство	Очевидность превосходства одного вида деятельности над другим подтверждается наиболее сильно
2, 4, 6, 8	Промежуточные решения между двумя соседними суждениями	Применяются в компромиссном случае
Обратные величины приведенных выше чисел	Если при сравнении одного вида деятельности с другим получено одно из вышеуказанных чисел (например, 3), то при сравнении второго вида деятельности с первым получим обратную величину (т.е. 1/3)	

Попарное сравнения критериев на основе шкалы приведено в табл. 3.5. Сравнение было произведено автором работы на основе объективных представлений о значимости критериев. Несомненно, важнейшим критерием адекватности и применимости подхода является количество ошибок 2 рода. Данный критерий показывает качество работы СКУД, позволяет оценить достоверность проводимой идентификации. Возможность применения подхода в ММПЛ также является значимым в силу решения задач настоящего диссертационного исследования. Количество ошибок 1 рода (отказов при считывании) и время идентификации являются показателями удобства как для пользователя, так и для администрации объекта доступа.

Таблица 3.5. Числовые оценки матрицы попарных сравнений для критериев

Критерии	Время идентификации 1 000 посетителей	Количество ошибок 1 рода (отказов) на 1 000 считываний	Возможность применения в ММПЛ	Количество ошибок 2 рода на 1 000 считываний
Время идентификации 1 000 посетителей	1	1/2	1/7	1/9
Количество ошибок 1 рода (отказов) на 1 000 считываний	2	1	1/5	1/7
Возможность применения в ММПЛ	7	5	1	1/4
Количество ошибок 2 рода на 1 000 считываний	9	7	4	1

Расчет локального приоритета x_i i-го критерия производится по формуле 3.4. Результат расчета локальных приоритетов критериев приведен в табл. 3.6.

$$x_i = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}}}{\sum_{k=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{kj}}}, \quad (3.4)$$

где a_{ij} – результат попарного сравнения i-й и j-й альтернатив (критериев); n – количество альтернатив (критериев), $i = 1..n$, $j = 1..n$, $k = 1..n$.

Таблица 3.6 – Числовые оценки матрицы попарных сравнений для критериев

Критерии	Локальный приоритет критерия (вес критерия), x_i
Время идентификации 1 000 посетителей	0,04598
Количество ошибок 1 рода (отказов) на 1 000 считываний	0,07532
Возможность применения в ММПЛ	0,26494
Количество ошибок 2 рода на 1 000 считываний	0,61376

Метод анализа иерархий требует проведения проверки согласованности попарного сравнения альтернатив (критериев). Известно, что согласованность положительной обратно-симметричной матрицы эквивалентна требованию равенства ее максимального собственного значения λ_{max} с n. Метод полагает оценку отклонения от согласованности разностью $\lambda_{max} - n$, разделенной на $(n - 1)$, которая обозначается индексом согласованности (ИС). Условием согласованности матрицы является то, что отношение согласованности (ОС), равное отношению рассчитанного ИС к среднему ИС для матрицы того же размера, не превышает 10%. Расчеты производятся на основании формул (3.5)–(3.8). Оценка согласованности матрицы попарных сравнений критериев показала следующие результаты, приведенные в табл. 3.7.

$$\text{ИС} = \frac{\lambda_{max} - n}{n - 1}, \quad (3.5)$$

$$\lambda_{max} = X \cdot Y = (x_1, x_2, ..., x_n) \cdot (y_1, y_2, ..., y_n), \quad (3.6)$$

$$Y = (y_1, y_2, ..., y_n) = \left(\sum_{j=1}^{n} a_{1j}, \sum_{j=1}^{n} a_{2j}, ..., \sum_{j=1}^{n} a_{nj} \right), \quad (3.7)$$

$$\text{ОС} = \frac{\text{ИС}}{\text{ИСр}}, \quad (3.8)$$

где λ_{max} – собственное число матрицы; n – количество альтернатив (критериев), размерность матрицы; X – вектор локальных приоритетов; Y – вектор суммарных оценок матрицы по столбцам; a_{ij} – оценка попарного сравнения i-й альтернативы по отношению к j-й; ИСр – средний индекс согласованности для матрицы размера n.

Таблица 3.7. Численные результаты оценки согласованности для матрицы попарных сравнений критериев

λ_{max}	n	ИС	ИСр	ОС	Результат
4,229	4	0,0763	0,9	8,48 %	Значение ОС < 10 % соответствует условию согласованности матрицы

Аналогичным образом производилась оценка альтернатив по каждому из критериев. Попарное сравнение производилось на основе измеренных значений критериев для сравниваемых подходов (альтернатив). Значения попарных сравнений и оценка согласованности для каждого случая приведены в табл. 3.8–3.15.

Таблица 3.8. Числовые оценки матрицы попарных сравнений и оценка их согласованности для альтернатив по критерию «Время идентификации 1 000 посетителей»

Альтернативы	Предложенный подход	Подход на основе бесконтактных карт-идентификаторов	Подход с помощью проверки документа	Локальный приоритет альтернативы
Предложенный подход	1	1/3	9	0,308610
Подход на основе бесконтактных карт-идентификаторов	3	1	9	0,641935
Подход с помощью проверки документа	1/9	1/9	1	0,049455

Таблица 3.9. Численные результаты оценки согласованности для матрицы попарных сравнений альтернатив по критерию «Время идентификации 1 000 посетителей»

λ_{max}	*n*	ИС	Иср	ОС	Результат
3,135611	3	0,067805	0,58	7,53 %	Значение ОС < 10 % соответствует условию согласованности матрицы

Таблица 3.10. Числовые оценки матрицы попарных сравнений и оценка их согласованности для альтернатив по критерию «Количество ошибок 1 рода (отказов) на 1 000 считываний»

Альтернативы	Предложенный подход	Подход на основе бесконтактных карт-идентификаторов	Подход с помощью проверки документа	Локальный приоритет альтернативы
Предложенный подход	1	5	1/6	0,188134
Подход на основе бесконтактных карт-идентификаторов	1/5	1	1/9	0,056207
Подход с помощью проверки документа	6	9	1	0,755659

Таблица 3.11. Численные результаты оценки согласованности для матрицы попарных сравнений альтернатив по критерию «Количество ошибок 1 рода (отказов) на 1000 считываний»

λ_{max}	*n*	ИС	Иср	ОС	Результат
3,16323	3	0,08162	0,58	9,07 %	Значение ОС < 10 % соответствует условию согласованности матрицы

Таблица 3.12. Числовые оценки матрицы попарных сравнений и оценка их согласованности для альтернатив по критерию «Возможность применения в ММПЛ»

Альтернативы	Предложенный подход	Подход на основе бесконтактных карт-идентификаторов	Подход с помощью проверки документа	Локальный приоритет альтернативы
Предложенный подход	1	9	1	0,473684
Подход на основе бесконтактных карт-идентификаторов	1/9	1	1/9	0,052632
Подход с помощью проверки документа	1	9	1	0,473684

Таблица 3.13. Численные результаты оценки согласованности для матрицы попарных сравнений альтернатив по критерию «Возможность применения в ММПЛ»

λ_{max}	n	ИС	Иср	ОС	Результат
3	3	0	0,58	0 %	Значение ОС < 10 % соответствует условию согласованности матрицы

Таблица 3.14. Числовые оценки матрицы попарных сравнений и оценка их согласованности для альтернатив по критерию «Количество ошибок 2 рода на 1000 считываний»

Альтернативы	Предложен-ный подход	Подход на основе бесконтактных карт-идентификаторов	Подход с помощью проверки документа	Локальный приоритет альтернативы
Предложенный подход	1	1	9	0,473684
Подход на основе бесконтактных карт-идентификаторов	1	1	9	0,473684
Подход с помощью проверки документа	1/9	1/9	1	0,052632

Таблица 3.15. Численные результаты оценки согласованности для матрицы попарных сравнений альтернатив по критерию «Количество ошибок 2 рода на 1000 считываний»

λ_{max}	n	ИС	Иср	ОС	Результат
3	3	0	0,58	0 %	Значение ОС < 10 % соответствует условию согласованности матрицы

Глобальный приоритет s_i i-ой альтернативы рассчитывается с учетом локальных приоритетов критериев и альтернатив в рамках каждого исследуемого критерия по формуле (3.9). Результаты расчетов глобальных приоритетов альтернативных подходов приведены в табл. 3.16.

$$s_i = \sum_{j=1}^{n} x(A_i, K_j) \cdot x(K_j), \qquad (3.9)$$

где n – количество критериев (n = 4); s_i – глобальный приоритет i-ой альтернативы, i = 1, 2, 3; $x(A_i, K_j)$ – локальный приоритет i-ой альтернативы в рамках j-го критерия; $x(K_j)$ – локальный приоритет j-го критерия.

Таблица 3.16 – Сводная таблица рассчитанных локальных приоритетов и рассчитанные значения глобальных приоритетов альтернатив

Альтернативы	Время идентификации 1000 посетителей (K_1)	Количество ошибок 1 рода (отказов) на 1000 считываний (K_2)	Возможность применения в ММПЛ (K_3)	Количество ошибок 2 рода на 1000 считываний (K_4)	Глобальный приоритет Альтернативы A_i (S_i)
	Численное значение локального вектора приоритета, $x(Kj)$				
	0,04598	0,07532	0,26494	0,61376	
Предложенный подход (A_1)	0,308610	0,188134	0,473684	0,473684	0,444588
Подход на основе бесконтактных карт-идентификаторов (A_2)	0,641935	0,056207	0,052632	0,473684	0,338422
Подход с помощью проверки документа (A_3)	0,049455	0,755659	0,473684	0,052632	0,216990

Полученные результаты оценки приоритетов альтернатив показали, что предложенный подход к идентификации и аутентификации в СКУД ММПЛ на основе современных идентификационных признаков имеет наивысший приоритет (s_1 = 0,444588) и, следовательно, является наилучшей альтернативой по выделенным критериям. В свою очередь удовлетворение подхода данным критериям показывает достоверность проведения процедуры идентификации, возможность использования в ММПЛ, отказоустойчивость и адекватное время срабатывания всех механизмов проверки.

3.4 Выводы

В ходе проведенного анализа было установлено, что на сегодняшний день мобильные устройства связи могут быть использованы в качестве идентификаторов доступа. Данные обстоятельства позволили автору сделать предположение о возможности применения подобных идентификационных признаков в СКУД ММПЛ.

В данной главе подробно рассмотрен предложенный автором подход, который заключается в использовании мобильных устройств в качестве идентификаторов для ПИАФ электронных проходных СКУД ММПЛ, отличающийся возможностью варьирования набора идентификационных данных и технологий их передачи в соответствии с требуемым уровнем защищенности объекта. При этом, отличительной особенностью подхода является отсутствие зависимости от конкретных протоколов и технологий передачи данных.

В качестве примеров реализации рассмотрены предложенные автором схема генерации секретного ключа и алгоритмы аутентификации на основе таких технологий передачи данных, как использование QR-кодов и NFC-меток. Данные алгоритмы легли в основу разработанной автоматизированной системы усиленной аутентификации «I-mob».

Оценка эффективности и адекватности предложенных автором методики верификации и подхода к идентификации и аутентификации в СКУД ММПЛ была проведена путем сравнения с аналогами. При этом в случае с методикой были определены количественные критерии сравнения и проведен практический эксперимент. Для оценки подхода использован метод анализа иерархий, позволяющий осуществить многокритериальный выбор наилучшей альтернативы.

Апробация показала, что предложенная методика верификации субъекта доступа эффективнее аналогичных решений с точки зрения массовости применения. Результаты оценки предложенного подхода к идентификации и аутентификации в СКУД ММПЛ показали, что он имеет наивысший приоритет по сравнению с аналогами и, как следствие, является наилучшей альтернативой по выделенным критериям.

ЗАКЛЮЧЕНИЕ

Идентификация личности является одним из ключевых мероприятий в обеспечении безопасности посетителей ММПЛ. Несмотря на актуальность этой задачи и существование различных технических решений в области СКУД, нерассмотренными остаются вопросы идентификации посетителей в случае если ММПЛ не подлежит обязательной охране полицией, а его особенности функционирования не позволяют внедрить полноценный пропускной режим. Существующие СКУД не позволяют организовать идентификацию посетителей подобных объектов без нарушения протекающих бизнес-процессов. Вместе с тем, наблюдается недостаток представленных в литературе методических рекомендаций, программного и алгоритмического обеспечения процесса идентификации посетителей в ММПЛ.

Автором выявлены особенности функционирования ММПЛ и проблемы в организации КПР на их территории, которые послужили предпосылками поиска современных идентификационных признаков и разработки нового научно обоснованного технического решения в области идентификации личности, имеющего существенное значение для усовершенствования системы обеспечения общественной безопасности страны. В результате проведенного диссертационного исследования была достигнута поставленная цель в повышении эффективности процесса идентификации посетителей в местах массового пребывания людей за счет применения современных идентификационных признаков. Автором предложено методическое и программно-алгоритмическое обеспечение исследуемого процесса.

В рамках методического обеспечения предложены:

1) модель процесса идентификации в системах контроля и управления доступом для мест массового пребывания людей;

2) методика верификации субъекта доступа при удаленной регистрации на основе механизма доверенных лиц;

3) подход к идентификации и аутентификации в системах контроля и управления доступом мест массового пребывания людей.

Программно-алгоритмическое обеспечение включает в себя:

– алгоритм аутентификации на основе применения QR-кодов;

– алгоритм аутентификации на основе применения NFC-меток;

– систему усиленной мобильной аутентификации «I-mob»;

– программу для двухфакторной аутентификации на основе современных идентификационных признаков «TFAS».

Апробация системы усиленной мобильной аутентификации «I-mob» в Акционерном обществе «ОЭЗ ТВТ «Томск» позволила организовать процедуру удаленной регистрации и верификацию пользователей, а также сократить общее время, затрачиваемое на регистрацию на 17%, что подтверждается актом внедрения (Приложение 2). Внедрение программы для двухфакторной аутентификации на основе современных идентификационных признаков «TFAS» в СКУД Общества с ограниченной ответственностью «Удостоверяющий центр Сибири» позволило применять мобильные устройства в качестве идентификаторов доступа. При этом эксплуатация в течение 5 месяцев показала, что уровень ошибок 1 рода составил не более 0,3%, а фактов некорректной аутентификации (ошибок 2 рода) за указанный период зафиксировано не было, что подтверждается актом внедрения (Приложение 2).

Теоретические наработки, изложенные в данном диссертационном исследовании, используются в учебном процессе ТУСУРа, что подтверждается актом внедрения (Приложение 2).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Косов Ю.В. Международный терроризм как глобальная проблема [Электронный ресурс] / Ю.В. Косов // Anthropology : web-кафедра философской антропологии. – Электрон. текст. дан. – [Б. м.], 2004. – URL: http://anthropology.ru/ru/text/kosov-yuv/mezhdunarodnyy-terrorizm-kak-globalnaya-problema (дата обращения: 02.03.2015).

2. UN Global Counter-Terrorism Strategy [Electronic resource] // United Nations. Counter-Terrorism Implementation Task Force. – Electronic data. – [S. l., 2016]. – URL: https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy (access date: 22.08.2016).

3. Корнаухова Т.В. От борьбы к профилактике терроризма / Т.В. Карнаухова // Известия ВУЗов. Поволжский регион. Общественные науки. – 2012. – № 4 (24). – С. 26–33.

4. Inside Germany’s Controversial Terrorism Plan [Electronic resource] // Fortuna. – Electronic data. – [S. l., 2016]. – URL: http://fortune.com/2016/08/24/germany-action-plan-counter-terrorism/ (access date: 22.08.2016).

5. Концепция общественной безопасности в Российской Федерации : утв. Президентом РФ 20 ноября 2013 г. [Электронный ресурс] // Гарант : информационно-правовой портал. – Электрон. текст. дан. – М., 2013. – URL: http://www.garant.ru/products/ipo/prime/doc/70425172/ (дата обращения: 05.07.2014).

6. Бреев А.В. Основные меры противодействия терроризму в Российской Федерации / А.В. Бреев // Юридическая наука. – 2012. – № 2. – С. 111–114.

7. Алексеев О.Н. Противодействие терроризму в США: опыт и проблемы / О.Н. Алексеев // Теория и практика общественного развития. – 2012. – № 7. – С. 201–203.

8. Combating terrorism [Electronic resource] // Federal Foreign Office. – Electronic data. – [Berlin], 2016. – URL: http://www.auswaertiges-

amt.de/EN/Aussenpolitik/GlobaleFragen/TerrorismusOK/Terrrorismus_node.html (access date: 22.08.2016).

9. Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий) : постановление Правительства РФ от 25 марта 2015 г. № 272 [Электронный ресурс] // Гарант : информационно-правовое обеспечение. – Электрон. текст. дан. – М., 2015. – URL: http://base.garant.ru/ 70937940/ (дата обращения: 30.12.2015).

10. Об антитеррористической защищенности объектов (территорий) : постановление Правительства Российской Федерации от 25 декабря 2013 г. № 1244 [Электронный ресурс] // Гарант : информационно-правовое обеспечение. – Электрон. текст. дан. – М., 2013. – URL: http://base.garant.ru/ 70552494/ (дата обращения: 01.07.2014).

11. О безопасности : федеральный закон от 28 декабря 2010 г. № 390-ФЗ (с изм. и доп.) [Электронный ресурс] // Гарант : информационно-правовое обеспечение. – Электрон. текст. дан. – М., 2016. – URL: http://base.garant.ru/ 12181538/ (дата обращения: 08.07.2016).

12. О противодействии терроризму : федеральный закон от 06 марта 2006 г. № 35-ФЗ (ред. от 06.07.2016) [Электронный ресурс] // Гарант : информационно-правовое обеспечение. – Электрон. текст. дан. – М., 2006. – URL: http://www.garant.ru/hotlaw/federal/134216/ (дата обращения: 01.09.2016).

13. О стратегии национальной безопасности Российской Федерации до 2020 года : указ Президента от 12 мая 2009 г. № 537 [Электронный ресурс] // Российская газета. – Электрон. текст. дан. – М., 2009. – URL: https://rg.ru/ 2009/05/19/strategia-dok.html (дата обращения: 23.05.2015).

14. Белоножкин В.И. Информационные аспекты противодействия терроризму / В.И. Белоножкин, Г.А. Остапенко. – М. : Горячая линия – Телеком, 2015. – 112 с.

15. Рыкунов В. Охранные системы и технические средства физической защиты объектов / В. Рыкунов. – М. : Секьюрити Фокус, 2011. – 288 с.

16. Африн А.Г. Методы и средства контроля и управления доступом в АСУ ТП на основе биометрических характеристик пользователя : дис. … канд. техн. наук / А.Г. Африн. – Оренбург, 2008. – 163 с.

17. Грушо А.А. Безопасные архитектуры распределенных систем // А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина, С.Я. Шоргин // Системы и средства информатики. – 2014. – Т. 24, вып. 3. – С. 18–31.

18. Меньших В.В. Автоматная модель действий злоумышленника на охраняемом объекте / В.В. Меньших, Д.Ю. Калков // Вестник Воронежского института МВД России. – 2014. – № 2. – С. 196–200.

19. Волхонский В.В. Теоретические и методологические основы функционирования устройств и систем обеспечения комплексной безопасности объектов информатизации : автореф. дис. … д-ра техн. наук. – СПб., 2011. – 34 с.

20. Dmitrienko A. Security and privacy aspects of mobile platforms and applications : Doktor-Ingenieurs genehmigte Dissertation / A. Dmitrienko. – Darmstadt, 2015. – 186 p.

21. Багринцева О.В. Разработка моделей и алгоритмов автоматизированного контроля доступа пользователей к информации в интегрированных системах безопасности : автореф. дис. … канд. техн. наук / О.В. Багринцева. – Воронеж, 2015. – 16 с.

22. Якоб Д.А. Разработка методики исследования особенностей функционирования информационных контрольно-пропускных систем : дис. … канд. техн. наук : 05.13.01 / Д.А. Якоб. – Екатеринбург, 2013. – 163 с.

23. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2009. – 28 с.

24. Tsankov P. Access Control Synthesis for Physical Spaces [Electronic resource] / P. Tsankov, D. Torabi. D.A. Basin. – ETH-Zürich, 2016. – Doi: 10.3929/ethz-a-010635851. – URL: http://e-collection.library.ethz.ch/eserv/eth:48966/eth-48966-01.pdf (access date: 22.08.2016).

25. Ворона В.А. Концептуальные основы создания и применения системы защиты объектов / В.А. Ворона, В.А. Тихонов. – М. : Горячая линия – Телеком, 2015. – 184 с. – (Обеспечение безопасности объектов, вып. 1).

26. Ворона В.А. Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. – М. : Горячая линия – Телеком, 2015. – 272 с. – (Обеспечение безопасности объектов, вып. 2).

27. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 13 февраля 2013 № 17 [Электронный ресурс] // ФСТЭК России. – Электрон. текст. дан. – М., 2013. – URL: http://fstec.ru/component/attachments/download/566 (дата обращения: 09.10.2014).

28. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. – М. : Стандартинформ, 2010. – 30 с.

29. Рыжова В.А. Проектирование и исследование комплексных систем безопасности / В.А. Рыжова. – СПб.: НИУ ИТМО, 2012. – 157 с.

30. Ворона В.А. Охранные подразделения / В.А. Ворона, В.А. Тихонов. – М. : Горячая линия – Телеком, 2012. – 211 с. – (Обеспечение безопасности объектов, вып. 6).

31. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов / Ю.Б. Михайлов. – М. : Горячая линия – Телеком, 2015. – 322 с.

32. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2012. – 16 с.

33. Определение и классификация средств и систем контроля и управления доступом [Электронный ресурс] / КОМКОМ : системы безопасности. – Электрон. дан. – М., 2014. – URL: http://www.comcom.ru/baza_znanij/detail/11413/ (дата обращения: 09.04.2015)

34. Выбор и применение систем контроля и управления доступом : рекомендации Р 78.36.005-2011 / М-во внутренних дел РФ, Департамент гос. защиты имущества. – М., 2011. – 77 с.

35. Исхаков А.Ю. Двухфакторная аутентификация на основе программного токена / А.Ю. Исхаков, Р.В. Мещеряков, И.А. Ходашинский // Вопросы защиты информации. – 2013. – № 3 (102). – С. 23–28.

36. An embedded access control system for restricted areas in smart buildings [Electronic resource] / H.S. Maciel [et al.] // 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech). – Doi: 10.1109/SpliTech.2016.7555926. – URL: https://www.researchgate.net/publication/307572918_An_embedded_access_control_system_for_restricted_areas_in_smart_buildings (access date: 22.08.2016).

37. Мельников Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. – М. : Флинта : Наука, 2013. – 448 с.

38. Нотация IDEF0 [Электронный ресурс] / Документация Business Studio. – Электрон. дан. – [Б. м., б. г.]. – URL: http://www.businessstudio.ru/wiki/docs/v4/doku.php/ru/csdesign/bpmodeling/idef0 (дата обращения: 03.12.2015).

39. Методология функционального моделирования IDEF0 : руководящий документ : офиц. изд. / Госстандарт России. – М., 2000. – 75 с.

40. Исхаков А.Ю. Модель процесса идентификации в системах контроля и управления доступом / А.Ю. Исхаков // Вестник СибГУТИ. – 2016. – № 1. – С. 93–98.

41. Руководство по составлению спецификаций на СКУД : пер с англ. / Британская Ассоциация индустрии безопасности. – М. : Секьюрити Фокус, 2014. – 170 с.

42. Explanations and Relaxations for Policy Conflicts in Physical Access Control [Electronic resource] / F. Turkmen // IEEE 25th International Conference on Tools with Artificial Intelligence (ICTAI). – Doi: 10.1109/ICTAI.2013.57. – URL: http://ieeexplore.ieee.org/document/6735268/?reload=true&arnumber=6735268 (access date: 10.07.2016).

43. Как выбрать турникет? [Электронный ресурс] // Каталог СКУД. Антитеррроризм 2015. – М., 2015. – С. 20–21. – Электрон. версия печатн. публ. – URL: http://www.secuteck.ru/imag/accesscontrol-0-2015/ (дата обращения: 01.02.2016).

44. СКУД как часть антитеррористической защиты критически важных объектов [Электронный ресурс] // Системы безопасности. – 2016. – № 2. – С. 64–67. – Электрон. версия печатн. публ. – URL: http://www.secuteck.ru/ imag/ss-2-2016/ (дата обращения: 01.09.2016).

45. Anomaly analysis for physical access control security configuration [Electronic resource] / W.M. Fitzgerald [et al.] // 7th International Conference on Risks & Security of Internet and Systems (CRiSIS). – Doi: 10.1109/CRISIS.2012.6378953. – URL: https://www.computer.org/csdl/proceedings/crisis/2012/3087/00/p16.pdf (access date: 10.06.2016).

46. Исхаков А.Ю. Автоматизированная система учета посещений Особой экономической зоны технико-внедренческого типа «Томск» / А.Ю. Исхаков // Научная сессия ТУСУР–2013 : материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 16–18 мая 2013 г. : в 5 ч. – Томск : В-Спектр, 2012. – Ч. 4. – С. 147–150.

47. Тесаков В. Эффективное применение турникетов в офисных зданиях [Электронный ресурс] / В. Тесаков // Технологии защиты. – 2015. – № 5. – Электрон. версия печатн. публ. – URL: http://www.tzmagazine.ru/jpage.php?uid1=1348&uid2=1450&uid3=1465 (дата обращения: 11.05.2016).

48. Интернет-СМИ освободят от ответственности за комментарии читателей // Известия. – 2016. – 05 мая.

49. Быков О. Что надо знать, заказывая карты Mifare для СКД / О. Быков // Алгоритм безопасности. – 2011. – № 4. – С. 40–41.

50. Быков О. Перевод СКУД с карт EM MARIN на карты MIFARE® : полезные сведения для владельца объекта СКД [Электронный ресурс] / О. Быков // Avtoritet.Net. – Электрон. дан. – [Б. м.], 2014. – URL: http://avtoritet.net/library/press/245/8158/articles/8745 (дата обращения: 05.08.2015).

51. Рынок контроля доступа в России 2016 [Электронный ресурс] // Каталог СКУД. Антитеррористм 2016. – М., 2016. – С. 8–13. – Электрон. версия печатн. публ. – URL: http://www.secuteck.ru/imag/accesscontrol-0-2016/ (дата обращения: 01.08.2016).

52. Филатова Н.Н. Структурный синтез схем автоматизации в условиях неполных требований к технической реализации / Н.Н. Филатова, А.Г. Требухин // Известия ВолгГТУ. – 2012. – № 13. – С. 72–79.

53. Олифер В. Компьютерные сети : принципы, технологии, протоколы : учебник / В. Олифер, Н. Олифер. – 5-е изд. – СПб. : Питер, 2016. – 992 с.

54. Stockley M. Browser fingerprints – the invisible cookies you can’t delete [Electronic resource] / M. Stockley // Nakedsecurity by sophos. – Electronic data. – [S. l.], 2014. – URL: https://nakedsecurity.sophos.com/2014/12/01/browser-fingerprints-the-invisible-cookies-you-cant-delete/ (access date: 22.08.2016).

55. Исхаков А.Ю. Исследование уязвимостей веб-приложений методом грубой силы / А.Ю. Исхаков, А.О. Шумская // Технологии Microsoft в теории и практике программирования : сборник трудов IX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / Том. политехн. ун-т. – Томск : Изд-во Том. политехн. ун-та, 2012. – С. 280–281.

56. Shet V. Are you a robot? Introducing “No CAPTCHA reCAPTCHA” [Electronic resource] / V. Shet // Google Security Blog. – Electronic data. – [S. l.], 2014. – URL: https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html (access date: 22.08.2016).

57. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учеб. пособие / А.А. Афанасьев [и др.]. – М. : Горячая линия – Телеком, 2012. – 550 с.

58. DRAFT NIST Special Publication 800-63B Digital Authentication Guideline [Electronic resource] / Federal Information Processing Standards // National Institute of Standards and Technology. – Electronic data. – [S. 1.], 2016. – URL: https://pages.nist.gov/800-63-3/sp800-63b.html (access date: 15.09.2016).

59. Niemiec M. Federated identity in real-life applications [Electronic resource] / M. Niemiec, W. Kolucka-Szypula. – Networks and Communications (EuCNC), 2015 European Conference. – Doi: 0.1109/EuCNC.2015.7194124. – URL: http://ieeexplore.ieee.org/document/7194124/ (access date: 20.07.2016).

60. Gouriev D. A new protocol for Single Sign-on for the web / D. Gouriev, K. Belemuk // International Journal of Open Information Technologies. – 2014. – № 6. – P. 21–24.

61. Единая система идентификации и аутентификации (ЕСИА) [Электронный ресурс] // Минкомсвязь России. – Электрон. дан. – М., 2016. – URL: http://minsvyaz.ru/ru/activity/directions/13/ (дата обращения: 18.07.2016).

62. Koussa S. Federated Identities: OpenID vs SAML vs OAuth [Electronic resource] / S. Koussa // Software Secured. – Electronic data. – [S. l.], 2014. – URL: https://softwaresecured.com/federated-identities-openid-vs-saml-vs-oauth/ (access date: 22.08.2016).

63. Что такое универсальная электронная карта [Электронный ресурс] // УЭК. – Электрон. дан. – М., 2016. – URL: http://www.uecard.ru/for-citizens/ what-is-uec/ (дата обращения: 17.08.2016).

64. Об электронной подписи : федеральный закон от 06 апреля 2011 г. № 63-ФЗ (дейст. ред. от 2016) [Электронный ресурс] // КонсультантПлюс : официальный сайт. – Электрон. дан. – [Б. м.], 2016. – URL: http://www.consultant.ru/ document/cons_doc_LAW_112701/ (дата обращения: 03.09.2016).

65. Количество зарегистрированных граждан в ЕСИА выросло на 2,7 млн в конце 2015 года [Электронный ресурс] // Минкомсвязь России. – Электрон. дан. – М., 2016. – URL: http://minsvyaz.ru/ru/events/34565/ (дата обращения: 14.04.2016).

66. Малков А.А. Оценка времени премодерации в автоматизированных системах социальной аутентификации / А.А. Малков, Л.Н. Кротов, Е.Л. Кротова // Информационные технологии моделирования и управления. – 2012. – № 1 (73). – С. 21–27.

67. Fourth-Factor Authentication: Somebody You Know [Electronic resource] / J. Brainard [et al.] // Gibson Research Corporation. – Electronic data. – [S. l.], 2006. – URL: https://www.grc.com/sn/files/The_Fourth_Factor.pdf (access date: 10.01.2015).

68. Introducing Trusted Contacts [Electronic resource] // Facebook. – Electronic data. – [S. l.], 2013. – URL: https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts/10151362774980766/ (access date: 20.07.2014).

69. Малков А.А. Технология аутентификации с помощью доверенных лиц : автореф. дис. … канд. техн. наук / А.А. Малков. – Уфа, 2013. – 16 с.

70. Исхаков А.Ю. Методика верификации личности субъекта доступа при удаленной регистрации с помощью доверенных лиц / А.Ю. Исхаков // Доклады ТУСУРа. – 2016. – № 3.

71. Попов Г.А. Анализ параметров информационной безопасности автоматизированных систем на основе использования уточненных экспертных оценок / Г.А. Попов, Е.А. Попова, А.В. Мельников // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2015. – № 1. – С. 33–39.

72. Ахаев А.В. Алгоритм оценивания функционального наполнения программных продуктов на основе нечеткого логического вывода / А.В. Ахаев // Доклады ТУСУР. – 2013. – № 2 (28). – С. 169–174.

73. Schechter S. It’s Not What You Know, but Who You Know: A Social Approach to Last-resort Authentication / S. Schechter, S. Egelman, R.W. Reeder // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09). – New York, 2009. – P. 1983–1992. –Doi: 10.1145/1518701.1519003. 99.

74. Российский рынок продаж мобильных телефонов, смартфонов и планшетных ПК : итоги 1-го квартала 2016 года [Электронный ресурс] // Мобильные телекоммуникации. – Электрон. дан. – М., 2016. – URL: http://www.mobilecomm.ru/rossijskij-rynok-prodazh-mobilnyh-telefonov-smartfonov-i-planshetnyh-pk-itogi-1-go-kvartala-2016-goda (дата обращения: 01.08.2016).

75. Бочкова Н.И. Сравнительный анализ решений по передаче голоса в мобильных сетях широкополосного доступа / Н.И. Бочкова, С.М. Ярлыкова // T-Comm. – 2013. – № 7. – С. 16–19.

76. ITU Statistic [Electronic resource] // Committed to connected the world. – Electronic data. – Geneva, 2016. – URL: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (access date: 02.07.2016).

77. Российский рынок бытовой техники и электроники: во 2 квартале 2016 продолжается позитивный тренд продаж [Электронный ресурс] // GfK. – Электрон. дан. – М., 2016. – URL: http://www.gfk.com/ru/insaity/press-release/rossiiskii-rynok-bytovoi-tekhniki-i-ehlektroniki-vo-2-kvartale-2016-prodolzhaetsja-pozitivnyi-trend-prodazh/ (дата обращения: 12.08.2016).

78. Montjoye Y.-A. de Unique in the Crowd: The privacy bounds of human mobility [Electronic resource] / Y.-A. de Montjoye, C.A. Hidalgo, M. Verleysen, V.D. Blondel // Scientific Reports. – 2013. – Vol. 3. – Doi 10.1038/srep01376. – URL: http://www.nature.com/articles/srep01376 (access date: 11.05.2015).

79. BYOD: концепция, технологии и решения [Электронный ресурс] // СвязьКомплект. – Электрон. дан. – М., 2016. – URL: https://skomplekt.com/solution/byod.htm (дата обращения: 01.08.2016).

80. Bring Your Own Device [Electronic resource] // Microsoft. – Electronic data. – [S. l.], 2016.– URL: https://www.microsoftstore.com/store/msusa/en_US/cat/BYOD/categoryID.69993600 (access date: 01.08.2016).

81. Kaneshige T. VMware Going 'All In' with BYOD [Electronic resource]/ T. Kaneshige // CIO. – Electronic data. – [S. l.], 2012.– URL: http://www.cio.com/ article/2396105/byod/vmware-going--all-in--with-byod.html (access date: 01.08.2016).

82. Embrace BYOD Now [Electronic resource] // SAP: The Best-Run Businesses Run SAP. – Electronic data. – [S. l.], 2012.– URL: http://fm.sap.com/byod/ (access date: 22.08.2016).

83. The New Workplace: Supporting “Bring your own” [Electronic resource] / IBM. – Somers, NY, 2012. – The electronic version of the printing publication. – URL: http://www-935.ibm.com/services/in/en/attachments/pdf/The_New_Workplace_Supporting_Bring_your_own.pdf (access date: 22.08.2016).

84. Технические средства и методы защиты информации : учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, А.А. Солдатов. – 4-е изд., испр. и доп. – М. : Горячая линия – Телеком, 2012. – 616 с.

85. Ворона В.А. Теоретические основы обеспечения безопасности объектов информатизации : учеб. пособие для вузов / В.А. Ворона, В.А. Тихонов, Л.В. Митрякова. – М. : Горячая линия – Телеком, 2016. – 304 с.

86. Практическое руководство по безопасности и защите ваших данных при использовании мобильных телефонов [Электронный ресурс] // We fight censorship. – Электрон. дан. – [Б. м.], 2016. – URL: http://www.wefightcensorship.org/ru/article/prakticheskoe-rukovodstvo-po-bezopasnosti-i-zashchite-vashih-dannyh-pri-ispolzovaniihtml.html (дата обращения: 25.08.2016).

87. Мобильный доступ – безопасные решения мобильного контроля доступа [Электронный ресурс] // HID Global. – Электрон. дан. – [Б. м.], 2016. –

URL: https://www.hidglobal.ru/solutions/mobile-access (дата обращения: 25.08.2016).

88. Карты и идентификаторы iCLASS SE – Карты для работы с защищенными объектами идентификации (SIO) с поддержкой многих приложений [Электронный ресурс] // HID Global. – Электрон. дан. – [Б. м.], 2016. – URL: https://www.hidglobal.ru/products/cards-and-credentials/iclass-se (дата обращения: 24.07.2016).

89. Исхаков А.Ю. Система аутентификации на основе QR-кодов / А.Ю. Исхаков // Научная сессия ТУСУР – 2013 : материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 16–18 мая 2013 г. : в 5 ч. – Томск : В-Спектр, 2012. – Ч. 4. – С. 147–150.

90. Исхаков А.Ю. Недостатки NFC меток при аутентификации / А.Ю. Исхаков // Ползуновский вестник. – 2013. – № 2. – С. 267–269.

91. NFC Forum Technical Specifications [Electronic resource] // NFC Forum. – Electronic data. – [S. l.], 2016.– URL: http://members.nfc-forum.org/specs/spec_list/ (access date: 10.09.2016).

92. Coskun V. Near Field Communication (NFC) : From Theory to Practice / V. Coskun, K. Ok , B. Ozdenizci. – [S. l.] : Wiley, 2011. – 636 p.

93. Smartphones and BLE Services: Empirical Insights [Electronic resource] / M. Radhakrishnan [et al.] // Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference, Dallas, TX, 2015. – P. 226–234. – Doi: 10.1109/MASS.2015.92. – URL: http://ieeexplore.ieee.org/document/7366936/citations (access date: 10.07.2016).

94. Announcing the Advanced Encryption Standard (AES) [Electronic resource] / Federal Information Processing Standards // National Institute of Standards and Technology. – Electronic data. – [S. l.], 2001. – URL: (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (access date: 19.05.2015).

95. Bluetooth core specification [Electronic resource] // National Institute of Bluetooth SIG, Inc. – Electronic data. – [S. l.], 2016. – URL:

https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy (access date: 10.07.2016).

96. Ul Haq M.S. Design and implementation of sandbox technique for isolated applications [Electronic resource] / M.S. Ul Haq, L. Liao, M. Lerong // 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, 2016. – P. 557–561. – Doi: 10.1109/ITNEC.2016.7560422. – URL: http://ieeexplore.ieee.org/document/7560422/ (access date: 07.09.2016).

97. Гутковская О.Л. Контурный метод анализа сетей VPN [Электронный ресурс] / О.Л. Гутковская, Д.Ю. Пономарев // Современные проблемы науки и образования. – 2015. – № 1-1. – Электрон. версия печатн. публ. – URL: http://cyberleninka.ru/article/n/konturnyy-metod-analiza-setey-vpn#ixzz4LSH4u9fs (дата обращения: 20.02.2016).

98. Iskhakov A.Yu. Choosing a Method for Generating One-Time Passwords and an Information Transport Technology in the Authentication System for ACS / A.Yu. Iskhakov, R.V. Meshcheryakov, I.A. Hodashinsky // Proceedings of 2014 International Conference on Network Security and Communication Engineering (NSCE 2014), Hong Kong, December 25–26, 2014. – London : CRC Press, 2015. – P. 15–17.

99. Исхаков А.Ю. Система двухфакторной аутентификации на основе QR-кодов / А.Ю. Исхаков // Безопасность информационных технологий. – 2014. – № 3. – С. 97–101.

100. Технология NFC [Электронный ресурс] // Techportal.ru. – Электрон. дан. – [Б. м.], 2016. – URL: http://www.techportal.ru/glossary/technology-nfc.html (дата обращения: 27.08.2016).

101. What is a Secure Element? [Electronic resource] // Rambus Bell ID. – Electronic data. – [S. l.], 2014. – URL: https://www.bellid.com/blog/what-is-a-secure-element/ (access date: 09.05.2015).

102. Android 4.4 KItkat [Электронный ресурс] // Android. – Электрон. дан. – [Б. м.], 2016. – URL: https://www.android.com/intl/ru_ru/versions/kit-kat-4-4/ (дата обращения: 27.07.2016).

103. Как настроить и пользоваться Apple Pay в России // MacDigger. – Электрон. дан. – [Б. м.], 2016. – URL: http://www.macdigger.ru/iphone-ipod/kak-nastroit-i-polzovatsya-apple-pay-v-rossii.html (дата обращения: 10.08.2016).

104. An implementation of QR code encoder for Objective-C ported from Psytec library [Electronic resource] // GitHub, Inc. – Electronic data. – [S. l.], 2016. – URL: https://github.com/myang-git/QR-Code-Encoder-for-Objective-C (access date: 11.07.2016).

105. Исхаков А.Ю. Обеспечение безопасности web-приложения / А.Ю. Исхаков // Студент и научно-технический прогресс : Информационные технологии : материалы 50 Международной научной студенческой конференции / Новосиб. гос. ун-т. – Новосибирск, 2012. – С. 54.

106. Исхаков А.Ю. Фаззинг веб-приложений / А.Ю. Исхаков // Студент и научно-технический прогресс : Информационные технологии : материалы 50 Международной научной студенческой конференции / Новосиб. гос. ун-т. – Новосибирск, 2012. – С. 39

107. Исхаков А.Ю. Автоматизация выявления уязвимостей веб-сайтов / А.Ю. Исхаков // Сборник трудов молодых ученых и сотрудников кафедры ВТ / под ред. Т.И. Алиева. – СПб. : ИТМО, 2013. – С. 70–73

108. Саати Т. Принятие решений : метод анализа иерархий / Т. Саати. – М. : Радио и связь, 1993. – 278 с.

109. Коробов В.Б. Преимущества и недостатки метода анализа иерархий / В.Б. Коробов, А.Г. Тутыгин // Известия РГПУ им. А.И. Герцена. – 2010. – № 122. – С. 108-115.

ПРИЛОЖЕНИЕ 1
Свидетельства о регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015663362

I-mob. Система усиленной мобильной аутентификации

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники» (RU)***

Автор: ***Исхаков Андрей Юнусович (RU)***

Заявка № **2015660401**
Дата поступления **29 октября 2015 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***16 декабря 2015 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015663283

"TFAS. Программа для двухфакторной аутентификации на основе современных идентификационных признаков"

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР) (RU)***

Авторы: ***Исхаков Андрей Юнусович (RU),***
Мещеряков Роман Валерьевич (RU)

Заявка № **2015619374**
Дата поступления **07 октября 2015 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***15 декабря 2015 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

ПРИЛОЖЕНИЕ 2

Акты внедрения

Экз.№1

АО «ОСОБАЯ ЭКОНОМИЧЕСКАЯ ЗОНА
ТЕХНИКО-ВНЕДРЕНЧЕСКОГО ТИПА «ТОМСК»
Академический проспект, 8/8,
г. Томск, 634055
тел. (3822) 488-650, факс (3822) 488-665
office@oez.tomsk.ru
ОКПО 95124992 , ОГРН 1067017162420
ИНН/КПП 7017153992/701701001

www.russez.ru

_____ № _____

На № _____ от _____

«УТВЕРЖДАЮ»
Советник генерального директора
по безопасности
_____ М.Г. Клименко
«12» _____ 2016 г.

АКТ

О внедрении результатов кандидатской диссертационной работы

Исхакова Андрея Юнусовича

Комиссия в составе:
Начальник службы безопасности - Сорокин Евгений Викторович
Начальник управления правового обеспечения – Клименко Сергей Валерьевич
Руководитель группы администрирования и развития ИТ – Булдаков Александр Владимирович
составила настоящий акт о нижеследующем.

Особая экономическая зона технико-внедренческого типа «Томск» предоставляет современную инфраструктуру для компаний, занимающихся инновационным бизнесом. В список объектов ОЭЗ ТВТ «Томск» входят 3 офисных здания, общая площадь которых составляет более 35 000 м^2. Все здания являются местами массового пребывания людей, поскольку каждое из них ежедневно посещают более 700 человек. Для обеспечения безопасности на объектах действуют пропускной и внутриобъектовый режимы.

В рамках совместной деятельности ТУСУРа и АО «ОЭЗ ТВТ «Томск» результаты диссертационной работы Исхакова А.Ю. используются для повышения эффективности процесса идентификации посетителей.

Разработанное Исхаковым А.Ю. программное обеспечение (ПО) «Система усиленной мобильной аутентификации «I-mob» использовалось для апробации предложенной им методики

удаленной верификации субъекта доступа и подхода к идентификации и аутентификации посетителей. Применение данной системы позволило организовать процедуру удаленной регистрации и верификации пользователей. ПО реализовано в виде веб-ориентированного приложения, что позволяет использовать его на различных программных и аппаратных платформах и значительно повышает практическую ценность.

Результаты работы Исхакова А.Ю. внедрены в деятельность ОЭЗ ТВТ «Томск», благодаря чему были достигнуты следующие показатели:

1. Апробация разработок Исхакова А.Ю. в течение 4 месяцев подтвердила эффективность предложенной методики с точки зрения сокращения общего времени, затрачиваемого на регистрацию, на 17%. С точки зрения массовости применения предложенная методика верификации личности на основе доверенных лиц является в несколько раз более эффективной используемых ранее решений. Адекватность методики, выраженная в достоверности проведения процедуры верификации, подтверждается отсутствием выявленных ошибок.

2. Комиссия отмечает целесообразность использования модели процесса идентификации, методики верификации субъекта доступа, подхода к идентификации и аутентификации, а также методического и программного-алгоритмического обеспечения для повышения эффективности процесса идентификации посетителей на реальных объектах с массовым пребыванием людей.

Настоящий акт составлен в 3 (трех) экземплярах.

Начальник службы безопасности — Е.В. Сорокин

Начальник управления правового обеспечения — С.В. Клименко

Руководитель группы администрирования и развития ИТ — А.В. Булдаков

Экз. №1

Удостоверяющий центр Сибири

Общество с ограниченной ответственностью
«Удостоверяющий центр Сибири»

634009, г. Томск, пр-т Ленина, 110
ИНН/КПП/ОГРН 7017311494/701701001/1127017020767

тел: (382 2) 900-111
факс: (382 2) 900-111
e-mail: office@udcs.ru
http:// www.udcs.ru

г. Томск «30» августа 2016 г.

А К Т

о внедрении результатов диссертационной работы

Исхакова Андрея Юнусовича

Настоящий акт составлен о том, что результаты диссертационного исследования Исхакова А.Ю. внедрены в деятельность ООО «УЦ Сибири». В марте 2016 г. в систему контроля и управления доступом компании был внедрен программный комплекс «TFAS», позволяющий использовать мобильные средства связи в качестве идентификаторов доступа. Программный комплекс был сконфигурирован на выполнение процедур усиленной аутентификации посредством технологии одноразовых паролей. Апробация в течение 5 месяцев показала, что уровень ошибок 1 рода составил не более 0,3%. При этом фактов некорректной аутентификации (ошибок 2 рода) на протяжении всего периода эксплуатации зафиксировано не было.

В связи с этим считаем целесообразным использование предложенных Исхаковым А.Ю. подхода к идентификации и аутентификации, а также методического и программного-алгоритмического обеспечения с целью повышения эффективности идентификации посетителей на реальных объектах.

Настоящий акт составлен в 3 (трех) экземплярах.

Директор А.В. Перфильев

Зам. директора Н.С. Михайлов

Специалист по защите информации А.В. Котенко

Экз. № 1

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ
И РАДИОЭЛЕКТРОНИКИ»**

ТУСУР

ОКПО 02069326, ОГРН 1027000867068,
ИНН 7021000043, КПП 701701001

пр. Ленина, 40, г. Томск, 634050

тел: (382 2) 510-530
факс: (382 2) 513-262, 526-365
e-mail: office@tusur.ru
http:// www.tusur.ru

_____№ _____

УТВЕРЖДАЮ
Проректор ТУСУР по учебной работе
_____ П.Е. Троян
«26» 09 2016г.

АКТ
о внедрении результатов диссертационной работы
Исхакова Андрея Юнусовича в учебный процесс

Комиссией в составе:

Председатель комиссии – Давыдова Е.М, к.т.н., декан факультета безопасности ТУСУР

Члены комиссии:

Костюченко Е.Ю., к.т.н., доцент каф. КИБЭВС ТУСУР;

Евсютин О.О., к.т.н., доцент каф. БИС ТУСУР;

составлен настоящий акт о нижеследующем.

Результаты диссертационной работы А.Ю. Исхакова «Методическое и программно-алгоритмическое обеспечение процесса идентификации посетителей в местах массового пребывания людей» используются в учебном процессе на факультете безопасности ТУСУР при чтении лекций по дисциплинам «Основы информационной безопасности» и «Программно-аппаратные средства обеспечения информационной безопасности» для подготовки специалистов по защите информации, обучающихся по специальностям «10.05.03 – Информационная безопасность

автоматизированных систем» и «10.05.04 – Информационно-аналитические системы безопасности».

В курсе по дисциплине «Основы информационной безопасности» используются предложенная Исхаковым А.Ю. модель процесса идентификации в СКУД в местах массового пребывания людей, а также методика верификации личности субъектов доступа на основе механизма доверенных лиц при удаленной регистрации.

В курсе «Программно-аппаратные средства обеспечения информационной безопасности» используются результаты диссертационной работы Исхакова А.Ю. по формированию подхода к идентификации и аутентификации в СКУД, основанного на использовании мобильных устройств в качестве идентификаторов.

Студенты в ходе выполнения групповых проектов и научно-исследовательских работ факультета безопасности имеют возможность ознакомиться с результатами проведенных Исхаковым А.Ю. исследований.

Настоящий акт составлен в 3 (трех) экземплярах.

к.т.н., декан факультета безопасности
Давыдова Е.М. _____ «29» 08 2016 г.

к.т.н, доцент каф. КИБЭВС
Костюченко Е.Ю. _____ «19» 08 2016 г.

к.т.н, доцент каф. БИС
Евсютин О.О. _____ «29» 08 2016 г.

ПРИЛОЖЕНИЕ 3

Сравнение технологий Bluetooth, BLE, NFC

Техническая спецификация	Bluetooth	Bluetooth с низким энергопотреблением	Near field communication
Радиочастота	2.4 ГГц	2.4 ГГц	13.56 МГц
Расстояние	до 100 м	более 100 м	до 0.2 м
Скорость передачи данных по воздуху	1-3 Мб/с	1 Мб/с	424 кбит/с
Ведомые устройства	7	Не предопределено; зависит от реализации	1
Безопасность	64/128-bit и определяемый пользователем прикладной уровень	128-bit AES с Counter Mode CBC-MAC и определяемый пользователем прикладной уровень	Предполагается использование прикладного уровня криптозащиты
Надежность	Адаптивная быстрая перестройка частоты, FEC, быстрый ACK	Адаптивная быстрая перестройка частоты, Lazy Acknowledgement, 24-битовый избыточный циклический код (CRC), 32-разрядная проверка целостности сообщения	Определяется режимом работы (технологией кодирования). В том числе проверка целостности
Задержка (от неподключенного состояния)	100 мс	6 мс	1 мс
Минимальное общее время передачи данных (зависит от состояния батареи)	100 мс	3 мс	1 мс
Государственное регулирование	Во всем мире		
Орган по сертификации	Bluetooth SIG	Bluetooth SIG	NFC Forum
Передача голоса	Да	Нет	Нет
Топология сети	Scatternet	Scatternet	Двухточечная сеть
Максимально потребляемый ток	<30 мА	<15 мА	50 мА
Обнаружение службы	Да	Да	Да
Определение конфигурации	Да	Да	Да
Варианты использования	Мобильные телефоны, игры, наушники, стерео аудио потоки, автомобили, ПК и т. д.	Мобильные телефоны, игры, ПК, часы, спорт и физкультура, здравоохранение, автомобили, бытовая электроника, автоматизация, промышленность и т. д.	Системы безопасности, автомобильные системы, сопровождение товаров, системы «Умный дом» и т.д.

ПРИЛОЖЕНИЕ 4

IDEF0-диаграмма блока удаленной регистрации посетителя без подтверждения личности