**УДК 378.147+159.922**

# СПОСОБЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ЛИЧНОСТИ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ В ВЫСШЕЙ ШКОЛЕ

**Стефаненко Павел Викторович,** д-р пед. наук, профессор,
профессор кафедры гуманитарных дисциплин
ГОУВПО «Академия гражданской защиты» МЧС ДНР
83050, г. Донецк, ул. Розы Люксембург, 34а
E-mail: agz@mail.dnmchs.ru
Тел.: + 38 (062) 303-27-02

*Дистанционное обучение является современной формой образования, которая предусматривает организацию процесса обучения на удалении. Одной из существенных проблем его осуществления является проблема идентификации и аутентификации личности пользователя, в частности студента, обучающегося удалённо по специально разработанным дистанционным курсам, с использованием информационно-коммуникативных технологий.*

*При осуществлении дистанционного обучения нужно быть уверенным, что студент самостоятельно выполняет все задания преподавателя. Рассмотрению некоторых способов решения сложного процесса идентификации и аутентификации личности посвящена данная статья.*

***Ключевые слова:*** *дистанционное обучение; идентификация; аутентификация; биометрический образ; биометрический эталон.*

**Постановка проблемы и её связь с актуальными научными и практическими исследованиями.** При организации дистанционного обучения (далее – ДО) отдельно стоит проблема идентификации пользователей при проведении контрольных мероприятий. Она решается несколькими способами. Одним из вариантов является присутствие во время проведения тестирования лица, обеспечивающего идентификацию студента, а также тьютора, следящего за соблюдением всех правил проведения контрольных мероприятий. Возможно, и чисто техническое решение с использованием различных систем идентификации пользователей. Для решения данной проблемы, необходимо разработать технологии, которые позволят контролировать процесс удалённого проверочного мероприятия и то, что его сдаёт именно тот человек, который должен. Студент должен пройти процедуру идентификации перед началом контрольных проверок, а также подтверждение идентификации в течение всего мероприятия.

Известно, что идентификация – это «процедура распознания субъекта по его уникальному идентификатору, присвоенному данному объекту ранее и занесённому в базу данных в момент регистрации субъекта в качестве легального пользователя системы», а аутентификация – «процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор» [2].

Исследователи в этой области отмечают, что проверка пользователя (студента, обучающегося) может быть односторонней или взаимной и, как правило, представляет собой обмен информацией между обучающимися и базой данных, отвечающих за принятие решения – «да» или «нет». Эта проверка осуществляется с помощью специальных технических преобразований, необходимых для того, чтобы удостовериться в подлинности объекта и для защиты трафика «пользователь-система» от внешнего воздействия. То есть процедуры идентификации и аутентификации являются взаимосвязанными процессами проверки подлинности обучающихся. Именно от решения задач «распознания» и «проверки подлинности» зависит допуск к системе конкретному пользователю, т. е. будет ли он авторизован и получит ли доступ к ресурсам системы после положительного прохождения им процедуры аутентификации. Необходимо заметить, что для каждого пользователя в системе предоставляется свой перечень прав, которыми он может пользоваться.

**Изложение основного материала исследования**. В настоящее время в образовательных заведениях, в том числе в вузах, начинает применяться электронная идентификация обучающегося, в которой сбор информации происходит с минимальным участием последнего. Это характерно при организации дистанционного обучения и, особенно, во время контроля полученных студентами знаний.

Учёные-исследователи И. Х. Бикмухаметов, А. А. Гладких, Е. Ю. Гурина, А. В. Густырь, В. Е. Дементьев, В. И. Овсянников и др., касающиеся решения этих вопросов, рассматривают

различные пути идентификации и аутентификации личности студента. Рассмотрим и проанализируем некоторые из них.

На данный момент существуют следующие методы идентификации пользователей в системах дистанционного образования [6]:

– биометрическая идентификация, основанная на анализе биометрических характеристик человека (БХЧ), которые делятся на две группы: статические и динамические БХЧ. К статическим БХЧ относят измерения неизменяемых анатомических данных, таких как отпечаток пальца, геометрия руки, геометрия лица, рисунок сетчатки или радужки глаза и т.д. К динамическим или поведенческим БХЧ относят измерения каких-либо действий человека, например, динамика подписи, динамика работы на клавиатуре, походка, голос и др.;

– идентификация на основе карт с магнитной полосой. Пользователям выдается карта, на которую записана уникальная информация, позволяющая идентифицировать человека;

– парольная идентификация на основе многоразовых и одноразовых паролей.

Многоразовые пароли. У каждого пользователя имеется пара логин-пароль, при помощи которых происходит идентификация. Введенный пароль сверяется с паролем в базе данных и на основе этой проверки разрешается или запрещается доступ.

Одноразовые пароли. Для идентификации пользователя используется какой-либо механизм обмена одноразовыми паролями. Например, у пользователя может быть список паролей для доступа и при каждой попытке идентификации сервер просит ввести пароль под определенным номером. Если пользователь отправляет правильный пароль, то идентификация проходит успешно.

Иидентификация на основе цифровых сертификатов. При данном подходе на сервере системы отсутствует информация о паролях пользователей. Пользователи проходят идентификацию, посылая цифровой сертификат, в котором хранится информация для идентификации, зашифрованная закрытым ключом пользователя. Во время проверки происходит дешифрование сертификата открытым ключом и сверка необходимой информации. Если подтверждается, что закрытый ключ действительно принадлежит идентифицируемому пользователю, идентификация проходит успешно.

Идентификация на основе смарт-карт и USB-ключей. Смарт-карта – это пластиковая карта со встроенной микросхемой, на которую записана идентификационная информация пользователя (закрытый ключ ЭЦП, цифровой сертификат и т. д.) Для доступа к этой информации необходимо предъявить PIN-код. Подобной функциональностью обладают USB-ключи (аппаратные ключи eToken, RuToken, Al-ladin и т.д.).

К традиционным методам аутентификации в системе ДО авторы относят аутентификацию с помощью пары «логин-пароль» – наиболее распространённый метод. Но логин и пароль могут быть переданы кому-то ещё, это же относится и к аутентификации по почте или по методу «вопрос-ответ».

Аутентификация по устройству может производиться с помощью специальных карточек. Карточку сложно подделать. Пользователю будет неудобно её кому-то передавать, так как существующие карточки используются во многих целях (кредитные карты, пропуска студентов и др.). Но для реализации этого метода пользователю нужно приобретать считывающие устройства, что увеличивает финансовые затраты и ликвидирует главное преимущество ДО: везде и в любое время [1; 5].

Развитие информационных технологий позволяет решить проблему идентификации при помощи технологий биометрического мониторинга. В их основу положены методы биометрической идентификации, которая работает со статическими и динамическими образами объекта – студента. Биометрическая характеристика – это измеримая физиологическая или поведенческая черта человека, которая подразделяется на две группы – физиологическую (статическую) – характеристику, полученную путём измерения анатомических данных человека (отпечатки пальцев, форма лица, кисти, структура сетчатки глаз и др.), и поведенческую (динамическую) – группа биометрических характеристик, основанных на данных, полученных путём измерений действий человека, импульсов его мышц (рукописные и голосовые образы).

Общий принцип работы биометрической системы заключается в том, что студент с помощью регистрирующего устройства (сканер, камера и др.) предоставляет системе образец – опознаваемое изображение или запись статической или динамической характеристики. Биометрический образец обрабатывается системой, в результате чего формируется эталон студента, служащий для проверки. Как правило, эталон представляет собой числовую последовательность, которую нельзя использовать для восстановления самого образца.

Биометрический образ – это непосредственно наблюдаемый системой образ личности, без использования каких-либо операций по его предварительной обработке и масштабированию. В нашем случае биометрическим образом является индивидуальный клавиатурный почерк студента.

При обращении к системе, снятая в процессе идентификации характеристика сравнивается с эталоном. Хотелось бы отметить, что значение, полученное при доступе в систему, и эталон на сто процентов никогда не совпадут, поэтому, для принятия положительного решения о доступе, степень совпадения должна превышать какую-то настраиваемую пороговую величину. Качественной характеристикой биометрической системы является коэффициент ошибочных отказов и ошибочных подтверждений [2].

Но, в свою очередь, биометрическая идентификация имеет ряд недостатков:

1. Надёжность идентификации. Биометрические системы можно разделить на несколько видов, в зависимости от используемой БХЧ [4]. Надёжность систем, использующих разные БХЧ, различается. К наиболее надёжным относятся методы идентификации по отпечатку пальца, по сетчатке и радужной оболочке глаза. Менее надежными являются системы идентификации по геометрии руки и лица, голосу, динамике подписи.

2. Возможность взлома системы. Биометрическая идентификация не даёт стопроцентной защиты от взлома. Например, систему, идентифицирующую по радужной оболочке глаза можно обмануть, предоставив системе фотографию пользователя в высоком разрешении. Тем же способом можно обмануть и некоторые сканеры отпечатков пальцев. Вероятность ошибки часто напрямую зависит от стоимости биометрического сканера. Для дорогих систем вероятность ложного пропуска может колебаться в районе 0,1 % для более дешевых вариантов доходить до 10 %.

3. Высокая стоимость систем. Одним из недостатков биометрической идентификации является необходимость использования дополнительного аппаратного обеспечения, а именно, биометрических сканеров. Их цена сильно зависит от используемой БХЧ.

4. Недостаточная разработанность стандартов в данной области. Наиболее проработанным является идентификация по отпечаткам пальцев. Многие методы, основанные на других БХЧ, появились не так давно, и их разработчики опираются на международные стандарты при разработке устройств биометрической идентификации.

Далее уделим внимание некоторым математическим вопросам идентификации. Распознание биометрического образа осуществляется в результате сравнения показателей, которые его характеризуют, с некоторым биометрическим эталоном.

Биометрический эталон – это данные о стабильной части контролируемых биометрических параметров и их допустимых отклонениях, хранящиеся в биометрической системе для последующего сравнения с ними вновь предъявляемых биометрических образов. Вид эталона определяется принятым в системе решающим правилом.

В самом простом случае стабильная часть контролируемых биометрических параметров и их отклонения выражаются двумя показателями математической статистики: математическое ожидание и дисперсия. Именно эти параметры определяют решающее правило, на основании которого осуществляется идентификация личности студента.

Хранение эталонных данных осуществляется в биометрической системе – технической системе, которая построена на измерении биометрических параметров личности и способна после обучения её узнавать.

С этими эталонными данными следует сравнивать характеристики вновь предъявляемых биометрических образов, например, контролируемых параметров клавиатурного почерка студентов, идентификация личности которых осуществляется в процессе контроля выполнения конкретного задания.

В перспективе целесообразно разработать индивидуальную биометрическую систему, для чего привлечь к работе исследователей в сфере проектирования (научных работников) и разработчиков биометрических систем (инженеров).

Фундаментальный подход к разработке биометрической системы предусматривает выполнение всех процедур классического процесса формирования биометрического эталона.

В результате стремительной коммерциализации рынка биометрических технологий производители подобных систем фактически диктуют потребителям выгодные для себя условия и продают системы, ориентированные на среднестатистического пользователя. В первую очередь, их поведение обусловлено недостаточным уровнем конкуренции на развивающемся рынке биометрических систем [7].

Ещё одним негативным моментом является то, что современные биометрические системы идентификации личности дают значительный разброс своих показателей качества по отношению к заявленным в рекламе среднестатистическим показателям. Для половины пользователей купленная биометрическая система может работать существенно лучше, чем обещано в рекламе, но для другой половины эти обещания не оправдаются.

Кроме того, низкий уровень качества идентификации системой может являться результатом неудачного выбора словаря-пароля или следствием использования системой неудачной проекции биометрических параметров конкретной личности.

При разработке индивидуальной биометрической системы следует учитывать все вышеуказанные моменты.

Далее необходимо рассмотреть особенности принципиальной схемы функционирования современных биометрических систем. Прежде чем перейти к непосредственному описанию схемы, определим, что процесс идентификации личности студента в терминах биометрии называется аутентификация.

Более точно, аутентификация – это процесс доказательства и проверки подлинности заявленного элементом информационной технологии имени в рамках заранее определённого протокола.

В отличие от обычной идентификации, этот процесс предполагает низкий уровень доверия к тестируемой личности. Это значит, что тестируемый об этом процессе знать не должен.

В основе схемы аутентификации лежит обучение на множестве, состоящем из нескольких примеров биометрических образов пользователя (студента). Таким образом, в данном случае мы имеем дело с работой систем искусственного интеллекта, основанных на примерах [7].

В этом процессе в качестве учителя, в общем случае, выступает пользователь биометрической системы. Его функция в процессе аутентификации сводится к тому, что он предъявляет биометрической системе примеры различных вариантов биометрических образов (студентов) или векторы контролируемых параметров. Они могут быть представлены, например, в виде многократного повторения предварительно установленной парольной фразы.

Представленные системе примеры подаются непосредственно на вход нейронной сети, которая в совокупности с некоторым алгоритмом обучения является учеником биометрической системы и может находиться в двух режимах: режиме обучения и режиме тестирования качества обучения.

Применение нейронных сетей в качестве вычислительного базиса биометрических систем обусловлено тем, что динамические образы личности обладают свойством изменчивости во времени. С учётом этого свойства, для более точного формирования определённого эталона, пользователю системы необходимо задать несколько примеров реализации одного и того же биометрического образа (характеристик студента).

Обучение на примерах является отличительной характеристикой искусственных нейронных сетей.

При этом параметры биометрического эталона конкретного студента включают в себя: значения весов нейронной сети и значения смещающих коэффициентов для конкретной личности.

Алгоритм работы системы биометрической аутентификации включает следующие операции: преобразование неэлектрических величин (при клавиатурном мониторинге – положение рук) в электрические сигналы; кодирование сигналов и ввод их в процессор, осуществляющий программную обработку данных; масштабирование амплитуд входных сигналов и поиск для них формального эталонного значения; приведение сигналов к единому масштабу времени; вычисление вектора функционалов (вектора контролируемых параметров), которые могут быть линейными и нелинейными.

Завершая рассмотрение общих принципов биометрической идентификации, отметим, что в процессе дистанционного обучения необходимо учитывать технические аспекты защиты системы сканирования подлинности доступа.

В связи с этим, рекомендуется регулярно осуществлять аудит биометрической информации – процесс, который предполагает регистрацию, хранение и обработку результатов биометрической аутентификации за достаточно длительный интервал времени с целью выявления попыток атак на биометрические фрагменты системы защиты.

Аутентификация по биометрическим показателям в данный момент является наиболее продуктивной. Этот метод значительно уменьшает вероятность подмены одного пользователя другим. Однако его осуществление требует высоких затрат.

Проверка биометрических характеристик производится по следующим направлениям [3].

Верификация – проверка подлинности индивида (биометрические данные хранятся в базе данных и сравниваются с живым оригиналом). Могут быть два рода ошибок – принятие своего за чужого или чужого за своего.

Идентификация – биометрический шаблон пользователя сравнивается со всеми шаблонами базы данных на единичное совпадение.

Ограничение доступа – составляется список биометрических параметров, при совпадении с которыми пользователю отказывается в доступе.

В настоящее время в отечественных системах ДО применяются следующие методы биометрической аутентификации [2].

Контактные биометрические технологии: отпечаток пальца; отпечаток ладони; динамика работы с клавиатурой; динамическая проверка подписи.

Бесконтактные биометрические технологии: распознавание лица; термография лица; распознавание голоса; сканирование сетчатки глаза; сканирование радужной оболочки глаза.

**Выводы и перспективы дальнейших исследований**. Все вышеперечисленные технологии идентификации и аутентификации личности при дистанционном обучении в высшей школе не являются исчерпывающими, требуют дальнейших научных исследований и большой экспериментальной практической работы.

К новым перспективным исследовательским направлениям можно отнести следующие биометрические методы: методы, основанные на распознавании расположения ногтей и их контуров, идентификации солености тела, геометрических характеристик уха; множественная биометрия, при которой идентификация, аутентификация ведётся по нескольким биометрическим характеристикам сразу (находятся на стадии разработки): биометрическое шифрование; аутентификация и контроль пользователей по телефонным звонкам; метод идентификации по почерку вместе с проверкой пароля; метод аутентификации по входу в систему через LAN / Internet и одновременно через свой мобильный телефон; методы считывания изображения расположения вен, аутентификация по ДНК, биометрия мозговых волн, определение запаха тела, распознавание походки [8].

Таким образом, применение технических систем идентификации и аутентификации личности студента с элементами искусственного интеллекта в системе дистанционного обучения позволит повысить эффективность его функционирования.

**Библиографический список**

1. Бикмухаметов, И. Х. Дистанционное обучение : учеб. пособие / И. Х. Бикмухаметов. – Уфа : Уфимская гос. акад. экономики и сервиса, 2006. – 152 с.

2. Гладких, А. А. Базовые принципы информационной безопасности вычислительных систем : учеб. пособие для студентов, обучающихся по специальностям 08050565, 21040665, 22050165, 23040165 / А. А. Гладких, В. Е. Дементьев. – Ульяновск : УлГТУ, 2009. – 156 с.

3. Гурина, Е. Ю. Механизмы аутентификации пользователя для дистанционных систем образования / Е. Ю. Гурина, А. А. Модестов // Безопасность информационных технологий. – 2013. – Т. 20, № 1. – Москва : НИЯУ МИФИ. – С. 49–54.

4. Ложников, П. С. Распознавание пользователей в системах дистанционного образования: обзор [Электронный ресурс] / П. С. Ложников // Образовательные технологии и общество. – 2001. – № 2, Т. 4. – С. 211–216. // READera : сайт. – Электрон. дан. – Режим доступа: https://readera.org/raspoznavanie-polzovatelej-v-sistemah-distancionnogo-obrazovanija-obzor-14061940. – Дата обращения: 04.01.2021. – Загл. с экрана.

5. Овсянников, В. И. Введение в дистанционное образование : учеб. пособие для системы повышения квалификации и профессиональной переподготовки специалистов / В. И. Овсянников, А. В. Густырь ; МГОПУ им. М. А. Шолохова. – Москва : РИЦ «Альфа», 2001.

6. Описание механизмов идентификации личности учащихся при электронном дистанционном обучении [Электронный ресурс] // Открытый класс. Сетевые образовательные сообщества : сайт. – Электрон. дан. – [б. м.], 2010-2020. – Режим доступа: http://www.openclass.ru/node/254604. – Дата обращения: 02.01.2021. – Загл. с экрана.

7. Стефаненко, П. В. Теоретические и методические основы дистанционного обучения в высшей школе: дисс. … докт. пед. наук : 13.00.04 / Стефаненко Павел Викторович ; Институт педагогики и психологии профессионального образования АПН Украины. – Киев, 2002. – 478 л.+прил. 492 л.

8. Biometrics [Электронный ресурс] : сайт. – Электрон. дан. – [б. м.]. – Режим доступа: http://biometrics.pbworks.com/w/page/14811357/FrontPage. – Дата обращения: 12.12.2021. – Загл. с экрана.



*Рецензент д-р пед. наук, проф. Е. И. Приходченко*
*Статья поступила в редакцию 25.01.2021*

# PERSONAL IDENTIFICATION AND AUTHENTICATION METHODS IN DISTANCE LEARNING IN HIGHER EDUCATION

Prof. **Stefanenko Pavel Viktorovich,** Doctor of Pedagogic Sciences,
Professor of the Humanitarian Sciences Department
"The Civil Defence Academy" of EMERCOM of DPR
83050, Donetsk, 34a Roza Luxemburg Str.
E-mail: agz@mail.dnmchs.ru
Phone: +38 (062) 303-27-02

*Distance learning is a modern form of education that provides for the organization of the learning process at a distance. One of the essential problems of its implementation is the problem of identification and authentication of the user's identity, in particular, a student studying remotely in specially developed distance courses using information and communication technologies.*

*When implementing distance learning, you need to be sure that the student independently completes all the teacher's tasks. This article is devoted to the consideration of some ways to solve the complex process of identification and authentication of a person.*

***Keywords:*** *distance learning; identification; authentication; biometric image; biometric standard.*