При использовании материалов статьи необходимо использовать данную ссылку:
Фролов Р.Н., Дудченко А.В., Колкарева И.Н. Актуальные проблемы стандартизации требований к верификации личности пользователя в сети при организации дистанционного обучения // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 2 (54). С. 65-71

УДК 006.022+006.024

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СТАНДАРТИЗАЦИИ ТРЕБОВАНИЙ К ВЕРИФИКАЦИИ ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ В СЕТИ ПРИ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Фролов Р.Н., Дудченко А.В., Колкарева И.Н.

В статье рассмотрены технические и организационно-правовые аспекты верификации пользователей при организации доступа к on-line ресурсам в рамках дистанционного обучения в новых реалиях, связанных с распространением коронавирусной инфекции COVID-19. Отмечено, что имеющиеся решения являются недостаточными, так как простая регистрация и авторизация пользователей в сети не позволяет однозначно верифицировать подлинность лица, выполняющего задания, без применения видеосвязи (видеофиксации личности). Предложены мероприятия по выработке новых требований к верификации и совершенствованию правовой базы более надежной аутентификации и верификации пользователей при их работе в сети. В заключении отмечается, что на сегодняшний день решение многих вопросов, связанных с верификацией личности в электронной информационно-образовательной среде, остается в компетенции образовательных организаций, а федеральное законодательство лишь рамочно обозначает правила проведения аутентификации и верификации лиц. В связи с этим учебные заведения должны решить проблему получения согласия на обработку персональных (биометрических) данных в момент оформления отношений со студентом, до издания приказа о его зачислении в вуз, обозначив все нормативно-правовые, технические и организационные особенности локального характера.

Ключевые слова: аутентификация личности, верификация, дистанционное обучение, биометрические показатели, защита персональных данных.

Новые вызовы, связанные с распространением в первом квартале 2020 года глобальной биологической опасности в виде коронавируса COVID-19, предъявили новые требования к организации всех сторон жизни в условиях предпринимаемых со стороны государства ограничительных мер. Одной из сфер деятельности, в которых в числе первых был введен дистанционный режим работы, стало образование.

Министерство науки и высшего образования 14 марта 2020 года издало приказ за № 397 «Об организации образовательной деятельности в организациях, реализующих образовательные программы высшего образования и соответствующие дополнительные профессиональные программы, в условиях предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации». В частности, основные положения данного приказа предусматривают:

Фролов Руслан Николаевич, кандидат технических наук, доцент ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова» (Краснодарский филиал)
г. Краснодар
Дудченко Анна Владимировна, кандидат юридических наук, доцент ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова» (Краснодарский филиал)
г. Краснодар
Колкарева Инна Николаевна, кандидат юридических наук, доцент ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова» (Краснодарский филиал)
г. Краснодар

«организацию контактной работы обучающихся и педагогических работников исключительно в электронной информационно-образовательной среде; использование различных образовательных технологий, позволяющих обеспечивать взаимодействие обучающихся и педагогических работников опосредованно (на расстоянии), в том числе с применением электронного обучения и дистанционных образовательных технологий» [1]. Таким образом, все виды занятий (лекционные, практические, лабораторные), итоговую и промежуточную аттестации предполагается осуществлять в дистанционной форме на всех уровнях системы образования (СПО, ВО) вплоть до нормализации эпидемиологической ситуации в России и мире. И если техническая готовность системы образования к повсеместному ведению образовательного процесса в дистанционном режиме не вызвала серьезных нареканий, то организационная и юридическая стороны данной проблемы требуют более подробного рассмотрения и оценки.

На первый план в этой связи выходят вопросы однозначной аутентификации и верификации лиц, выполняющих электронные варианты заданий и проходящих промежуточную и итоговую аттестацию. Очевидно, что имеющиеся на сегодня средства и методы управления доступом, такие как: авторизация через логин и пароль, введение кодовых слов, цифровых паролей из SMS-сообщений, не позволяют гарантированно верифицировать соответствие физического лица, выполняющего задания, его «цифровому образу». То есть нельзя однозначно, с приемлемой достоверностью, поставить знак равенства между конкретным обладателем прав на вход в систему (студентом, учеником и т.д.) и человеком, реально выполняющим предложенные задания в сети.

В случае с текущим процессом обучения на уровне начального образования можно частично «закрыть глаза» на некоторые возможности сторонней помощи ребенку в выполнении отдельных заданий. Если усложнить систему авторизации и аутентификации пользователей (здесь, например, можно привести образовательный портал на базе интерактивной платформы uchi.ru), то данный ресурс, очевидно, будет не способен внедрить новые подходы и просто будет перегружен дополнительными задачами, вследствие большого количества пользователей по всей России. Поэтому такие ресурсы можно использовать исключительно как учебно-вспомогательные, тренировочные, без возможности проводить посредством них итоговую аттестацию. При этом уровень высшего образования (особенно такие виды дистанционного взаимодействия как защита курсовых работ, и иные разновидности промежуточного и итогового контроля) должен однозначно верифицировать личность студента, выходящего на связь. Дело в том, что имеющиеся в настоящее время средства авторизации, как было отмечено выше, не позволяют однозначно решить данную проблему.

Как пример можно привести прием зачетов, экзаменов или курсовых работ в on-line системах дистанционного тестирования на базе популярных продуктов Indigo, Iren и в других системах контроля знаний и аттестации [2]. В этом случае студент получает свой персональный логин и пароль для входа в систему тестирования посредством любого популярного и удобного для него браузера, что позволяет полностью перейти на on-line сдачу зачета или экзамена путем дистанционного тестирования. И здесь, уже на начальном этапе работы такой схемы, стали обозначаться первые проблемы достоверности верификации личности. Дело в том, что без визуального контакта в режиме реального времени, такое прохождение теста не может считаться однозначно достоверным, так как есть лазейка предоставить авторизованное в сети рабочее место другому лицу с более высоким уровнем подготовки в аттестуемой предметной области. В этом случае капча (CAPTCHA) также не спасает от возможности подмены лица, выполняющего задание, так как выполняет несколько иную функциональную задачу: определить, кем является пользователь системы – человеком или компьютером (ботом) и никак не привязана к личности человека, получившего доступ к системе.

В качестве одного из наиболее доступных вариантов решения данной проблемы, напрашивается видеосвязь в режиме реального времени посредством многочисленных on-line сервисов, таких как zoom.us, videomost.com и других. Видеосвязь с помощью таких систем, как правило, стабильна и позволяет вести широковещание, то есть экзаменатор может одновременно контролировать прохождение аттестации несколькими студентами. Однако данные системы накладывают определенные требования, которые предполагают точное согласование времени и наличия именно в это время технической возможности подключения к видеоконференции. Это вполне осуществимо при проведении занятий в формате

видеолекции, защите курсовых работ и проектов, но организационно и технически крайне затруднено в варианте выполнения как практических, лабораторных работ, так итогового и промежуточного контроля в форме зачетов или экзаменов. Особенно это будет затруднительно реализовать со студентами заочной формы обучения в случае, когда у них нет текущей сессии и, в силу занятости по основному месту работы, не всегда имеется возможность выйти на связь в строго установленное время.

Очевидно, что обозначенная проблема должна быть решена с той или иной степенью надежности и экономической целесообразности. Авторам представляется, что в этом случае ключ к решению проблемы можно найти в применении биометрических средств и методов идентификации личности, к которым относят различные виды, представленные на Рисунке 1.

Рисунок 1. Классификация биометрических средств идентификации (по данным [8])

Из представленного на схеме всего многообразия средств, для целей аутентификации и однозначной верификации пользователя при организации дистанционного обучения наиболее реалистичными представляется: форма кисти руки, папиллярные линии пальца (отпечаток пальца), форма лица и голос. Такие средства как: код ДНК и биопризнаки, находятся за гранью разумной экономической целесообразности, так как речь не идет о доступе к финансовым операциям. Все эти системы биометрической аутентификации, широко применяемые в настоящее время для идентификации личности в банковском секторе, должны быть встроены в модули систем электронной информационно-образовательной среды (далее – ЭИОС) (например, moodle) с целью обеспечения однозначной верификации личности не только при входе в систему, но и в процессе выполнения заданий или прохождения аттестации.

Здесь можно рассмотреть технологии распознавания лиц для учета рабочего времени. Суть данных технологий состоит в том, чтобы по полученному с камеры видеонаблюдения изображению произвести сверку образа физического лица с образом, хранимым в эталонной базе на сервере, фиксируя, таким образом, время прихода на работу и выхода с неё. В этом случае придется иметь на сервере базу биометрических данных (будут собираться при поступлении студента в учебное заведение или при зачислении ученика в школу), которая впоследствии может стать эталонной.

Вместе с тем следует обратить внимание на наличие существенной проблемы нормативно-правового обеспечения использования дистанционного образования в современных российских реалиях.

На сегодняшний день самой актуальной проблемой остается преодоление несоответствия дефиниции «персональные данные» всем законодательным актам, опосредующим процесс верификации и аутентификации лица. В данный период к персональным данным формально-юридически может быть отнесена практически любая информация о человеке, а имеющийся массив всевозможных разъяснений Роскомнадзора и иных ведомств об отнесении фото- и видео-изображения, дактилоскопических данных и

иной информации к биометрическим персональным данным не добавляет ясности.

Процесс идентификации личности и одновременно защита его персональных данных в период использования данного способа взаимоотношений обучающихся с учебным заведением, также явно демонстрирует ряд неразрешённых законодателем аспектов.

Законодательство обозначает перечень профессий и специальностей среднего профессионального образования, обучение по которым полностью в дистанционной форме не допускается (Приказ Министерства образования и науки России от 20.01.2014 №22) [3]. Документ ограничивает такую возможность не только для будущих зубных техников и операторов чесально-вязального оборудования, что представляется вполне логичным, но и для юристов, бухгалтеров и дизайнеров. Примечательно, что на сегодняшний день, аналогичный обобщенный перечень направлений подготовки и специальностей в рамках высшего образования не утвержден.

Также, при применении данного способа идентификации личности в системе возникает вопрос о правовом положении студента и способах защиты его персональных данных.

Оператору необходимо получить соответствующее согласие от субъекта персональных данных в соответствии с нормами Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [4]. Явно выраженное согласие субъекта персональных данных на их обработку является единственным законным основанием для любого вида обработки персональных данных. Вместе с тем законодатель предусмотрел ряд случаев на обработку персональных данных без согласия субъекта: в специальных целях обработки; специальным субъектом на стороне оператора; либо в указанных случаях в совокупности.

Носитель персональных данных, необходимых для верификации и аутентификации, должен принимать решение о согласии на их обработку свободно, своей волей и в своем интересе. Сложившаяся практика разрешения споров между субъектами оборота персональных данных свидетельствует о необходимости соответствия согласия следующим требованиям:

– должно быть выражено в форме действия с определенными, а неабстрактными намерениями. Молчание или бездействие лица, которые могут быть предусмотрены политикой конфиденциальности оператора формой согласия, не будет удовлетворять указанному требованию. Так же и в случае использования интернет-ресурсов с применением настроек конфиденциальности по умолчанию при отсутствии их изменения пользователем согласие на обработку персональных данных не будет считаться данным в надлежащей форме.

– должно быть информативно-наполненным, т.е. содержать одобрение, основанное на уяснении целей обработки; оператора и иных лиц, которые будут иметь доступ к конфиденциальной информации; сроках обработки и иной значимой информации, касающейся обработки персональных данных. Очевидно, что зачастую студентам необходимо разъяснить значение используемых терминов для полного соответствия согласия требованиям закона, поскольку без такого разъяснения информированность данного согласия может быть оспорена в суде.

– должно быть сознательным. Такое условие к даче согласия предполагает осмысленное принятие решения. Вынужденный характер дачи согласия ставит под сомнение его соответствие требованиям закона.

Форма согласия законодательно определена, но также вызывает некоторое непонимание в части правоприменения. В частности, согласие может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено отечественным законодательством. При этом помимо собственноручной подписи субъекта персональных данных на бумажном носителе признается и согласие в форме электронного документа, подписанного в соответствии с законодательством Российской Федерации электронной подписью, а также совершение конклюдентных действий. На практике получается, что зачастую студентами становятся лица, недостигшие возраста гражданской правосубъектности, и согласие от их имени должны давать их законные представители. Таким образом, использование биометрических данных студента не допустимо, а требуется создание эталонной базы, как студентов, так и всех их законных представителей. В такой ситуации может возникнуть конфликт защищённости баз данных операторов обработки персональных данных лиц. А это полностью противоречит целям и задачам образовательной деятельности.

При реализации образовательных программ или их частей, в которых используются только технологии электронного обучения и дистанционного обучения, «университет самостоятельно (или) с применением ресурсов

других организаций, должен производить идентификацию личности студента»[5].

То есть, чтобы сдать экзамен, пройти финальный тест или выполнить другое действие, студенту необходимо будет пройти идентификацию, запустив специальный скрипт, который можно разместить в учетной записи обучающегося. Программа подключится к вашей камере и сделает снимок человека, сидящего перед экраном, после чего она сверяет полученный кадр с фотографическим изображением, имеющимся в базе данных студентов университета. Только после получения подтверждения сходства доступ к заданию может быть разблокирован.

Сегодня весьма целесообразно перенять опыт отечественной финансовой системы, использующей Единую биометрическую систему на основе норм Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [6]. В 2018 году было запущено мобильное приложение «Ключ Ростелеком», которое основано на необходимости удалённого прохождения биометрической идентификации с помощью смартфона. В данной системе согласно Постановлению Правительства Российской Федерации от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» может использоваться сочетание двух параметров: «данные изображения лица человека, полученные с помощью фото- и видеоустройств; данные голоса человека, полученные с помощью звукозаписывающих устройств». Законодатель выбрал именно эти параметры по двум причинам:

1. Надёжности (они имеют наименее благоприятные показатели FAR / FRR).

2. Доступности (наличие веб-камеры, которая есть в любом современном мобильном устройстве).

Предполагается, что основанная на этих подходах система будет функционировать следующим образом. Обучающийся перед входом в ЭИОС активирует web-камеру на своем компьютере, с которого планируется выход в сеть для дистанционного выполнения заданий (сдачи зачета или экзамена). Сравнение поступающего видео с фотографией, хранимой на сервере учебного заведения, даст программный ключ к открытию банка заданий для выполнения. Как только web-камера в процессе выполнения задания фиксирует другое лицо (то есть рабочее место за компьютером занимает посторонний), то происходит разрыв соединения и аннулирование результатов выполнения задания.

Данные подходы и предложения представляются наиболее реалистичными в силу того, что в настоящее время уже существуют программные продукты, способные блокировать или предоставлять доступ к компьютеру, используя для этого технологию распознавания лиц. Для этого нужно лишь наличие web-камеры, распознающей «знакомое» лицо. Наиболее популярной программой, реализующей данный подход, является KeyLemon. Разработчики данного программного продукта уделили особое внимание безопасности данной системы. Например, программа может отличать реальное лицо от фотографии, различает лицо при нескольких уровнях освещения и содержит ряд других функций [7].

На сегодняшний день решение многих вопросов, связанных с верификацией личности в электронной информационно-образовательной среде, остается в компетенции образовательных организаций, а федеральное законодательство лишь рамочно обозначает правила проведения аутентификации и верификации лиц. В связи с этим учебные заведения должны решить проблему получения согласия на обработку персональных (биометрических) данных

в момент оформления отношений со студентом, до издания приказа о его зачислении в вуз, обозначив все нормативно-правовые, технические и организационные особенности локального характера. iea

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. Приказ Министерства науки и высшего образования Российской Федерации от 14 марта 2020 г. № 397 «Об организации образовательной деятельности в организациях, реализующих образовательные программы высшего образования и соответствующие дополнительные профессиональные программы, в условиях предупреждения распространения новой коронавирусной инфекции на территории Российской Федерации» // [Электронный ресурс] URL:

https://minobrnauki.gov.ru/ru/documents/card/?id_4=1064
2. Фролов Р.Н., Сидаравичене Е.М. Разработка информационных средств тренировочного тестирования школьников при подготовке к сдаче ЕГЭ // Вестник ИМСИТ, 2015. № 2 (62). С. 61-64.
3. Приказ Министерства образования и науки Российской Федерации от 20 января 2014 г. № 22 «Об утверждении перечней профессий и специальностей среднего профессионального образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий» // [Электронный ресурс] URL: https://rg.ru/2014/02/28/perechen-dok.html
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3451.
5. Приказ Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» // [Электронный ресурс]: URL: www.pravo.gov.ru.
6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
7. Программа, позволяющая организовать доступ к компьютеру по идентификации лица KeyLemon (условно-бесплатная) // [Электронный ресурс] URL: http://best-soft.ru/programs/8916.
8. Уков В.С. Интегральная защита информации // [Электронный ресурс] URL: http://www.vrsystems.ru/stati/integralnaya_zashita_informacii-1.htm

---

TOPICAL PROBLEMS OF STANDARDIZATION OF REQUIREMENTS ON VERIFICATION OF THE USER PERSONALITY IN THE NETWORK AT THE ORGANIZATION OF REMOTE LEARNING

Frolov Ruslan N., candidate of engineering sciences, Associate Professor, Department of Accounting and Analysis, Krasnodar branch of G.V. Plekhanov Russian University of economics, Krasnodar
Dudchenko Anna V., candidate of law sciences, Associate Professor, Department of Accounting and Analysis, Krasnodar branch of G.V. Plekhanov Russian University of economics, Krasnodar
Kolkareva Inna N., candidate of law sciences, Associate Professor, Department of Accounting and Analysis, Krasnodar branch of G.V. Plekhanov Russian University of economics, Krasnodar

The article deals with technical and organizational and legal aspects of user verification when organizing access to on-line resources in the framework of distance learning in the new realities associated with the spread of COVID-19 coronavirus infection. It is noted that the available solutions are insufficient, since simple registration and authorization of users in the network does not allow unambiguously verifying the authenticity of the person performing tasks without using video communication (video identification). Measures are proposed to develop new verification requirements and improve the legal framework for more reliable authentication and verification of users when they work in the network. In conclusion, it is noted that today the solution of many issues related to identity verification in the electronic information and educational environment remains within the competence of educational organizations, and Federal legislation only defines the framework rules for authentication and verification of individuals. In this regard, educational institutions must solve the problem of obtaining consent to the processing of personal (biometric) data at the time of registration of relations with the student, before issuing an order for his enrollment in the University, indicating all the legal, technical and organizational features of a local nature.

Key words: personality authentication, verification, distance learning, biometric indicators, protection of personal information.

REFERENCES:

1. Prikaz Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsii ot 14 marta 2020 g. № 397 «Ob organizatsii obrazovatel'noy deyatel'nosti v organizatsiyakh, realizuyushchikh obrazovatel'nyye programmy vysshego obrazovaniya i sootvetstvuyushchiye dopolnitel'nyye professional'nyye programmy, v usloviyakh preduprezhdeniya rasprostraneniya novoy koronavirusnoy infektsii na territorii Rossiyskoy Federatsii» [*Order of the Ministry of Science and Higher Education of the Russian Federation dated March 14, 2020 No. 397 «On the organization of educational activities in organizations implementing educational programs of higher education and relevant additional professional programs, in the event of the spread of a new coronavirus infection in the Russian Federation»*] // [Electronic resource] URL: https://minobrnauki.gov.ru/ru/documents/card/?id_4=1064

2. Frolov R.N., Sidaravichene Ye.M. Razrabotka informatsionnykh sredstv trenirovochnogo testirovaniya shkol'nikov pri podgotovke k sdache YEGE [*Development of information tools for training testing of schoolchildren in preparation for passing the exam*] // Vestnik IMSIT [*IMSIT Vestnik*], 2015. № 2 (62). pp. 61-64.

3. Prikaz Ministerstva obrazovaniya i nauki Rossiyskoy Federatsii ot 20 yanvarya 2014 g. № 22 «Ob utverzhdenii perechney professiy i spetsial'nostey srednego professional'nogo obrazovaniya, realizatsiya obrazovatel'nykh programm po kotorym ne dopuskayetsya s primeneniyem isklyuchitel'no elektronnogo obucheniya, distantsionnykh obrazovatel'nykh tekhnologiy» [*Order of the Ministry of Education and Science of the Russian Federation dated January 20, 2014 No. 22 «On approval of the lists of professions and specialties of secondary vocational education, the implementation of educational programs for which is not allowed using exclusively e-learning, distance learning technologies»*] // [Electronic resource] URL: https://rg.ru/2014/02/28/perechen-dok.html

4. Federal'nyy zakon ot 27.07.2006 № 152-FZ «O personal'nykh dannykh» [*Federal Law of July 27, 2006 No. 152-fz « On Personal Data»*] // Sobraniye zakonodatel'stva Rossiyskoy Federatsii [*Collection of Legislation of the Russian Federation*], 31.07.2006, № 31 (1 ch.), st. 3451.

5. Prikaz Ministerstva obrazovaniya i nauki Rossiyskoy Federatsii ot 23 avgusta 2017 g. № 816 «Ob utverzhdenii Poryadka primeneniya organizatsiyami, osushchestvlyayushchimi obrazovatel'nuyu deyatel'nost', elektronnogo obucheniya, distantsionnykh obrazovatel'nykh tekhnologiy pri realizatsii obrazovatel'nykh program» [*Order of the Ministry of Education and Science of the Russian Federation dated August 23, 2017 No. 816 «On approval of the Procedure for the use by organizations engaged in educational activities of e-learning, distance learning technologies in the implementation of educational programs»*] // [Electronic resource]: URL: www.pravo.gov.ru.

6. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» [*Federal Law of July 27, 2006 No. 149-ФЗ «On Information, Information Technologies, and Information Protection»*] // Sobraniye zakonodatel'stva Rossiyskoy Federatsii [*Collected Legislation of the Russian Federation*], 31.07.2006, № 31 (1 ch.), st. 3448.

7. Programma, pozvolyayushchaya organizovat' dostup k komp'yuteru po identifikatsii litsa KeyLemon (uslovno-besplatnaya) [*A program that allows you to organize access to a computer by identifying a person KeyLemon (shareware)*] // [Electronic resource] URL: http://best-soft.ru/programs/8916.html

8. Ukov V.S. Integral'naya zashchita informatsii [*Integral information protection*] // [Electronic resource] URL: http://www.vrsystems.ru/stati/integralnaya_zashita_informacii-1.htm