УДК 004.732

А.Ю. Исхаков

Методика верификации личности субъекта доступа при удаленной регистрации с помощью доверенных лиц

Рассматриваются вопросы подтверждения личности при удаленной регистрации пользователей в системах контроля и управления доступом. На основе сформированных критериев проведен анализ современных способов верификации и определены основные проблемы их применения в выбранной предметной области. Автором предлагается применить механизм доверенных лиц в качестве инструмента верификации при удаленной регистрации. Подробно рассмотрена методика применения данного механизма и представлены результаты ее апробации.

Ключевые слова: места массового пребывания людей, система контроля и управления доступом, верификация, доверенные лица.
doi: 10.21293/1818-0442-2016-19-3-70-75

В июле 2016 года были внесены изменения в Федеральный закон № 35-ФЗ «О противодействии терроризму» [1] 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 [2] 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».

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 возникновению угроз общественной безопасности.

Между тем идентифицировать людей нужно не только при использовании интернет-ресурсов, но и в обычной жизни. Особенно это касается мест массового пребывания людей (ММПЛ), под которыми понимаются общественные места с высокой плотностью человеческих потоков и вероятностью возникновения неуправляемой толпы [3]. Подобные объекты должны быть обеспечены системами безопасности, в том числе системами контроля и управления доступом (СКУД), позволяющими идентифицировать личность каждого посетителя.

Идентификация посетителей ММПЛ подразумевает их регистрацию в СКУД независимо от используемого набора идентификационных характеристик. Наиболее распространенным способом регистрации посетителей является непосредственное обращение в службу или подразделение ММПЛ, осуществляющее функции контроля за соблюдением пропускного режима. При этом предполагается предъявление человеком документа, удостоверяющего личность.

Как было сказано ранее, ММПЛ характеризуются высокой плотностью потоков посетителей, поэтому применение такого способа регистрации зачастую приводит к увеличению временных затрат и, как следствие, замедлению бизнес-процессов. Кроме того, такой подход предполагает возможные сложности при подтверждении 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 также актуальной становится проблема проверки подлинности документов.

В связи с этим предлагается рассмотреть вопрос о возможности применения удаленной регистрации в СКУД. При этом особое внимание необходимо уделить вопросам определения механизма ве-

рификации, применимого в данной предметной области.

Постановка задачи

Примерами реализации удаленной регистрации посетителей в системе могут служить заказ пропуска на конференцию (выставку) посредством телефонного звонка, отправки электронного сообщения или заполнения онлайн-формы на сайте. Тогда, как правило, идентификатором выступает сгенерированный и распечатанный самим пользователем билет или пропуск.

Стоит отметить, что в большинстве случаев отсутствует возможность убедиться в достоверности представленной информации и, как следствие, подтвердить личность регистрируемого пользователя. Применение в качестве идентифицирующих признаков биометрических характеристик хоть и обеспечивает высокую степень достоверности, но в то же время подразумевает непосредственное посещение субъектом доступа ММПЛ для проверки документов, удостоверяющих личность. Подобное решение приводит к первоначальной проблеме – замедлению бизнес-процессов.

Одним из способов верификации является привязка регистрируемой учетной записи к номеру мобильного телефона путем отправки одноразовых паролей в виде SMS-сообщений. Такой подход используется, в том числе, в системах многофакторной аутентификации [4] для проведения финансовых операций через системы онлайн-банков, а также для получения государственных услуг в электронной форме.

Но в случае с банком или государственной услугой «привязка» определенного сотового телефона как дополнительного фактора аутентификации осуществляется непосредственно при посещении клиентом офиса и предъявления документа, удостоверяющего личность. Другими словами, сам процесс регистрации не является удаленным. Необходимо учитывать, что удаленная регистрация в ММПЛ преследует цель полностью отменить необходимость предварительного посещения объекта. Поэтому в данном случае применение SMS-сообщений в качестве единственной верифицирующей информации не всегда является достаточной. Номер телефона может быть зарегистрирован на другого человека, и определить данный факт невозможно без привлечения правоохранительных органов. Данное обстоятельство, вероятно, стало одной из причин поправок, внесенных в стандарт Digital Authentication Guideline [5], в части рекомендаций недопущения применения SMS-сообщений в качестве одного из элементов многофакторной аутентификации.

Таким образом, можно утверждать, что в настоящее время актуальна проблема верификации личности при удаленной регистрации посетителей ММПЛ, в основе инженерных технических систем безопасности которых лежит СКУД. Соответственно, важной представляется задача разработки подходов и методического обеспечения процедуры удаленной регистрации пользователей СКУД, предусматривающей верификацию личности человека без необходимости предварительного посещения объекта в целях минимизации неудобств и ограничений для протекающих в ММПЛ бизнес-процессов.

Автором предлагается рассмотреть механизм доверенных лиц в качестве способа решения обозначенной выше проблемы.

Верификация пользователей при удаленной регистрации

В настоящее время существует ряд способов, которые используются для установления сведений о личности регистрируемого пользователя. Был проведен сравнительный анализ таких способов на предмет возможности их применения в ММПЛ. Особое внимание было уделено существующим ограничениям такого использования.

В качестве критериев при сравнении были выделены: возможность установления личности, возможность фальсификации сведений злоумышленником, возможность удаленного проведения процедуры, возможность использования способа нерезидентами РФ, а также массовость применения. Перечисленный набор критериев, по мнению автора, в полной мере охватывает спектр вопросов, которые необходимо учесть при организации пропускного режима в ММПЛ.

Очевидно, что возможность фальсификации 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 экспертами в области защиты информации и инженерно-технических систем безопасности по шкале от 1 до 10, где 1 – низкая сложность, 10 – очень высокая сложность.

Под возможностью установления личности понимается способность администратора системы получить паспортные данные зарегистрировавшегося человека.

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 затраты для их получения.

В табл. 1 представлен сравнительный обзор способов установления сведений о личности, используемых в современных подсистемах регистрации, на основе выделенных критериев.

Таблица 1

Способы установления сведений о личности при регистрации

Способ	Сложность фальсификации	Установление личности	Удаленная верификация	Использование нерезидентами РФ	Массовость
Личная проверка документов, удостоверяющих личность	8. Использование чужого паспорта (изменение внешнего вида). Человеческий фактор при проверке фотографии	Да	Нет	Да	Да
Отправка кода активации на мобильный телефон	2. Использование чужих SIM-карт, услуги сервисов анонимных мобильных номеров	Да	Да	Да	Да
Отправка кода активации на указанный e-mail	1. 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	1. Использование анонимайзеров (прокси-серверы, VPN/SSH-туннели, Tor, I2P)	Нет	Да	Да	Да
Хранение browser Fingerprint, HTTP-referer и прочих характеристик клиента	1. Настройка анонимизации в браузерах	Нет	Да	Да	Да
Использование Federated Identity технологий (OpenID, oAuth протоколы)	1. Использование фальшивых аккаунтов у Federated Identity провайдеров	Нет	Да	Да	Нет
Использование «подтвержденных учетных записей» ФГИС ЕСИА	7. 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	8. Кража носителя сертификата ключа проверки электронной подписи и PIN-кода	Да	Да	Да. *Множество ограничений*	Нет

Способ отправки кода активации на мобильный телефон удовлетворяет всем критериям, необходимым для ММПЛ. Способ характеризуется сравнительно простой фальсификацией с использованием чужих SIM-карт и распространенных интернет-сервисов анонимных мобильных номеров. Таким образом, сведения о владельце SIM-карты могут быть недостоверными.

Использование «подтвержденных учетных записей» ФГИС ЕСИА и применение технологий электронной подписи обладают высокой сложностью фальсификации данных о личности, так как для их получения применяется проверка документов и необходимо личное присутствие. Эти способы позволяют однозначно установить личность пользователя, верифицировать его удаленно, кроме того, они доступны для нерезидентов РФ.

Применение технологий электронной подписи пока не является массовым для физических лиц ввиду необходимости материальных затрат на получение сертификата ключа, а также посещения удостоверяющего центра. В то же время бесплатная для населения учетная запись ФГИС ЕСИА на сегодняшний день есть более чем у 26 млн граждан РФ, что подтверждает ее распространение. Кроме того, получить такую учетную запись может каждый гражданин (в том числе нерезидент РФ).

Способы установления сведений о личности с использованием учетных записей ФГИС ЕСИА, а также технологий электронной подписи удовлетворяют критериям использования для установления личности пользователей ММПЛ, однако они не могут быть использованы для всех категорий пользователей в связи с необходимостью предварительного получения записи и ключа.

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

1) высокая сложность фальсификации данных злоумышленником;

2) возможность варьирования степени достоверности верификации в соответствии с требуемым уровнем защищенности объекта;

3) возможность удаленного взаимодействия и использование лицами, не имеющими гражданства РФ.

Методика верификации субъекта доступа

Автором предлагается в подсистеме регистрации СКУД использовать подход, основанный на механизме доверенных лиц. Он основан на подтверждении личности пользователя 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 исследо-

вательская группа Джона Брэйнарда [6]. 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 года [7]. 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 [8] А.А. Малков предложил алгоритм работы автоматизированной системы восстановления доступа к учетной записи, основанный на технологии социальной аутентификации с помощью доверенных лиц. 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 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 для 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 конкретизации и 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 ММПЛ. В ходе проводимого исследования были сформулированы основные потребности потенциальных пользователей такой методики – должностных лиц, ответственных за организацию пропускного режима в ММПЛ. 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.

Ниже представлены основные шаги предлагаемой методики.

Шаг 1. В системе *VS* размещается заявка на посещение ММПЛ некоторым субъектом доступа *Subject*. В составе заявки содержатся идентификационные данные *Subject_identity*. Заявка может быть подана как самим субъектом доступа *Subject*, так и некоторым доверенным лицом, обладающим в системе *VS* статусом *Voucher*.

Шаг 2. Если заявка подана зарегистрированным пользователем, обладающим статусом *Voucher*, то перейти к шагу 3. Иначе субъект доступа *Subject* предоставляет список доверенных лиц, обладающих статусом *Voucher*, которые готовы подтвердить личность *Subject*.

Шаг 3. Система *VS* генерирует одноразовый верификационный ключ *Verification_code* и передает его субъекту доступа по основному каналу передачи данных *Channel*.

Шаг 4. Субъект доступа *Subject* по дополнительному каналу *Second_channel* подтверждает получение верификационного ключа *Verification_code*.

Шаг 5. Если заявка была подана зарегистрированным пользователем, обладающим статусом *Voucher*, то перейти к шагу 6. Иначе необходимо организовать верификацию субъекта доступа *Subject* посредством указанных на шаге 2 доверенных лиц, обладающих статусом *Voucher*:

5.1. *VS* отправляет каждому доверенному лицу *Voucher*, указанному на шаге 2, уведомление о необходимости верифицировать субъекта доступа *Subject*.

5.2. Доверенные лица, обладающие статусом *Voucher*, подтверждают личность субъекта доступа путем заполнения опросника в системе *VS*.

5.3. *VS* рассчитывает интегральную оценку r_k результатов [9] заполнения опросника доверенными лицами по формуле (1):

$$r_k = \frac{\sum_{i=1}^{n} y_{ki}}{\sum_{i=1}^{n} \max_j(\delta_{ij})}, \quad (1)$$

где y_{ki} – оценка, соответствующая ответу k-го доверенного лица $Voucher_k$ на вопрос $q_i \in Q$; δ_{ij} – нормированная в диапазоне [0; 1] оценка j-го варианта ответа на i-й вопрос $q_i \in Q$, причем выполняется (2):

$$\sum_{j=1}^{ki} \delta_{ij} = 1; \quad (2)$$

$Q = \{q_1, q_2, \ldots, q_n\}$ – множество вопросов, на которые должно ответить доверенное лицо *Voucher* для верификации субъекта доступа *Subject*; $|Q| = n$.

5.4. *VS* принимает решение по результатам процедуры верификации субъекта *Subject* согласно функции *Ver,* рассчитанной согласно (3):

$$Ver(R_{pos}, Pc) = \begin{cases} ИСТИНА, \text{если } |R_{pos}| \geq Pc \\ ЛОЖЬ, \text{иначе.} \end{cases}, \quad (3)$$

причем R_{pos} – множество интегральных оценок результатов ответов доверенных лиц, превышающих пороговое значение оценки Pg. $R_{pos}=\{r_k | \ r_k \geq Pg\}$, $R_{pos} \subset R$; Pg – пороговое значение оценки $r_k \in R$; Pc – минимально допустимое количество доверенных лиц *Voucher*, подтвердивших личность субъекта доступа *Subject*.

В случае если функция *Ver* принимает значение *ИСТИНА*, считается, что пользователь *Subject* верифицирован (предоставляется инструментарий для получения идентификатора). Иначе субъект доступа формирует новый список доверенных лиц, после чего осуществляется переход к шагу 5.1.

Указания к методике:

1. В качестве подтверждающих доверенных лиц должно быть не менее 3 человек (согласно исследованию С. Шехтера, С. Игельмана и П.Б. Ридера от 2009 г.).

2. Для получения статуса *Voucher* субъект доступа должен пройти дополнительную процедуру верификации. Ее смысл заключается в ознакомлении субъекта доступа с правилами и нормами ответственности за приобретаемые им права по верификации личности других субъектов, а также в подтверждении своего согласия. Примеры вариантов прохождения дополнительной процедуры верификации в зависимости от типов ММПЛ:

– письменное согласие (при посещении ММПЛ);

– подписание согласия средствами квалифицированной электронной подписи;

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

Область применения методики

Множество рассматриваемых объектов доступа следует разделить на 2 класса:

1-й класс – объекты, в которых любое посещение должно быть инициировано некоторым заинтересованным представителем ММПЛ. То есть подразумевается, что каждый посетитель может попасть в ММПЛ 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.

2-й класс – 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.

Апробация методики

Для сравнения предложенной методики с приведенными способами установления личности пользователя была проведена их апробация. Апробация предполагала необходимость зарегистрироваться и пройти верификацию для посещения некоторого 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 одно и то же мероприятие с необходимостью получения идентификатора. Среди участников присутствовали лица в возрасте от 24 до 56 лет.

Для сравнения способов были выделены следующие количественные показатели:

1) количество человек, воспользовавшихся способом (посчитавших его наиболее удобным для процедуры);

2) среднее время, потребовавшееся для регистрации пользователя;

3) среднее время, потребовавшееся для верификации пользователя;

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

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. Число людей (в данном случае – 103 посетителя) 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. 2.

Приведенные результаты иллюстрируют тот факт, что длительность процедуры верификации с

использованием механизма доверенных лиц значительно (в несколько) раз превышает соответствующие значения для двух других способов.

Таблица 2

Количественные показатели апробации процедуры верификации в ММПЛ

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

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, превышает в 3,7 раза количество использовавших для этого учетную запись ФГИС ЕСИА, а количество использовавших ЭП – в 19,5 раза.

Заключение

На основании проведенной апробации можно заключить, что верификация с использованием механизма доверенных лиц дополняет способы верификации посредством «подтвержденной» учетной записи ФГИС ЕСИА, а также верификации с использованием ЭП. Другими словами, данный механизм позволяет пользователям пройти процедуру регистрации удаленно, не имея при этом дополнительных учетных записей и ключей. На прохождение регистрации с помощью подтверждения личности доверенными лицами уходит в среднем в 4–5 раз больше времени, однако средний показатель для данного способа не превышает разумно допустимого, который можно исчислять количеством суток.

Следует отметить, что время процедуры зависит от количества доверенных лиц, выполняющих верификацию, а также особенностей ММПЛ. Предусмотренная методикой возможность наделения уже верифицированных пользователей статусом *Voucher* позволит сократить затрачиваемое время, оптимизировав при этом процедуру регистрации. Результаты, полученные в ходе апробации методики, подтверждают возможность ее использования для удаленной регистрации посетителей ММПЛ на практике.

Работа выполнена при поддержке Минобрнауки России в рамках мероприятия 1.3 федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение о предоставлении субсидии № 14.577.21.0172 от 27 октября 2015 г., идентификатор RFMEFI57715X0172).

Литература

1. О противодействии терроризму: Федеральный закон РФ от 26.03.2003 г. № 35-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_58840/, свободный (дата обращения: 10.08.2016).

2. Зыков В. Интернет-СМИ освободят от ответственности за комментарии читателей [Электронный ресурс]. – Режим доступа: http://izvestia.ru/news/612511, свободный (дата обращения: 15.07.2016).

3. 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]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102370057, свободный (дата обращения: 20.07.2016).

4. Технология усиленной аутентификации пользователей информационных процессов / И.А. Ходашинский, М.В. Савчук, И.В. Горбунов, Р.В. Мещеряков // Доклады ТУСУРа. – 2011. – № 2 24), ч. 3. – С. 236–248.

5. DRAFT NIST Special Publication 800-63-3 Digital Authentication Guideline [Электронный ресурс]. – Режим доступа: https://pages.nist.gov/800-63-3/sp800-63-3.html, свободный (дата обращения: 10.08.2016).

6. Reeder R.W. When the Password Doesn't Work, Secondary Authentication for Websites / R.W. Reeder, S. Schechter // IEEE Security & Privacy. – 2011. – № 9 (2). – P. 43–49.

7. Introducing Trusted Contacts [Electronic resource]. – URL: https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts/10151362774980766/ (access date: 15.07.2016).

8. Малков А.А. Технология аутентификации с помощью доверенных лиц : автореф. дис. … канд. техн. наук : 05.13.19. – Уфа, 2013. – 18 с.

9. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады ТУСУРа. – 2012. – № 1 (25), ч 2. – С. 119–125.

Исхаков Андрей Юнусович
Аспирант ТУСУРа
Тел.: +7-923-421-58-28
Эл. почта: iay@security.tomsk.ru

Iskhakov A.Yu.

Subject verification method based on the trustees mechanism for remote registration

Identity verification for remote user registration in access control systems is the main problem described in this article. Modern verification methods and their main problems in application in the chosen subject area were analyzed. The authors propose to apply the mechanism of trustees as a verification tool for remote user registration.

Keywords: crowded place, access control system, verification, trustees.