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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Томск – 2016

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)

Научный руководитель – Мещеряков Роман Валерьевич,
доктор технических наук, профессор

Официальные оппоненты: Якунин Алексей Григорьевич,
доктор технических наук, профессор,
заведующий кафедрой информатики, вычислительной техники и информационной безопасности Алтайского государственного технического университета,
г. Барнаул

Шамин Алексей Алексеевич,
кандидат технических наук, заведующий отделом разработки микропроцессорных терминалов
ООО «НТП Киберцентр»,
г. Томск

Ведущая организация – федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет» (ФГБОУ ВО «ТГТУ»)

Защита состоится «22» декабря 2016 г. в 10 часов 00 мин. на заседании диссертационного совета Д 212.268.03 на базе ТУСУРа адресу: 634050, г. Томск, пр. Ленина, 40, ауд. 203.

С диссертацией можно ознакомиться в библиотеке ТУСУРа по адресу: 634045, г. Томск, ул. Красноармейская, 146 и на сайте https://storage.tusur.ru/files/51443/dissertation.pdf

Автореферат разослан « ____ » _____ 2016 г.

Ученый секретарь диссертационного совета  Зыков Дмитрий Дмитриевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В современном мире одной из наиболее значимых угроз безопасности населения является международный терроризм. Стремясь распространить среди мирного населения панику, страх и сомнения в силах государственных структур, преступники в качестве объектов посягательств выбирают места массового пребывания людей (ММПЛ). Для нейтрализации подобных угроз спецслужбы всего мира предпринимают различные действия по усилению мер безопасности на таких объектах. На сегодняшний день строгое определение ММПЛ отсутствует, хотя действующим законодательством РФ установлены критерии категорирования подобных мест и требования к их антитеррористической защищенности.

В общем случае под ММПЛ понимаются общественные места с высокой плотностью человеческих потоков и вероятностью возникновения неуправляемой толпы. Подобные свойства характерны для самых разнообразных объектов. Это не только вокзалы, аэропорты и метрополитены, но и большие офисные здания, кинозалы, театры, и т.д. Одним из базовых мероприятий по обеспечению антитеррористической защищенности является внедрение контрольно-пропускного режима (КПР). Поскольку КПР предполагает исключение несанкционированного прохода на охраняемую территорию, одной из важнейших задач в его реализации является идентификация личности посетителей.

Для транспортной инфраструктуры, критически важных объектов, некоторых государственных и муниципальных учреждений законодательство жестко регламентирует реализацию КПР, в т.ч. в части решения задачи идентификации посетителей, с обязательным привлечением сотрудников полиции. В остальных случаях законом определена лишь ответственность собственника ММПЛ за безопасность людей, находящихся на его территории. Примерами таких объектов являются выставочные комплексы; кинозалы; офисные центры, площади которых арендуются множеством различных компаний и т.д. Зачастую администрация таких ММПЛ, действуя в угоду бизнес-процессам, использует пропускной режим для недопущения тех, кто не оплатил билет, а также решения различных статистических задач, не подразумевающих идентификацию личности посетителей (подсчет количества проходов, маркетинговые исследования и т.д.). Этот факт значительно упрощает беспрепятственный проход на объект злоумышленников, позволяет им без каких-либо усилий слиться с толпой мирных граждан. Кроме того, отсутствие сведений о посетителях затрудняет расследование преступлений и различных инцидентов органами безопасности.

В рамках данной работы под ММПЛ понимаются не подлежащие обязательной охране силовыми структурами категории объектов массового пребывания людей, особенности функционирования которых не позволяют внедрить полноценный пропускной режим. Анализ литературы показал, что решение задачи идентификации личности в различных аспектах представлено в работах А.Г. Сабанова, В.А. Вороны, Ю.Ю. Громова, А.Г. Якунина, В.А. Тихонова, Р.В. Мещерякова, А.А. Малюка, Г.А. Остапенко, А.А. Шелупанова, А.А. Малкова,

В.В. Волхонского, B. Schneier, J. Brainard, S. Schechter, N. Skandhakumar, S. Egelman, R.W. Reeder, а также ряда других отечественных и зарубежных ученых. Исследования особенностей управления большими потоками посетителей ММПЛ проводились такими учеными как С.В. Поршнев, В.В. Холщевников, А.А. Егоров и др. Например, в диссертации Д.А. Якоба представлена методика исследования особенностей функционирования контрольно-пропускных систем 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.

Политика тотальной проверки и регистрации паспортных данных посетителей неприменима в ММПЛ ввиду ее негативного влияния на протекающие бизнес-процессы. Использование современных СКУД позволяет автоматизировать процесс идентификации посетителей, однако требует их предварительной регистрации. Традиционный способ регистрации предполагает посещение субъектом доступа охраняемого объекта с целью подтверждения личности и получения пропуска. Реализация такого подхода в ММПЛ зачастую приводит к увеличению временных затрат и нарушению бизнес-процессов. Учитывая, что наиболее распространенным видом пропусков являются бесконтактные карты доступа, для ММПЛ характерна проблема организации изготовления, выдачи и оперативного управления идентификаторами. Существующие сервисы удаленной регистрации позволяют посетителю дистанционно внести идентификационные сведения, но не решают проблему подтверждении личности (верификации), так как в большинстве случаев невозможно убедиться в достоверности представленной информации.

Таким образом, особенности функционирования исследуемых объектов и наличие проблем с организацией КПР на их территории обусловливают актуальность задачи по разработке методических рекомендаций, программного и алгоритмического обеспечения, позволяющих организовать идентификацию посетителей ММПЛ без нарушения протекающих в них 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 внедрены в деятельность ООО «Удостоверяющий центр Сибири», АО «ОЭЗ ТВТ «Томск», в учебный процесс ТУСУРа по дисциплинам «Основы информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», а также использованы 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 и 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулирована цель, определены основные задачи, научная новизна и практическая значимость полученных результатов, а также положения, выносимые на защиту.

Первая глава посвящена вопросам идентификации в СКУД и особенностям организации данного процесса в ММПЛ. Сформулированы основные задачи СКУД, рассмотрены классификация, структура подобных комплексов и примеры их реализации. Дано формализованное описание задачи идентификации, построена модель процесса идентификации в СКУД и проведена ее адаптация для применения в ММПЛ.

Пусть в подсистеме идентификации и аутентификации (ПИАФ) зарегистрировано n субъектов доступа. При этом в момент регистрации i-го субъекта доступа создается его образ p_i – 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 и номер пропуска, рабочая частота используемой технологии передачи данных, PIN-код,

физиологические или поведенческие признаки человека. 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, а устройство считывания (УС) создает его образ, который используется для сравнения с образами, хранящимися в БД СКУД. Если в БД 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.

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.

Поскольку УС принимает и обрабатывает переданные ему образы для идентификации, а затем преобразует их в формат контроллера, его работу можно представить в виде выражения (1).

$$\hat{p}_k = F(\hat{p}), \qquad (1)$$

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. Для формализации данной задачи введем понятие меры близости:

$$Q(\hat{p}_k, p_i) - \text{мера близости между образами } \hat{p}_k \text{ и } p_i,\ p_i \in P,\ i = \overline{1..n}. \quad (2)$$

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. Мера сравнения может быть рассчитана с использованием расстояния Хэмминга, коэффициента парной корреляции, вероятностных оценок метода Байеса или 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:

$$Q(\hat{p}, p_i) = \Phi(\hat{z}, D_i),\ i = \overline{1..n}; \quad (3)$$

$$\hat{p} = p_i : \Phi(\hat{z}, D_i) \equiv \begin{cases} \min\left(\Phi(\hat{z}, D_i)\right), \text{если } \Phi - \text{метрика близости}, \\ \max\left(\Phi(\hat{z}, D_i)\right), \text{если } \Phi - \text{метрика различимости}, \end{cases} \quad (4)$$

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

Выражение (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 ограничениями выступают выражения (5) и (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.

$$\hat{p} \notin P : \Phi(\hat{z}, D_i) \le \lambda,\ p_i \in P,\ D_i \in D,\ i = \overline{1..n}, \quad (5)$$

$$\hat{p} \notin P : \Phi(\hat{z}, D_i) > \lambda,\ p_i \in P,\ D_i \in D,\ i = \overline{1..n}. \quad (6)$$

Условие (5) необходимо применять в случае использования метрики близости, а выражение (6) – при использовании метрики различимости.

На рис. 1 представлена декомпозиция первого уровня контекстной IDEF0-диаграммы процесса идентификации в СКУД. Первым этапом является проверка необходимости регистрации субъекта доступа в системе, затем происходит предъявление идентификатора пользователя. Далее в соответствии с конфигурацией СКУД и правилами осуществления КПР с предъявленного идентификатора выделяется набор идентификационных признаков, который проходит проверку на соответствие элементам множества P.

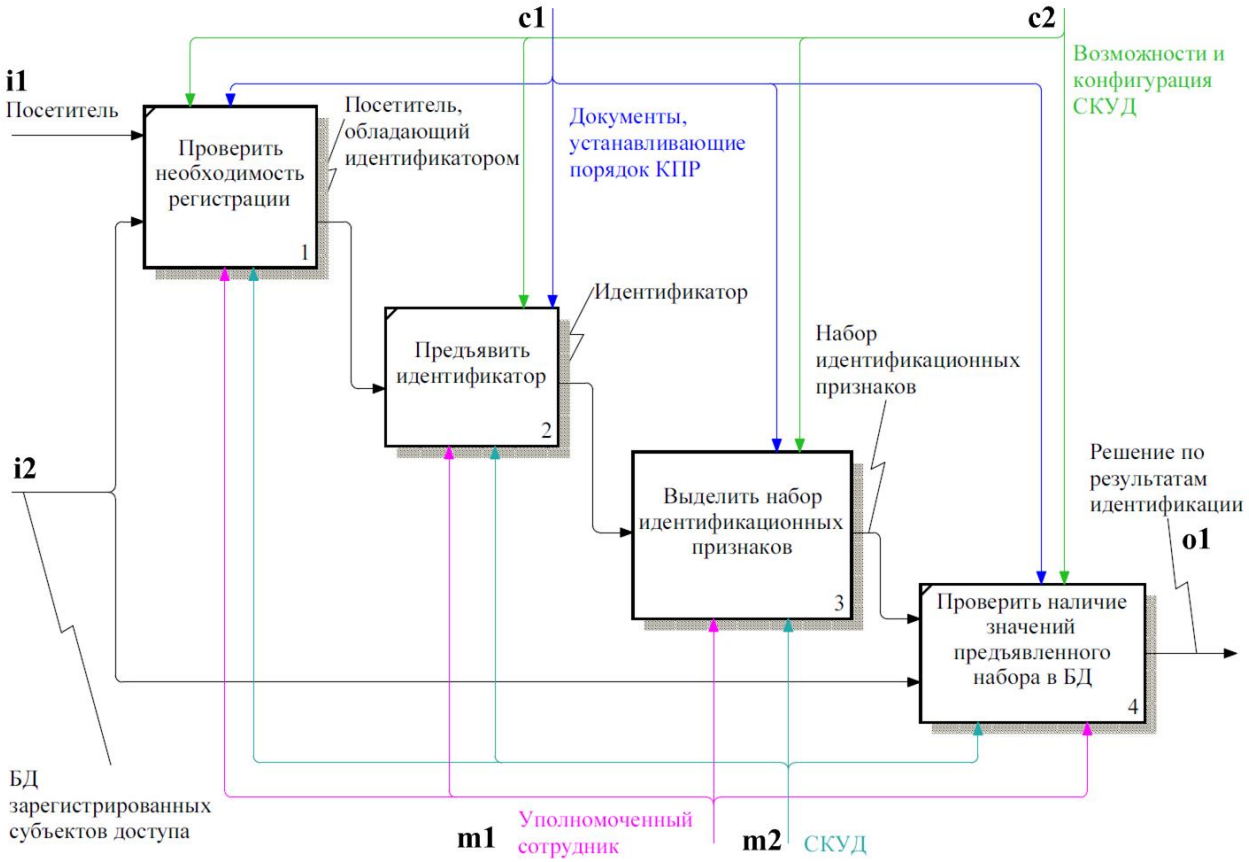

Рисунок 1 – Декомпозиция первого уровня IDEF0-диаграммы процесса идентификации в СКУД

Формирование множества *P* представляет собой процедуру регистрации пользователей в СКУД, являющуюся неотъемлемым этапом процесса идентификации. 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). Завершающим этапом является выдача субъекту доступа индивидуального пропуска в виде электронной карты, RFID-метки и т.д. При биометрической 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. Учитывая, что ММПЛ характеризуются большими потоками посетителей, в т.ч. заинтересованных в однократном визите, применение традиционной процедуры регистрации и выдачи пропуска в большинстве случаев невозможно, поскольку требует предварительного посещения объекта и приводит к замедлению бизнес-процессов.

В связи с этим автором предлагается адаптировать модель процесса идентификации в СКУД для ее применения в ММПЛ. Исходя из вышеизложенного, можно заключить что процедура регистрации субъектов доступа в СКУД ММПЛ должна быть предельно автоматизирована. Другими

словами, все действия на этапе регистрации должны проводиться удаленно и без привлечения оператора. Для этого автором предлагается предусмотреть возможность удаленной регистрации субъектов доступа. Проведенный анализ показал, что существующие механизмы верификации при удаленной регистрации недостаточно распространены для использования в ММПЛ. Например, верификация посредством таких инструментов как электронная подпись (ЭП) или «подтвержденная» учетная запись ФГИС «ЕСИА» осложнена их малой распространенностью среди населения ввиду необходимости предварительного посещения уполномоченного учреждения. Поэтому зачастую системы вообще не предусматривают процедуру подтверждения личности. Учитывая, что исключение верификации ставит под сомнение эффективность идентификации в целом, то использование удаленной регистрации в ММПЛ возможно только при условии сохранения процедуры подтверждения личности.

Также в исследовании отмечено, что использование СКУД в ММПЛ обусловливает проблемы оперативного управления, обслуживания и затрат на выпуск идентификаторов доступа. В связи с этим автором предлагается установить требования к адаптируемой модели, заключающиеся в предоставлении 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.

Также необходимо учесть, что используемые технологии транспорта идентификационных данных должны предусматривать проведение аутентификации для обеспечения необходимого уровня защищенности ММПЛ. Учитывая вышеизложенное, 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 «Оператор» из диаграммы процедуры регистрации (рис. 2).

Во второй главе проведен анализ существующих механизмов установления личности в автоматизированных системах. Установлено, что использование подтвержденных учетных записей ФГИС «ЕСИА», а также применение технологий ЭП удовлетворяют выдвинутым автором требованиям к разрабатываемой методике верификации. Однако, при использовании данных

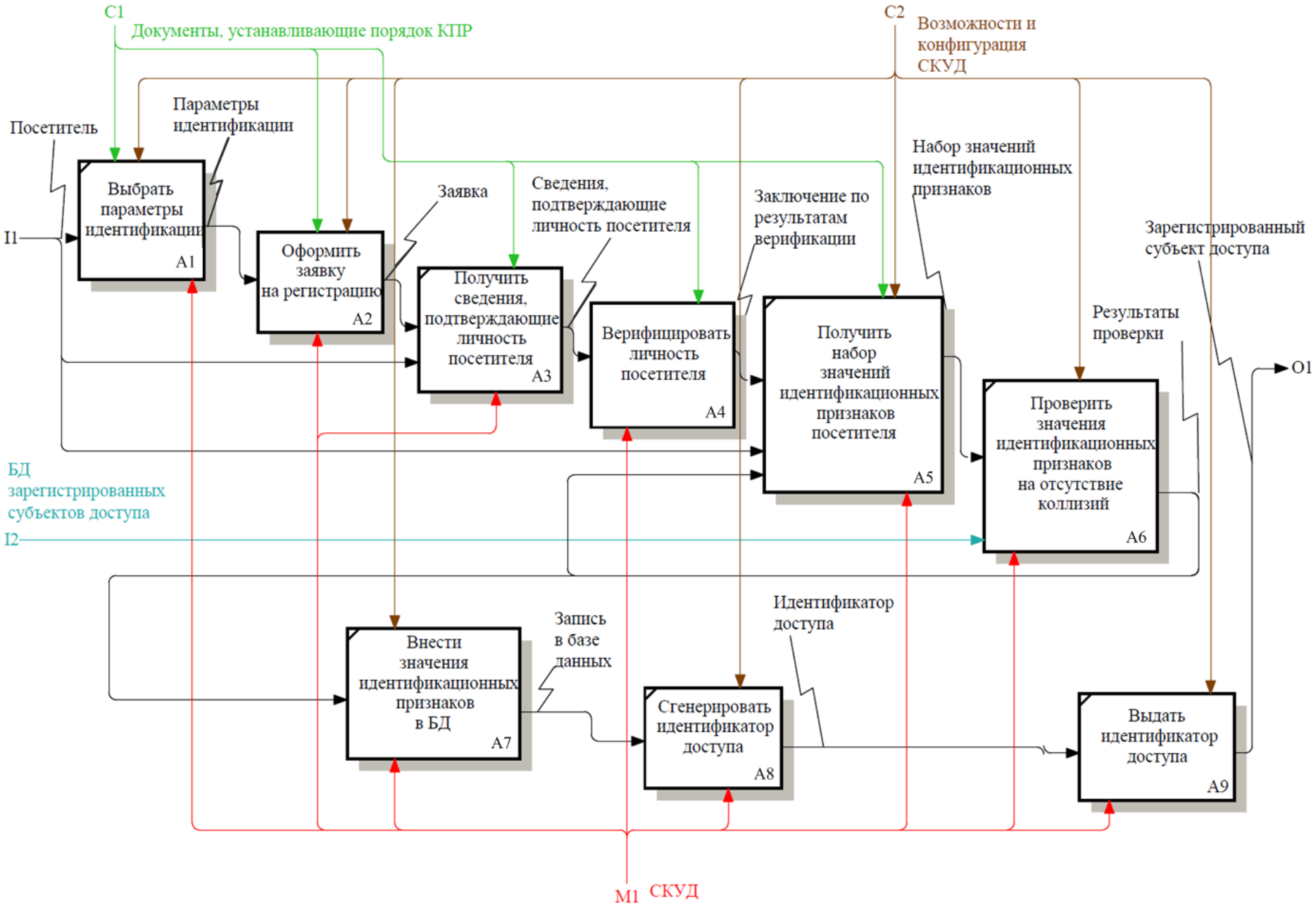

Рисунок 2 – Декомпозиция блока «Зарегистрировать посетителя» IDEF0-диаграммы модели процесса идентификации в СКУД ММПЛ

механизмов ограничивающим фактором является необходимость предварительного посещения уполномоченного учреждения (удостоверяющего центра, почтового отделения и т.д.).

Автором предлагается проводить верификацию субъекта доступа с помощью механизма доверенных лиц, подразумевающего подтверждение личности регистрируемого другими пользователями. При этом они должны обладать необходимыми привилегиями и лично удостовериться в правомерности совершения запрашиваемой операции.

Назначение методики: организация процесса подтверждения личности субъекта на этапе 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;

S_2 – множество зарегистрированных субъектов доступа;

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

При этом выполняются 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 подтверждения 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 $\hat{s}$, причем $i = 2..n$;

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 $s_k \in \acute{S}$;

R – множество интегральных оценок r_k компетентных доверенных лиц;

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:

$$y_{k1} = f_{\text{Harrington}}(\hat{y}_{k1}), \tag{7}$$

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. 1):

$$f_{\text{Harrington}}(x) = \begin{cases} 0{,}1, \text{ если } \lambda = 1; \\ 0{,}285, \text{ если } \lambda = 2; \\ 0{,}5, \text{ если } \lambda = 3; \\ 0{,}715, \text{ если } \lambda = 4; \\ 0{,}9, \text{ если } \lambda = 5. \end{cases} \tag{8}$$

4.5 *VS* оценивает компетенцию d_k субъекта $s_k \in S'$, используя нормированные оценки ответов δ_{ij} (пример оценок приведен в табл. 2). 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:

$$d_k = \frac{\sum_{i=2}^{n} y_{ki}}{\sum_{i=1}^{n} \max_j(\delta_{ij})}. \tag{9}$$

4.6 *VS* рассчитывает интегральную оценку r_k субъекта s_k:

$$r_k = \begin{cases} y_{1k} \cdot d_k, \text{ если } d_k \geq l_1; \\ 0, \text{ иначе.} \end{cases} \tag{10}$$

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

$$\exists\ R = \{r_k \mid r_k \neq 0\} \text{ и } |R| \geq l_2. \tag{11}$$

В случае выполнения условия – переход к шагу 4.7.

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

$$g(R, l_2) = \begin{cases} \textit{Истина}, \text{ если } F_{\text{Harrington}}\left[\frac{\sum_{k=1}^{m} r_k}{m}\right] \geq l_2; \\ \textit{Ложь}, \text{ иначе.} \end{cases}, \tag{12}$$

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. 1):

$$F_{\text{Harrington}}(x) = \begin{cases} \lambda = 1, \text{ если } x \in [0; 0,2]; \\ \lambda = 2, \text{ если } x \in (0,2; 0,37]; \\ \lambda = 3, \text{ если } x \in (0,37; 0,63]; \\ \lambda = 4, \text{ если } x \in (0,63; 0,8]; \\ \lambda = 5, \text{ если } x \in (0,8; 1]. \end{cases} \quad (13)$$

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.

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. 1 представлен предлагаемый состав содержательно описываемых наименований ее градаций, соответствующие им количественные значения и числовые интервалы. Данная шкала позволяет измерить степень интенсивности критериального свойства, имеющего субъективный характер.

Таблица 1 – 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. Данный шаг позволяет количественно оценить компетенцию доверенного лица, т.е. способность объективно верифицировать личность регистрируемого субъекта.

Таблица 2 – 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 шаге 4.1 системе *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) Исходя из результатов исследований J. Brainard , в данной методике подразумевается 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:

- письменное согласие (при посещении объекта доступа);
- подписание согласия средствами квалифицированной ЭП;
- подписание согласия «подтвержденной учетной записью» ФГИС «ЕСИА».

На рис. 3 представлен алгоритм применения предложенной методики.

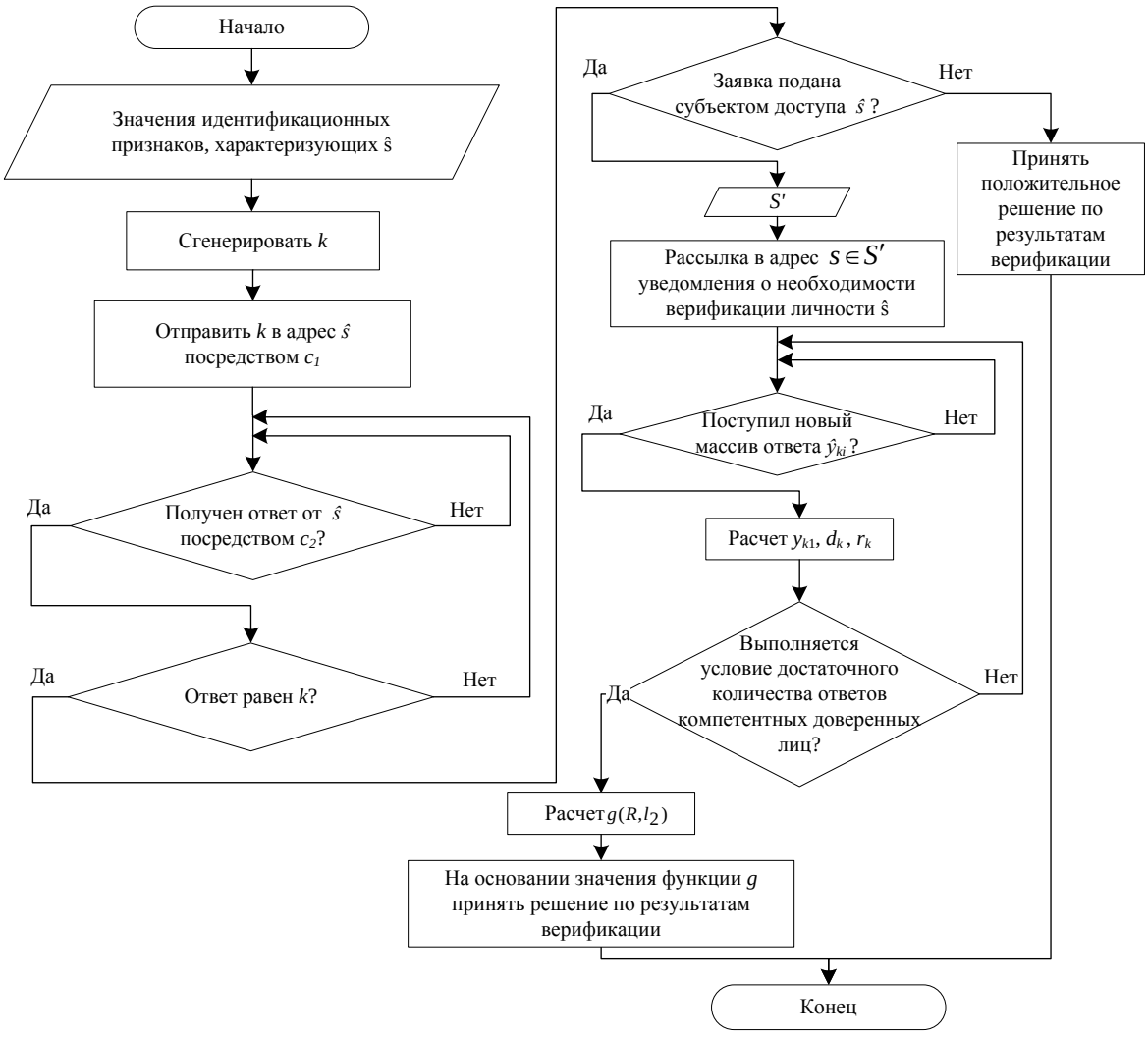

Рисунок 3 – Блок-схема алгоритма применения методики системой *VS*

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

В третьей главе изложен подход к идентификации и аутентификации в СКУД ММПЛ, а также представлены результаты апробации предложенного автором методического и программно-алгоритмического обеспечения.

Концепция подхода предполагает использование мобильных устройств в качестве идентификаторов доступа. Проведенный автором анализ существующих вариантов применения мобильных устройств связи в качестве идентификаторов доступа позволил выделить следующие недостатки при их использовании в СКУД ММПЛ:

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

– отсутствие документации, регламентирующей организацию ПИАФ в СКУД ММПЛ;

– проприетарность алгоритмов и используемого ПО.

Предлагаемый подход предоставляет возможность владельцу объекта в соответствии с требуемым уровнем защищенности ММПЛ самостоятельно определить набор идентификационных данных, а также технологий их передачи в СКУД, что обеспечивает гибкость и возможность масштабирования ПИАФ. В целях достижения универсальности подхода, а также массового применения построенных на его основе систем, автором не выдвигались требования к технологиям транспорта идентификационной информации. Подход предполагает возможность применения механизмов усиленной аутентификации, позволяющих защитить передаваемые данные от возможной компрометации злоумышленником. В качестве примера реализации подобных механизмов автором предлагается применять технологию одноразовых паролей (OTP). При этом, в качестве основы секретного ключа k используются следующие компоненты:

– численное значение графического пароля g для запуска приложения. В постоянной памяти 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 постоянного запоминающего устройства;

– случайный набор бит b, который сохраняется в скрытой области памяти 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. 4 представлена схема формирования сообщения M, предназначенного для передачи УС.

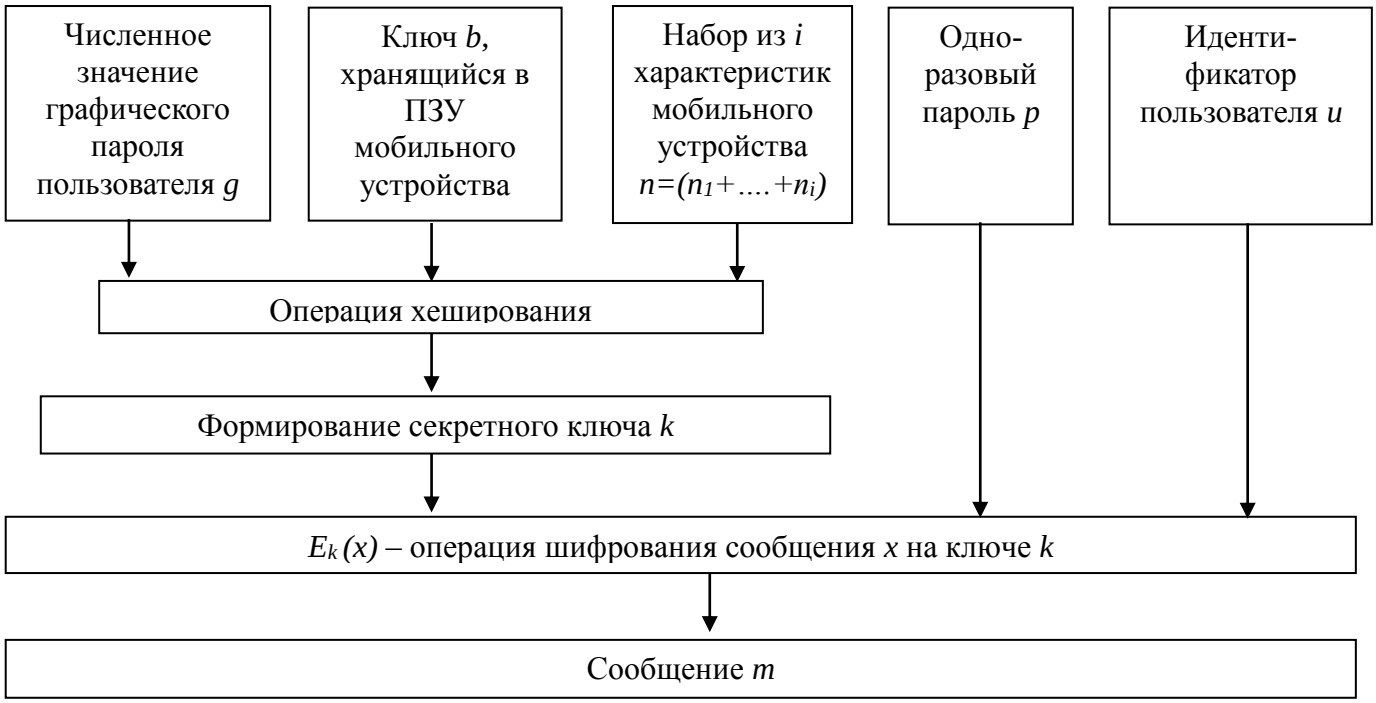

Рисунок 4 – Пример схемы формирования сообщения *m*, содержащего одноразовый пароль

Вторым фактором аутентификации выступает защита от несанкционированного доступа к приложению-аутентификатору (в случае потери или кражи) посредством применения графических паролей. Такие пароли содержат два взаимодополняющих компонента: изображение из пользовательской мультимедиа-библиотеки и набор жестов, рисуемых поверх изображения. Использование личных изображений повышает безопасность и запоминаемость пароля.

Автором предложены алгоритмы аутентификации, в основе которых лежат технологии передачи данных в виде QR кодов и динамических NFC меток. В качестве примера на рисунке 5 представлена схема аутентификации в режиме передачи QR кодов.

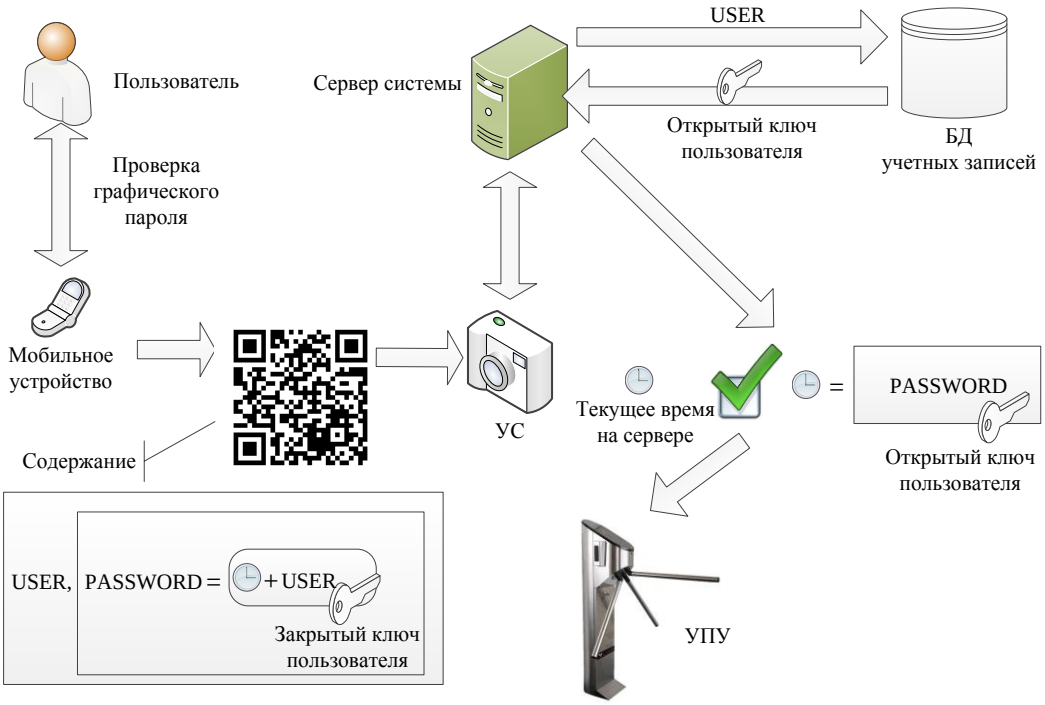

Рисунок 5 – Схема аутентификации в режиме передачи QR кодов

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

$$F(u,g,b,n) = Q\left(u \times E_{R[H(g*b*n),l]}(u \oplus t)\right) \quad (14)$$

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; ×, *, ⊕ – 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*.

Алгоритмическое обеспечение аутентификации с использованием технологии передачи данных в виде QR кодов представлено на блок-схемах рис. 6.

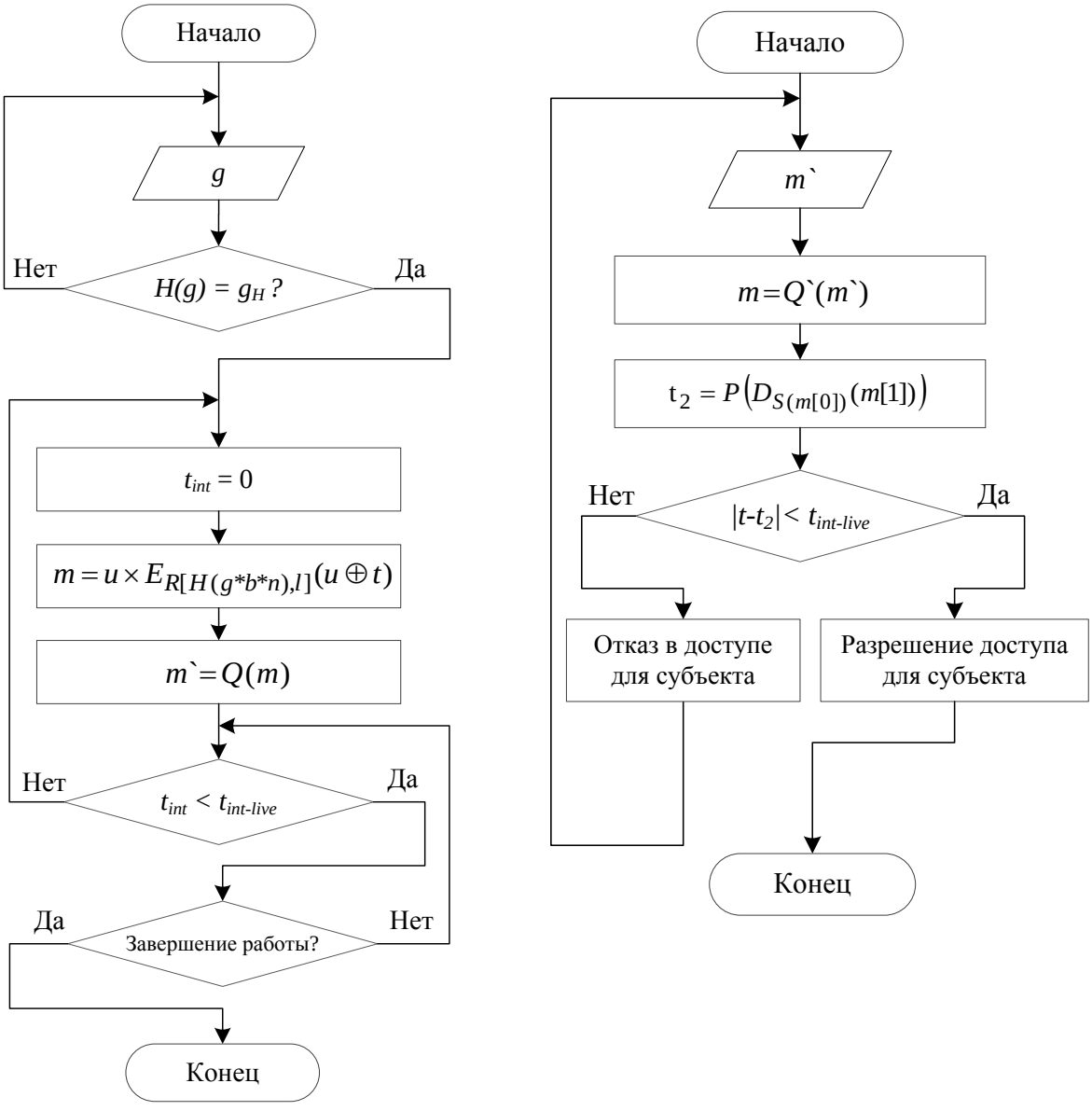

Рисунок 6 – блок-схемы: формирование QR кода для аутентификации (слева); выполнение процедуры аутентификации контроллером СКУД (справа).

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 «время 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 значения ОТР (выражение (16)):

$$F`(m`) = Array[Q`(m`)]. \quad (15)$$

Процедура расшифрования и выделения значения времени генерации пароля:

$$t_2 = P\left(D_{S(m[0])}(m[1])\right). \quad (16)$$

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 исполнительное устройство передается управляющее воздействие на пропуск субъекта доступа.

Также в главе подробно рассмотрена разработанная автором система идентификации посетителей для СКУД ММПЛ.

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 показали, что он имеет наивысший приоритет по сравнению с аналогами и является наилучшей альтернативой по выделенным критериям.

В заключении приведены основные результаты и выводы по проделанной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате проведенного диссертационного исследования была достигнута поставленная цель в повышении эффективности процесса идентификации посетителей в ММПЛ людей за счет применения современных идентификационных признаков.

Автором выявлены особенности функционирования подобных объектов и проблемы в организации контрольно-пропускного режима на их территории. В рамках разработки нового научно обоснованного технического решения в

области идентификации личности, имеющего существенное значение для усовершенствования системы обеспечения общественной безопасности страны, 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%. Практические эксперименты показали, что с точки зрения массовости применения предложенная автором 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. Полученные результаты подтверждаются актом внедрения.

Применение 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.

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

Основные результаты диссертационного исследования опубликованы в следующих работах:

Статьи, опубликованные в журналах, включенных ВАК в перечень ведущих рецензируемых научных журналов и изданий:

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

2. Исхаков А.Ю. Методика верификации личности субъекта доступа при удаленной регистрации с помощью доверенных лиц / А.Ю. Исхаков // Доклады ТУСУРа. – 2016. – № 3. – С. 59–64.

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

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

5. 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.

Публикации в других научных изданиях:

6. 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.

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

8. Исхаков А.Ю. Фаззинг веб-приложений // Материалы 50-й Международной научной студенческой конференции «Студент и научно-технический прогресс»: Информационные технологии / Новосиб. гос. ун-т. Новосибирск, 2012. С. 39

9. Исхаков А.Ю. Автоматизированная система учета посещений Особой экономической зоны технико-внедренческого типа «Томск» 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

10. 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.

Свидетельства о регистрации программ:

1. I-mob. Система усиленной мобильной аутентификации: свидетельство о гос. регистрации программы для ЭВМ № 2015663362 Российская Федерация / Исхаков А.Ю.; правообладатель ТУСУР. Зарегистрировано в Реестре программ для ЭВМ 16.12.2015.

2. TFAS. Программа для двухфакторной аутентификации на основе современных идентификационных признаков: свидетельство № 2015663283 Российская Федерация / Исхаков А.Ю., Мещеряков Р.В.; правообладатель ТУСУР. Зарегистрировано в Реестре программ для ЭВМ 15.12.2015.