ОТЗЫВ

официального оппонента на диссертацию Исхакова Андрея Юнусовича «Методическое и программно-алгоритмическое обеспечение процесса идентификации посетителей в местах массового пребывания людей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность работы

Несмотря на широкую распространенность систем идентификации и аутентификации, вопросы их организации с учетом специфики применения и использования в них тех или иных технологий и механизмов недостаточно изучены, и как следствие, далеко не в полной мере формализованы. Одним из ярких тому примеров является ряд проблем, возникающих при внедрении систем идентификации в местах массового пребывания людей (ММПЛ) – общественных местах с высокой плотностью человеческих потоков и вероятностью возникновения неуправляемой толпы. В рамках данной работы автор под ММПЛ понимает не подлежащие обязательной охране полицией объекты массового пребывания людей, особенности функционирования которых не позволяют внедрить полноценный пропускной режим.

В соответствии с действующим законодательством Российской Федерации для ММПЛ обязательна реализация комплекса инженерных, технических и организационных мероприятий по обеспечению мер безопасности посетителей, одним из которых может быть идентификация их личности и введение контрольно-пропускного режима на их территории. Однако, реализовать такой режим, идентификацию и регистрацию посетителей без нарушения протекающих на территории ММПЛ бизнес-процессов крайне сложно из-за специфических особенностей их функционирования.

Поскольку диссертация Исхакова А.Ю. посвящена разработке методического, технологического и программно-алгоритмического обеспечения процесса идентификации посетителей ММПЛ, организации их удаленной регистрации и, в конечном счете, направлена на разработку нового научно обоснованного технического решения в области создания более эффективных СКУД для ММПЛ, имеющего существенное значение для усовершенствования системы обеспечения общественной безопасности, ее тема, безусловно, является актуальной.

Оценка структуры и содержания диссертации

Диссертация состоит из введения, трех глав, заключения, трех приложений, а также списка использованных источников и литературы из 109 наименований. Общий объем работы составляет 140 страниц, и включает 33 рисунка и 21 таблицу. В целом работа имеет четкую логическую структуру. Из ее специфических особенностей можно назвать обильное использование аббревиатур и символьных обозначений. Большинство из аббревиатур носят ограниченное применение, либо введены автором, но используются по тексту редко, а в ряде случаев несут двойной смысл. Например, ОС – это операционная система (в списке сокращений) и ОС - отношение согласности (стр. 109). Иногда для одного и того же понятия используется разная аббревиатура, например, ИУ (стр. 20) и УИ (в списке сокращений). Все это усложняет восприятие текста, несмотря на наличие списка сокращений, который к тому же не совсем полон (обнаружилось отсутствие сокращений ИС (стр. 109), НСД (стр. 21) и СВТ – в блоке 4 рисунка 1.2. на стр.19). В то же время из положительных моментов можно отметить хорошее владение специальными терминами из рассматриваемой предметной области, а также отличное знание нормативных документов и законодательных актов, относящихся к

теме работы. Опечатки, вроде "похода" вместо "подхода" в названии подраздела 3.3.2 и "Ранее было определено ранее" на стр.36, встречаются крайне редко, и это, скорее, исключения из в целом очень грамотного текста. Стиль же изложения вообще не вызывает нареканий, равно как и оформление диссертационной работы, выполненное на очень высоком уровне.

Во введении дано обоснование актуальности темы диссертационной работы, поставлены цель и задачи исследования, перечислены основные полученные результаты, определена их практическая ценность.

В первой главе подробно рассмотрены классификация, структура и возможные архитектуры систем контроля и управления доступом (СКУД). Особое внимание уделено обзору устройств идентификации и их принципу действия. Учитывая, что данный материал входит во все образовательные программы всех форм обучения по направлению "Информационная безопасность", его можно было в работе и не приводить, хотя подготовлен он очень качественно. А вот привести информацию о зарубежном опыте решения рассматриваемых в работе проблем, связанных с идентификацией личностей в ММПЛ, было бы совсем неплохо. Но такая информация, к сожалению, в работе отсутствует. Нет в компактном виде и аналитической информации о законодательных актах и нормативных документах, регламентирующих требования по ИБ применительно к ММПЛ как у нас в стране, так и за рубежом, хотя о наличии таких требований упоминается на стр.39.

Далее автор формализует задачу идентификации, описывает бизнес-логику существующих решений в части используемых в СКУД методах регистрации и идентификации, показывает их неприменимость для решения задач осуществления контроля в ММПЛ, формулирует основные проблемы, обусловленные в основном необходимостью очной регистрации посетителей, предлагает собственную функциональную модель процесса идентификации в СКУД, лишенную выявленных недостатков. В главе приведен детальный анализ особенностей функционирования ММПЛ и применения в них СКУД. В частности, было установлено, что внедрение на таких объектах СКУД ограничивается необходимостью прохождения посетителями длительной, и не всегда надежной (или требующей очного присутствия в установленном месте) процедуры их регистрации. Завершающим этапом главы является формулирование требований, предъявляемых к процессам регистрации и идентификации посетителей в СКУД, предназначенных для применения на объектах с массовым пребыванием людей.

Как видно из приведенного краткого содержания раздела, его было бы более логично разделить на две отдельные части, первая из которых представляла бы аналитический обзор известных решений, а вторая – посвящена собственно описанию модели СКУД и предлагаемых автором концепций функционирования СКУД ММПЛ. К сожалению, разработка модели ограничилась в работе составлением IDEF0 диаграмм, тогда как здесь было бы уместно развить ее до уровня, позволяющего выполнять какие – либо численные оценки эффективности работы СКУД, рассчитываемые, например, по интенсивности людских потоков, необходимому для регистрации и идентификации времени, по виду используемого оборудования и технологий, статистических сведениях о возникновении ошибок на различных стадиях взаимодействия пользователя со СКУД и с кругом доверенных лиц. Например, возможным путем решения выявленной проблемы могло бы быть использование в ММПЛ считывателей паспортных данных, как это делается в аэропортах, но, надо полагать, такое решение было бы не оптимальным по таким характеристикам, как необходимость наличия паспорта и (возможно) высокая стоимость оборудования. Попытка сделать подобную оценку была предпринята в последней главе, но без учета перечисленных факторов.

Во второй главе представлена авторская реализация методики верификации пользователей при удаленной регистрации в СКУД, удовлетворяющая сформулированным в предыдущем разделе требованиям, главным из которых является неприменимость проведения регистрации пользователей с привлечением обслуживающего ММПЛ персонала.

В начале главы проведен детальный анализ современных механизмов установления личности в автоматизированных системах, которые возможно было бы применить для регистрации в СКУД ММПЛ. В качестве критериев качества при сравнении были выделены: надежность установления личности; вероятность фальсификации сведений злоумышленником; возможность удаленного проведения процедуры регистрации; возможность использования способа нерезидентами РФ; массовость применения. На основании этих критериев предпочтение было отдано процедуре регистрации, основанной на применении механизма доверенных лиц и примеры его использования в системах аутентификации. Далее автор подробным образом пошагово представляет адаптированную применительно к ММПЛ методику верификации субъекта доступа, основанную на этом механизме, и алгоритм её использования, приводит подробные пояснения по применению методики.

Пожалуй, в качестве непринципиального замечания можно отметить обильное использование при описании методики целой системы специальных обозначений, перечисление которых начинается со стр. 67 и заканчивается на стр.69. Многие из этих обозначений используются однократно (например, c_1, c_2, k), что приводит к неоправданному усложнению и затрудняет понимание сути текста. Из других аналогичных замечаний можно отметить то, что на стр. 59 рисунки 2.5 и 2.6 по своей содержательной части дублируют друг друга, представляя одну и ту же информацию различными способами. Не совсем понятно, почему использование фальшивых аккаунтов в почтовых службах и социальных сетях имеют различную сложность фальсификации, что следует понимать под уровнем 5 сложности фальсификации (точнее, что нужно к ней относить), и почему в таблице 2.3 не представлен такой распространенный в повседневной жизни вариант ответа, как "Коллега на работе". Неплохо было бы выпуклее показать и отличия предлагаемой методики верификации через доверенных лиц от известных решений, представленных, например, в той же работе Малахова [69]. Ведь эта методика выносится в автореферате как научная новизна работы, но использование известных решений для других применений по их прямому назначению не является новизной.

А вот более важным недочетом является отсутствие в главе рассмотрения вопросов, связанных с продолжительностью хранения сведений о регистрации в базе данных СКУД. Ведь, помимо перечисленных на стр.73 двух групп посетителей можно выделить и еще одну – группу посетителей, посещающих один и тот же объект эпизодически, но достаточно регулярно и продолжительное время, из-за наличия которых объем хранимых данных может резко возрасти. Решается данная проблема достаточно просто, причем даже без участия пользователя, но все же стоило оценить зависимость объема хранимых данных от характера ММПЛ, цели его посещения и регулярности его посещения пользователем.

Третья глава является, пожалуй, наиболее значимой в проведенных диссертационных исследованиях. В ней предложен новый подход к идентификации и аутентификации посетителей в ММПЛ, основанный на применении смартфонов и иных мобильных устройств, обязательным условием применения которых является возможность размещения в них стороннего приложения, позволяющего генерировать изображение на экране и/или позволяющего производить обмен данными по альтернативным каналам связи, например, с применением NFC- модуля. Предлагаемый подход отличается возможностью варьирования набора иден-

тификационных данных и технологий их передачи в соответствии с требуемым уровнем защищенности объекта. Оригинальна схема генерации секретного ключа и одноразового пароля, использующая временную синхронизацию работы мобильного и считывающего устройств.

В главе приведено подробное описание работы алгоритмов аутентификации на основе использования QR-кодов и NFC-меток и результаты их практического применения в разработанном диссертантом программно-аппаратном обеспечении СКУД ММПЛ, реализующей автоматизированную систему усиленной аутентификации на основе предложенной им концепции. К сожалению, описание используемого аппаратного обеспечения в данной главе совершенно не представлено, хотя очевидно, что стандартные считыватели не в состоянии осуществлять необходимые для реализации предложенного метода функции. И если описание методики проведения эксперимента по оценке времени регистрации пользователя в системе представлено должным образом, то описания методики эксперимента по оценке работы системы в части проведения процедур аутентификации и идентификации нет вообще. Непонятно, откуда взялись данные в таблице 3.3 на стр.107 по результатам 1000 посещений с применением для идентификации и аутентификации документа, бесконтактной RFID - карты и разработанной системы? Зато на более чем 7 страницах проводится обработка этих данных с применением метода анализа иерархий, хотя достаточно очевидно, что они мало что добавляют к приведенным в таблице данным, т.к. основаны на во многом субъективной расстановке приоритетов выбранных критериев оценки качества работы СКУД и выборе значений для интенсивностей относительной важности. Жаль, что в число рассматриваемых критериев не вошли стоимость аппаратного обеспечения, стоимость его владения и показатели надежности работы. Не лишним было бы в этой главе и остановиться на вопросах, связанных с областью возможного применения предложенного подхода. Ведь очевидно, что не у всего населения есть мобильные телефоны (не говоря уже о смартфонах), а тем более интернет, и не всегда, когда человек спонтанно захотел пойти в кино (особенно в другом городе), у него окажется достаточно времени для прохождения процедуры регистрации в понравившийся кинотеатр. По-видимому, полноценное решение обозначенной в работе проблемы требует комплексного подхода, основанного на использовании статистических данных и социальных исследованиях, и, надо полагать, разработка такого решения может составить суть дальнейшего развития работ по данной теме.

В приложения вынесены копии двух свидетельств о регистрации программ для ЭВМ и три акта внедрения: два из них – об интеграции разработанного соискателем методического и программного обеспечения в деятельность предприятий, а третий – об использовании результатов исследования в учебном процессе ТУСУР.

Научная новизна полученных результатов

Представленные соискателем результаты до работы автора и его публикаций ранее нигде не публиковались. Наиболее важными из них, обладающими признаками научной новизны, являются:

1) Модель процесса идентификации в СКУД, отличающаяся необходимостью проведения верификации на этапе удаленной регистрации и позволяющая организовать идентификацию личности посетителей ММПЛ.

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

3) Подход к идентификации и аутентификации в СКУД, основанный на использовании мобильных устройств в качестве идентификаторов, отличающийся возможностью варьирования набора идентификационных признаков и технологий их передачи в соответствии с требуемым уровнем защищенности объекта и позволяющий автоматизировать пропускной режим в ММПЛ с высокой степенью достоверности

Практическая ценность и внедрение результатов работы

Практическая значимость полученных результатов состоит в том, что применение предложенного методического и программно-алгоритмического обеспечения позволяет расширить круг достоверно идентифицируемых лиц, посещающих ММПЛ, практически без усложнения аппаратного обеспечения СКУД с применением уже существующих технических решений. Разработанный программный, и, как выяснилось в процессе обсуждения работы, и модернизированный аппаратный комплекс, был успешно инсталлирован и прошел апробацию в двух организациях, на практике позволил провести натурные эксперименты и подтвердил возможность успешного применения мобильных устройств для надежной идентификации посетителей в СКУД ММПЛ.

Обоснованность и достоверность полученных результатов и сделанных выводов

Автором адекватно используются функциональные модели процессов, математические методы, делаются корректные выводы на основе полученных данных. Достоверность результатов подтверждается строгостью применения математических методов, а также проверкой непротиворечивости и адекватности результатов, полученных как на промежуточных, так и на окончательных этапах работы, а также их согласованностью с результатами проведенных практических экспериментов.

Пункты научной новизны, основные положения и выводы хорошо аргументированы, корректны и подтверждаются экспериментальными данными.

Основные результаты работы докладывались и обсуждались на научных конференциях, форумах и семинарах международного, всероссийского и регионального уровней.

Рекомендации по использованию результатов работы

Результаты диссертационной работы Исхакова А.Ю. могут быть применены при проектировании и реализации пропускных систем в местах с большой проходимостью посетителей, например, в бизнес-центрах и отдельных офисах, в которых требуется обеспечение пропускного режима, но применение типовых решений, в том числе с использование вахтеров и охранников оказывается нерентабельным, либо ограничивает возможности по организации полноценных бизнес-процессов. Учитывая вектор развития нормативных актов в области обеспечения безопасности населения, возможность организации простой по реализации и весьма эффективной идентификации большой доли посетителей в местах массового пребывания людей может также послужить стимулом для установления новых норм и правил их посещения, требований к их владельцам и руководителям расположенных на территории ММПЛ фирм и к организаторам культурно-массовых мероприятий.

Соответствие содержания автореферата содержанию диссертации

Текст автореферата достаточно полно и точно отражает содержание диссертационной работы автора. В нем приведены и в целом раскрыты все пункты, составляющие научную новизну исследования: приведен математический аппарат предлагаемого подхода верификации на основе доверенных лиц, показаны функциональные модели описываемых процессов, в составе подхода к идентификации и аутентификации посетителей в СКУД ММПЛ пред-

ставлены соответствующие схемы и алгоритмы. Однако, не смотря на большой объем автореферата (24 страницы), вопрос о применении NFC в предлагаемом подходе так и остался неосвещенным.

Соответствие содержания диссертации содержанию опубликованных работ.

Основные результаты диссертационных исследовании опубликованы в 10 печатных работах, в том числе в пяти статьях в журналах, рекомендуемых ВАК РФ и в двух свидетельствах о регистрации разработанных программ для ЭВМ. Знакомство с отдельными публикациями соискателя свидетельствуют о том, что в них достаточно полно отражены все основные положения, выводы и рекомендации диссертации.

Соответствие темы диссертации заявленной научной специальности

Тема диссертационной работы соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по следующим пунктам паспорта.

Пункт 8. (Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем), поскольку разработанная автором модель работы системы идентификации в СКУД в ММПЛ позволяет анализировать системы с повышенным уровнем безопасности на объектах указанного типа, способных предотвратить ряд угроз, связанных с физическим проникновением злоумышленника.

Пункт 6. (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), поскольку предложенный механизм удаленной верификации пользователей, как часть системы идентификации, реализует метод противодействия угрозам модификации, а также предоставления ложной информации о посетителях.

Пункт 11. (Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа), поскольку предложенный подход к идентификации и аутентификации в СКУД с применением мобильных устройств позволяет автоматизировать процесс идентификации в ММПЛ и повысить его надежность, превышающий надежность аутентификации с помощью сотрудников охраны.

Замечания к работе:

1. Не все аспекты работы изложены достаточно подробно, в то время как излишнее внимание уделено описанию известных в области информационной безопасности вещей. При этом практически полностью отсутствует анализ состояния дел в области организации обеспечения безопасности ММПЛ на мировом уровне, нет свода нормативных документов по обеспечению безопасности ММПЛ, отсутствует описание эксперимента по оценке эффективности применения предложенного метода для идентификации посетителей ММПЛ, крайне скупо описано представляющее несомненный практический интерес разработанное программно-техническое обеспечение, а информация о практическом применении результатов работы сведена к упоминанию о местах внедрения в заключении по работе.
2. В работе отсутствует анализ влияния особенностей использования СКУД ММПЛ, обусловленных ее техническими возможностями, требуемой пропускной способности, отводимому на регистрацию времени, спецификой обслуживаемого контингента и иных условий применения на особенности построения ее структуры и значение ожидаемых критериев качества, перечисленных в разделе 3.3.2.

3. Работа излишне усложнена большим числом обозначений, не всегда однозначных аббревиатур, дублирующих по смысловому содержанию рисунков, а местами и не несущих существенной дополнительной информации математических выкладок.
4. Разработанная модель идентификации СКУД ММПЛ использовалась только для анализа протекающих в СКУД процессов, тогда как большое прикладное и теоретическое значение имело бы ее применение для оценки таких критериев, как время доступа, время обслуживания (при наличии очередей), вероятности появления ошибок первого и второго рода.

Заключение

Отмеченные выше замечания к диссертационной работы не носят принципиальный характер и не снижают ее общей положительной оценки. Диссертация является завершенной научно-квалификационной работой, выполненной на актуальную тему, в которой решена важная научно-техническая проблема организации пропускного режима и идентификации посетителей в местах массового пребывания людей. По своей актуальности, научной новизне, объему выполненных исследований и практической значимости полученных результатов представленная работа соответствует п.9. Положения о присуждении ученых степеней в редакции постановления Правительства РФ от 21.04.2016 № 335, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор Исхаков Андрей Юнусович заслуживает присуждения ему ученой степени кандидата технических наук по специальности «05.13.19 – Методы и системы защиты информации, информационная безопасность».

Зав. кафедрой информатики, вычислительной техники и информационной безопасности, зав. лабораторией информационно-измерительных систем ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», д.т.н., профессор

Якунин Алексей Григорьевич

656038, Барнаул, проспект Ленина, 46,
АлтГТУ, ФИТ, каф. ИВТ и ИБ
Тел. +7(3852) 290-786 раб/факс,
e-mail: yakunin@agtu.secna.ru

Подпись заверяю:
Начальник ОК ГПС
А.А. Дитенер
21.11.2016г.