CC BY 4.0

УДК 378
DOI: http://dx.doi.org/10.21686/1818-4243-2023-5-33-44

Д.А. Вилявин[1], Н.В. Комлева[2], Н.А. Мамедова[2], А.И. Уринцов[2]

[1] ООО Сколопендра, Москва, Россия
[2] Российский экономический университет им. Г.В. Плеханова, Москва, Россия

Цифровые профили компетенций в образовании

Цель исследования. *Тенденция персонализации обучения формирует запрос на разработку и внедрение программных средств для обработки цифрового следа обучающегося, для управления его образовательной траекторией. В комбинации с технологиями децентрализованной идентификации такие программные средства предполагают более активную роль обучающегося в вопросах построения его персональной траектории обучения. Дополнительными вызовами для разрабатываемых программных средств является функциональное требование по обеспечению независимости данных профиля обучающегося от отдельных образовательных сервисов при одновременном соблюдении стандартов информационной безопасности работы с данными. Цель выполненного исследования – расширить представление о возможности модификации онлайн-обучения за счет включения распределенных решений в область применения информационных технологий в образовании.*

Материалы и методы. *В статье подробно рассмотрены разработанные авторами решения по программной реализации цифрового профиля компетенций обучающегося – децентрализованного приложения, предназначенного для хранения данных учебной активности и подтвержденной квалификации, агрегированных из различных внешних образовательных платформ, сервисов. При формировании этих решений авторы исходили из преимуществ применения децентрализованного подхода к разработке программного обеспечения. Методологическая основа проведенного исследования представлена комплексом подходов и технологий, поддерживающих логику процесса разработки программного обеспечения – технология распределенного реестра, подход цифровой идентификации, стандарт хранения учетных данных.*

Результаты. *Авторами обоснован выбор решения для программной реализации цифрового профиля компетенций: подход SSI обеспечит децентрализованную идентификацию данных цифрового следа вне границ отдельных образовательных платформ, сервисов; применение стандарта проверяемых учетных данных VC создаст условия для децентрализованного хранения данных учебной активности. Результаты исследования могут представлять практический интерес для администрации отечественных образовательных организаций, администрации образовательных платформ и образовательных сервисов, реализующих программы онлайн обучения для эффективного и безопасного управления данными цифрового следа каждого отдельного обучающегося, построения в его интересах индивидуальной образовательной траектории и подтверждения компетенций.*

Заключение. *Внедрение и масштабирование цифрового профиля компетенций направлено на обеспечение идентификации, безопасного хранения, эффективного управления данными цифрового следа обучающегося, которые могут быть применены для построения индивидуальной траектории обучения. Цифровой профиль компетенций позволит реализовать функцию подтверждения любых форм активности, характера взаимодействия обучающегося с функциями образовательного сервиса, а также позволит обучающемуся контролировать использование размещенной в цифровом профиле информации и управлять ею. Как часть целого цифровой профиль рассматривается в общей архитектуре информационной системы, что предполагает взаимодействие программного приложения с иными подсистемами, в том числе в структуре образовательной платформы. Схема взаимодействия продемонстрировала для цифровой образовательной платформы «Цифровой тьютор», разработанной в Российском экономическом университете им. Г.В. Плеханова. Проведения дополнительных исследований требуют инструменты контроля активности и мотивации обучающегося для формализации его активной роли в вопросах управления персональной траекторией обучения.*

Ключевые слова: *образовательная платформа, цифровой профиль, персональная траектория обучения, разработка программного обеспечения, децентрализованное приложение, управление идентификацией.*

Daniil A. Vilyavin[1], Nina V. Komleva[2], Natalia A. Mamedova[2], Arkady I. Urintsov[2]

[1] Team Lead Backend, Skolopendra LLC, Moscow, Russia
[2] Plekhanov Russian University of Economics, Moscow, Russia

Digital Competence Profiles in Education

Purpose of research. *The trend of personalization of learning forms a demand for the development and implementation of software tools for processing the digital footprint of the learner, to manage his/her educational trajectory. In combination with decentralized identification technologies, such software tools assume a more active role of the learner in the creation of his/her personal learning trajectory. Additional challenges for the developed software tools are the functional requirement to ensure the independence of learner profile data from individual educational services, while at the same time complying with the standards of information security of working with data. The purpose of this research is to expand the understanding of the possibility of modifying online learning by including distributed solutions in the field of information technology application in education.*

Materials and methods. *The paper describes in detail the solutions developed by the authors for software implementation of a digital profile of learner's competencies - a decentralized application designed to store data of learning activity and confirmed qualifications aggregated from various external educational platforms and services. When forming these solutions, the authors proceeded from the advantages of using a decentralized approach to software development. The methodological basis of the research is represented by a set of approaches and technologies that support the logic of the software development process - distributed registry technology, digital identification approach, credentials storage standard.*

Results. *The authors substantiate the choice of solution for software implementation of digital competence profile: SSI approach will provide decentralized identification of digital footprint data beyond the boundaries of individual educational platforms and services; application of the standard of verifiable VC credentials will create conditions for decentralized storage of learning activity data. The results of the study may be of practical interest for the administration of domestic educational organizations,*

administration of educational platforms and educational services implementing online learning programs for effective and secure management of each individual student's digital footprint data, creating an individual educational trajectory in his/her interests and confirming competencies.

Conclusion. *Implementation and scaling of the digital competence profile are aimed at ensuring the identification, safe storage, and effective management of the learner's digital footprint data, which can be used to create an individual learning trajectory. The digital competence profile will allow to realize the function of confirming any forms of activity, the nature of interaction of the learner with the functions of the educational service, as well as allow the learner to control and manage the use of the information placed in the digital profile. As part of the whole, the digital profile is considered in the overall architecture of the information system, which implies the interaction of the software application with other subsystems, including in the structure of the educational platform. The scheme of interaction demonstrated for the digital educational platform "Digital Tutor" developed at the Plekhanov Russian University of Economics. Additional research requires tools for controlling the activity and motivation of the learner to formalize his/her active role in the issues of personal learning trajectory management.*

Keywords: *educational platform, digital profile, personal learning trajectory, software development, decentralized application, identity management.*

1. Введение

Обучение, как активная учебно-познавательная деятельность, может рассматриваться и как способ взаимодействия с окружающим миром, с точки зрения теории социального научения [1], и как реакция на ускоряющееся развитие окружающей действительности, которое оказывает серьезное воздействие на человека в соответствии с теорией кинематического общества [2]. Исследования в предметной области теории обучения показывают, что охват и темпы образовательной деятельности в глобальном аспекте растут [3]. Получили широкое развитие и активно масштабируются такие идеи, как «обучение на протяжении всей жизни», «самообразование как образ жизни», «образованность как фактор достижения успеха в жизни». И, если последние десятилетия информационные технологии оказывали, в основном, функции технической и, в некоторой степени, интеллектуальной поддержки образовательного процесса, то сегодня в фокусе внимания информационные технологии, которые обеспечат персонализацию обучения, в том числе: управление индивидуальной траекторией обучения, включение иммерсивных компонентов образовательной среды, проверку знаний, направленную на выявление пробелов в образовании. Такого рода задача формулирует, в первую очередь, запрос к разработке и внедрению цифрового профиля компетенций на основе инструментов децентрализованной идентификации (Decentralized identity) [4].

Эти инструменты позволяют выстраивать систему управления данными вокруг обучающегося, реализуя логику и подходы децентрализованных приложений (DApps) [5], каким и является индивидуальный цифровой профиль компетенций, и обеспечивая защиту персональной информации. Цифровой профиль аккумулирует данные об обучении, которые каждый человек накапливает на протяжении своей жизни и которые преимущественно хранятся в базах данных образовательных сервисов бессистемно и непродуктивно с точки зрения возможностей построения индивидуального (уникального) цифрового профиля компетенций.

Но даже, сформировав такой цифровой профиль, необходимо решить задачу подтверждения приобретенных компетенций. Иначе результат пользовательского запроса к данным цифрового профиля будет ограничен выгрузкой сведений об опыте обучения. На помощь приходят инструменты сбора и обработки цифрового следа обучающегося (метаданные о любых формах активности, о характере его взаимодействия с функциями образовательного сервиса) [6]. Отдельной задачей, требующей проведения дополнительных исследований, является реализация функции извлечения полезной информации из собранного цифрового следа [7].

Обобщая проблематику применения технологий децентрализованной идентификации [8] в свете тенденции персонализации обучения, обозначим комплекс задач, требующих решения. Первая сложность на пути внедрения инструмента децентрализованной идентификации обучающегося состоит в том, что данные цифрового следа сгенерированы и хранятся в базах данных различных сервисов, не связанных между собой ничем кроме того факта, что эти данные относятся к одному человеку и должны быть интегрированы в его цифровой профиль компетенций. Вторая сложность заключается в подтверждении приобретенных компетенций, поскольку без этого невозможно утверждать, что данные об обучении не содержат ошибок и не фальсифицированы. Обозначенные сложности относятся к техническим задачам системной архитектуры. Их преодоление раскроет потенциал цифрового профиля компетенций, непосредственное управление которым осуществляет владелец персональных данных – обучающийся, активно формирующий собственную образовательную траекторию [9]. Таким образом, необходимо предложить решение, которое обеспечило бы децентрализованную идентификацию данных цифрового профиля компетенций на основе сгенерированного и

обработанного цифрового следа вне границ отдельных образовательных платформ.

2. Материалы и методы

Чтобы использовать преимущества децентрализованной идентификации для агрегирования данных цифрового профиля компетенций с различных цифровых образовательных платформ и сервисов, следует изменить подход к управлению данными цифрового следа обучающегося. Для этого определим порядок формирования и хранения данных, наполняющих цифровой профиль компетенций.

В общем виде цифровая образовательная платформа включает две основные подсистемы – Learning Management System (LMS) и Learning Record Store (LRS).

LMS предназначена для администрирования процесса обучения и вне зависимости от типа (открытые, облачные, коробочные) обеспечивает поддержку онлайн курсов. В том, что разработка онлайн курсов осуществляется на основе образовательных стандартов, таких, к примеру, как SCORM, xAPI, cmi5, проявляется подход к стандартизации образовательных продуктов, поскольку это позволяет наполнять хранилище любой LMS, поддерживающей эти стандарты.

LRS, в свою очередь, обеспечивает хранение учебных активностей (взаимодействие с учебными материалами, оценки), формируя цифровой след и фиксируя в базах данных действия, осуществляемые обучающимся. Анализ такой информации позволяет и штатно мониторить учебный процесс в целом, и выявлять особенности траектории обучения отдельного пользователя образовательной платформы в процессе прохождения им онлайн курса.

Функциональные возможности LRS систем не претерпели серьезных изменений со времени первой версии спецификации Tin Can в 2013 году, эволюция затронула в большей степени архитектуру систем. С одной стороны, LRS позволяет охватить разные виды активностей обучающегося в разных учебных средах (живой класс, мобильный телефон, LMS). С другой, система хранения учебных активностей может быть интегрирована в LMS, а может распространяться в качестве отдельного продукта.

На текущий момент LRS системы чаще всего носят централизованный характер, т.е. хранят информацию об обучении только в той организации, где и осуществлялось обучение, и при условии наличия такого хранилища. Такой тип хранения крайне ограничивает процесс персонализации обучения, поскольку экспорт данных цифрового следа затруднен в силу многих причин – от правовых ограничений информационного обмена и уровня доверия к накопленным данным до технических ограничений при транзакции данных между информационными системами. Для подтверждения пройденного обучения выдается документ (диплом, свидетельство, сертификат), выданный образовательной организацией. Однако сам документ и факт его выдачи не могут являться достаточным подтверждением приобретенных компетенций, поскольку существуют риски подделки документа, фальсификации содержащихся в нем данных или данных о выдаче.

Все это формирует потребность в разработке информационной системы, которая предоставит возможность не только децентрализовано хранить данные учебной активности, но и хранить поступающие из различных внешних систем подтвержденные сведения в соответствии со стандартом проверяемых учетных данных (Verifiable Credentials (VC)) [10], свидетельствующие о получении образовательных документов. Архитектура подобной информационной системы предполагает применение технологии распределенного реестра [11]. Выбор в пользу альтернативного решения – применения технологии распределенных баз данных – является неверным. В таком случае архитектура была бы ограничена совокупностью взаимосвязанных абонентских систем, а вариант объединения всех цифровых образовательных сервисов в сеть локальных баз данных следует признать утопическим, поскольку необходимого уровня доверия и технической интеграции между цифровыми сервисами – держателями данных цифрового следа – нет. Таким образом, выбор технологии распределенного реестра для разработки решения по децентрализованному хранению данных цифрового следа закономерен. Если говорить о перспективе создания цифровой экосистемы образования в рамках национальной цифровой экосистемы (НЦЭ), то децентрализованная архитектура также является оптимальным решением, поскольку она обеспечит гибкость и функциональность работы цифровых сервисов – компонентов экосистемы образования на платформенной основе.

Механизм работы распределенной системы предполагает управление базами данных при отсутствии единого центра управления. Составление и запись обновления реестра осуществляется узлами независимо друг от друга. Алгоритмы консенсуса обеспечивают корректное состояние сети блокчейна, что гарантирует безопасность и достоверность хранимых данных [12]. Построенная на основе технологии распределенного реестра архитектура информационной системы обеспечивает работу децентрализованных цифро-

вых хранилищ, с возможностью подтверждения не только полученных документов об обучении, но и данных цифрового следа.

Представим возможности применения технологии распределенного реестра, в частности технологии блокчейн, и решений на основе подхода цифровой идентификации (Self-sovereign identity, SSI) и стандарта хранения ученых данных Verifiable Credentials для подтверждения документа об обучении.

Подтверждение документа осуществляется с применением алгоритмов криптографии, а механизм блокчейн нивелирует риск подмены или модификации уже добавленной информации. Уровень безопасности учетных данных обеспечивается посредством применения подхода SSI. Реализация принципа децентрализованной идентификации на основе механизма блокчейн не только позволяет изменить подход к разработке цифровых профилей компетенций в рамках вновь разрабатываемых информационных систем, но и предложить улучшения для существующих цифровых образовательных сервисов. Любые действия обучающегося во время образовательного процесса будут записаны, подтверждены и, пройдя алгоритм обработки цифрового следа, аккумулированы в цифровой профиль компетенций. Здесь уместно привести в качестве аналогии широко используемую в сфере электронной коммерции технологию NFT (non-fungible token). Она фиксирует право владения цифровым объектом за уникальным пользователем, а присваиваемый невзаимозаменяемый токен (NFT) позволяет идентифицировать собственника цифрового или материального актива. Можно предположить в парадигме форсайта, что расширение области применения криптографических токенов ускорит темпы цифровизации и замену бумажных документов, в том числе, в сфере образования.

Формирование и наполнение цифрового профиля компетенций создает предпосылки к дальнейшему его использованию при построении индивидуальной траектории обучения. Алгоритм информационной системы, представленный, например, отдельным модулем цифровой образовательной платформы, обеспечит поддержку принятия решения о построении индивидуального плана обучения и выдаче обучающемуся учебных объектов из репозитория LMS, задействуя инструменты децентрализованной идентификации.

Данная логика управления цифровым профилем компетенций реализуема с использованием LRS систем в качестве основного источника данных. Но для реализации принципа децентрализованной идентификации важно, что построение и дизайн LRS стандартизированы и описаны в спецификации по построению таких систем [13]. Необходимо, чтобы каждое хранилище учебных активностей, интегрируемых в цифровой профиль компетенций, обладало единым форматом хранения данных, получаемых из различных источников: онлайн-курсы, игры, симуляции и любые другие формы реализации обучающих ресурсов. Формат хранения каждой учебной активности описан в спецификации к стандарту xAPI. Использование стандарта делает возможным сбор цифрового следа в виде учебных активностей. Вместе с тем стандарт описывает исключительно структуру хранимых данных, но строгих требований к хранению этой информации нет. Это позволяет использовать его в работе децентрализованных цифровых хранилищ, в частности, для хранения данных в цифровом профиле компетенций.

Помимо учебных активностей обучающегося необходимо хранить достоверную информацию о полученных документах, подтверждающих прохождение обучения. При этом централизованная система управления базами данных не исключает риск подделки документов об обучении или фальсификации данных в них, например, подделку итоговых документов и результатов промежуточных контрольных аттестаций. Децентрализованный подход к управлению базами данных, реализованный через механизм блокчейн, снижает вероятность указанного риска до нуля и рекомендован к использованию при проектировании и реализации цифрового профиля компетенций.

Безусловно, применение инструментов децентрализованной идентификации в качестве стандартов разработки цифровых образовательных платформ сегодня может рассматриваться только в перспективе. Но для формирования цифровой экосистемы национального проекта «Образование» в комбинации с реализацией мероприятий Дорожной карты развития «сквозной» цифровой технологии «системы распределенного реестра» масштабирование инструментария децентрализованной идентификации является очевидным решением. Технология создания и исполнения децентрализованных приложений признана субтехнологией «сквозной» технологии «системы распределенного реестра». Децентрализованные приложения, необходимые для хранения данных учебной активности и подтвержденных сведений по стандарту VC, обладают рядом преимуществ:

- распространение данных из хранилища только с разрешения их владельца на использование данных в объеме и на период, определенных им;
- возможность взаимодействия неограниченного коли-

чества участников распределенной системы;

• прозрачная и открытая логика, обеспечивающая гарантированное исполнение заданных функций в рамках систем распределенного реестра.

Признаком внедрения субтехнологии для проектирования и разработки децентрализованного приложения, каким является цифровой профиль компетенций, следует считать применение средств, интерфейсов создания и исполнения алгоритмов цифровой идентификации (SSI) и сценариев извлечения из LRS полезной информации в общем объеме собранного цифрового следа. В России уже отмечены практики применения технологии децентрализованной идентификации на базе образовательных сервисов и платформ – выдача документов об обучении на основе механизма блочейн (цифровой диплом) с подтверждением полученного документа по стандарту оформления электронных документов W3C Verifiable Credentials (VC)[1]. Таким образом, в России уже предприняты первые успешные шаги по масштабированию технологии распределенного реестра в сфере образования. Чем большее распространение получит технология, тем скорее проявят себя преимущества децентрализованного подхода при взаимодействии LRS систем различных образовательных сервисов (платформ), которые будут использовать децентрализованное приложение – цифровой профиль компетенций.

3. Результаты

Цифровой профиль компетенций является принципиально новым решением с точки зрения организации работы с обучающимися. Децентрализованное приложение будет открытым для них и позволит обучающимся участвовать в управлении учебными активностями. Единый стандарт разработки таких децентрализованных приложений будет способствовать их интеграции с LMS и LRS системами, которые станут источниками данных, аккумулируемых цифровым профилем компетенций. Таким образом, данные цифрового следа становятся содержимым децентрализованного хранилища учебных активностей самых разных форм (онлайн-курсов, симуляций, игр, тренажеров).

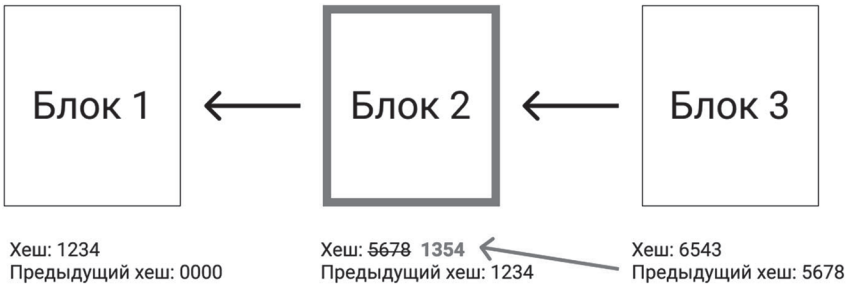

Рис. 1. Цепочка блоков в блокчейн
Fig. 1. The block chain in the blockchain

Цифровой профиль компетенций является основой для принятия решений при построении индивидуальной траектории обучения. Хранимые данные в децентрализованном приложении должны быть устойчивы к подмене документов и фальсификации данных, в противном случае риск недостоверной информации обесценит выработанные рекомендации по подбору онлайн-курсов и динамике процесса обучения. Достижение необходимого уровня безопасности хранящихся данных в цифровом профиле компетенций обеспечивается механизмом блокчейн, применение которого для демонстрации преимуществ технологии децентрализованной идентификации обосновано и уже дало первые положительные результаты.

Генерируемая механизмом блокчейн цепочка блоков хранит в себе информацию обо всех произведенных в информационной системе транзакциях – выдаче документов об обучении, прохождении промежуточных контрольных мероприятий и др. В цепочке блоков каждый последующий связывается с предыдущим с помощью вычисленного хеша из отправляемых данных (Рисунок 1), благодаря чему попытка изменения данных вызовет замену одного из блоков и приведет к потере целостности цепочки и данных. Блокчейн спроектирован таким образом, чтобы нарушение целостности блоков было очень трудным действием, которое требует огромного количества вычислительной мощности компьютера для пересчета всех блоков [14]. Нарушение целостности не будет зафиксировано только в том случае, если мошенник смог захватить контроль над более 51% общего числа узлов в децентрализованной сети.

Устойчивость к нарушению целостности цепочек блоков и криптографические алгоритмы защиты информация обусловливают целесообразность применения механизма блокчейн для подтверждения данных, генерируемых цифровым профилем компетенций. Например, хранение доказательств полученного документа об обучении возможно в одном из блоков в цепочке, что делает подмену данных или удаление данного блока крайне затруднительной операцией.

Однако на текущий момент механизм блокчейн не позво-

[1] Verifiable Credentials Data Model v1.1. W3C Recommendation. Режим доступа: https://www.w3.org/TR/vc-data-model/

ляет убедиться в достоверности хранимой информации, будь это документ об обучении или данные цифрового следа. Блокчейн в цифровых профилях применяется исключительно как децентрализованное хранилище ключей и идентификаторов, а их подтверждение реализовано через подход самостоятельной (независимой или суверенной) идентичности (SSI). SSI, как подход цифровой идентификации, позволяет пользователю контролировать использование размещаемой им в Интернете информации и управлять ею – делиться с частными лицами или публичными институтами, отслеживать использование или отменять доступ [15]. Децентрализованная архитектура на основе SSI приоритизирует такие характеристики взаимодействия пользователей информационных систем, как безопасность, конфиденциальность, индивидуальная автономия. Обучающийся и образовательная организация могут образовать доверительную связь, где обучающийся может поделиться своим цифровым следом (из хранилища цифрового профиля компетенций) с образовательной организацией для построения индивидуальной траектории. Например, при поступлении в университет абитуриенту необходимо подтвердить получение школьного аттестата. Подтверждение возможно реализовать с помощью SSI. На текущий момент некоторые организации и страны активно применяют такую модель в своей деятельности [16-18].

Подход SSI предоставляет следующие преимущества реализации доверительной связи:

- полностью разрешенные и соответствующие GDPR данные[1], поскольку клиент является собственником своих данных, может разглашать информацию в своих интересах и сам отвечает за их безопасность;
- выборочное раскрытие атрибутов (т. е. владельцы данных могут выбирать, какими фрагментами данных они хотят поделиться) то, что, на текущий момент, практически невозможно при обмене данными между участниками.

Подход Self-sovereign identity строится на нескольких основных блоках или уровнях. На первом уровне SSI – это набор принципов о том, как идентификация и контроль персональных данных должны работать в цифровых сетях. На другом уровне SSI – это набор технологий, основанных на базовых концепциях управления идентификацией, распределенных вычислениях, технологии блокчейн или распределенного хранилища данных (DLT) и криптографии.

Концепты, составляющие суть подхода SSI, известны давно, но благодаря цифровым технологиям стала возможной их реализация. К таким следует отнести:

1. Проверяемые учетные данные (Verifiable Credentials, VC) (например, документы об обучении, водительские права, сертификаты и другие виды документов).
2. Треугольник доверия между эмитентами, держателями и проверяющими.
3. Цифровой кошелек.
4. Цифровой агент.
5. Децентрализованная идентификация (DID).
6. Блокчейн, система распределенного реестра.

Проверяемые учетные данные (VC) – это центральный элемент архитектуры на основе SSI. Каждый VC имеет определенную структуру данных, поддержку различных форматов и параметров цифровой подписи. Проверяемые учетные данные были стандартизированы в консорциуме World Wide Web (W3C) в 2019 году.

На самом деле физическую версию проверяемых учетных данных (VC) мы используем постоянно – документы об обучении, например. В отношении физических версий актуальны риски потери, несанкционированного копирования и распространения, компрометации. Кроме того, использование физических версий невозможно в Интернете – необходимо оцифровывание данных в веб-форму. Такие действия занимают время, подвержены ошибкам и нарушениям конфиденциальности. VC, которые в настоящее время являются открытым стандартом консорциума World Wide Web (W3C), позволяют эмитентам конвертировать физические версии в цифровые VC, чтобы каждый мог хранить их в памяти любого устройства и использовать онлайн.

В сочетании с этим преимуществом простоты использования, обучающиеся также получают иные преимущества, работая с цифровыми аналогами физических документов:

- VC не могут быть скопированы или скомпрометированы;
- VC чрезвычайно трудно украсть (злоумышленнику потребуется украсть доступы к хранимым данным);
- VC поддерживают выборочное раскрытие информации;
- VC поддерживают меньший объем привилегий – имеется разрешение только на выполнение необходимых задач;
- выпуск VC не влечет существенных затрат;
- возможно их делегирование для использования другим лицом (при условии, что эмитент разрешает это).

Практика проектирования и разработки программных приложений показывает, что высока вероятность появления на рынке ИТ-продуктов множества различных цифровых профилей компетенций. Этап хаотичного насыщения рынка

[1] General Data Protection Regulation. Информация о GDPR на русском языке. Режим доступа: https://ogdpr.eu/ru

ИТ-продуктов и постепенного упорядочивания и концентрации завершится разработкой и внедрением стандарта разработки вида (класса) программных приложений. Сегодня Verifiable Credentials наращивают популярность, благодаря потенциалу блокчейн и распределенных реестров, которые могут служить децентрализованными проверяемыми реестрами данных. Однако, нельзя не отметить, что блокчейн не является единственным возможным вариантом, – проверяемые реестры данных бывают и централизованными. В будущем соотношение практики применения вариантов решения может измениться в долгосрочной перспективе по мере развития стандартов, но уже сейчас реестры обеспечивают эффективную работу экосистемы проверяемых учетных данных. Это и объясняет рост их популярности.

Экосистема SSI в сфере образования представлена несколькими категориями участников: Эмитент, Верификатор, Держатель (рисунок 2).

Verifiable Data Registry является местом, к которому осуществляется привязка децентрализованного идентификатора (DID). Каждый из участников общается между собой с помощью DID. Типичная схема подтверждения VC реализована следующим образом:

1. Эмитенты являются источником проверяемых учетных данных (VC) – у каждой учетной записи есть эмитент. Большинство эмитентов – это организации в виде государственных, муниципальных органов, учреждений и организаций. Физические лица также могут быть эмитентами.

2. Держатели (пользователи) запрашивают проверяемые учетные данные у эмитентов. Хранят их в своем цифровом хранилище и предоставляют доказательства VC, когда они запрашиваются Верификатором.

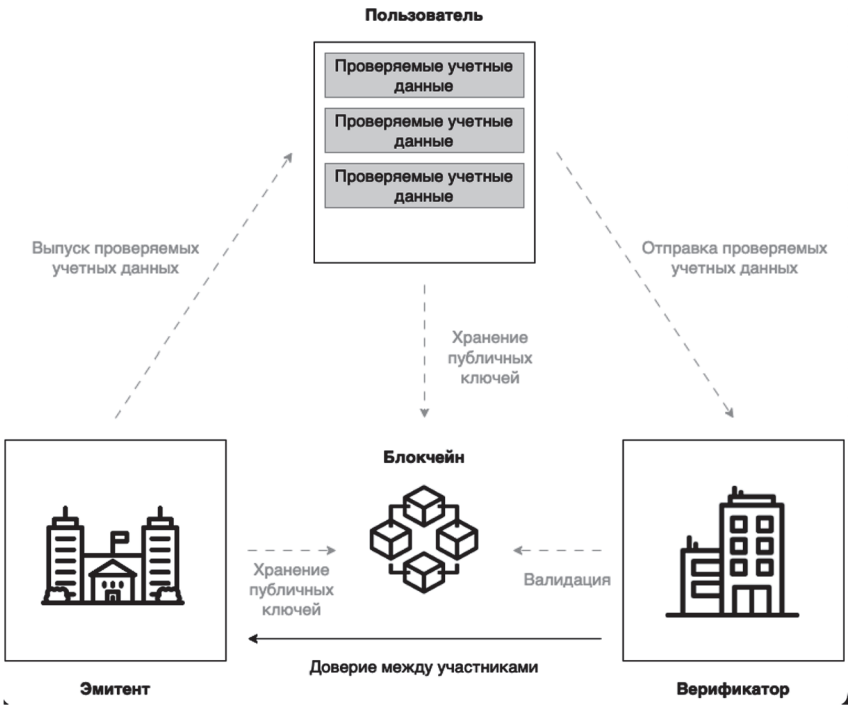

Рис. 2. Схема цифровой идентификации данных с использованием подхода SSI

Fig. 2. Digital data identification scheme using the SSI approach

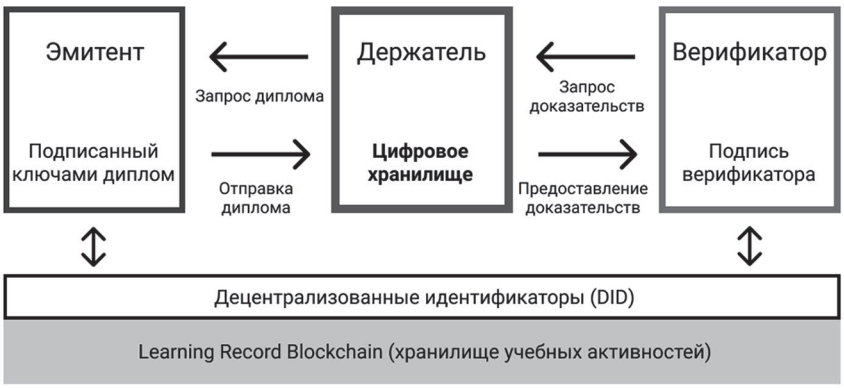

Рис. 3. Отношения между Эмитентом (университет), Держателем (студент) и Верификатором – треугольник доверия

Fig. 3. The relationship between the Issuer (university), the Holder (student) and the Verifier – the triangle of trust

3. Верификаторами могут выступать любые физические лица или организации. Верификаторы запрашивают доказательства у держателей одного или нескольких проверяемых VC. Если держатель согласен на передачу данных, то агент держателя возвращает доказательство, которое затем может проверить верификатор. Важным шагом в этом процессе является проверка цифровой подписи эмитента, обычно выполняемая с использованием DID.

Применительно к сфере образования в SSI архитектуре эмитентом является университет, который выдает цифровой эквивалент диплома (Verifiable Credential), держатель полученного документа – обучающийся. Цифровой альтернативой печатей, подписей и других подтверждающих элементов выступают криптографические ключи. На рисунке 3 изображен процесс получения документа об обучении.

4. Обсуждение

С помощью новых технологий, моделей и подходов происходит модификация онлайн-обучения. Благодаря этому, возросла популярность дистанционного обучения. Для дальнейшего развития обучения в онлайн предлагается развивать существующие решения, применяя новые подходы и инструменты к управлению хранилищем учебных активностей и к подтверждению полученных документов об обучении с помощью механизма блокчейн и подхода SSI. Это позволит сделать более активной роль обучающегося – он сможет полноценно реализовать свое право раскрывать информацию о своем обучении и самостоятельно обеспечивать ее безопасность.

Функционал децентрализованного приложения – цифрового профиля компетенций – предусматривает также для обучающегося возможность управлять аккумулированными данными цифрового следа. Извлеченная после обработки цифрового следа полезная информация может быть использована самим обучающимся или предоставлена образовательной организации для построения индивидуальной траектории обучения.

Например, после обучения в школе абитуриент подтверждает VC своих оценок в аттестате и в формате «треугольника доверия» предоставляет университету согласие на формирование траектории своего обучения в роли студента. При этом действующая доверительная связь создает оптимальные условия взаимодействия участников, но никак не ограничивает самих участников в принятии решений по организации процесса обучения. В программах дополнительного образования наличие подтвержденных компетенций позволит выстроить для конкретного слушателя индивидуальную программу обучения, сократив или, наоборот, увеличив число тем или даже отдельных модулей образовательной программы, и тем самым скорректировать оплату курса.

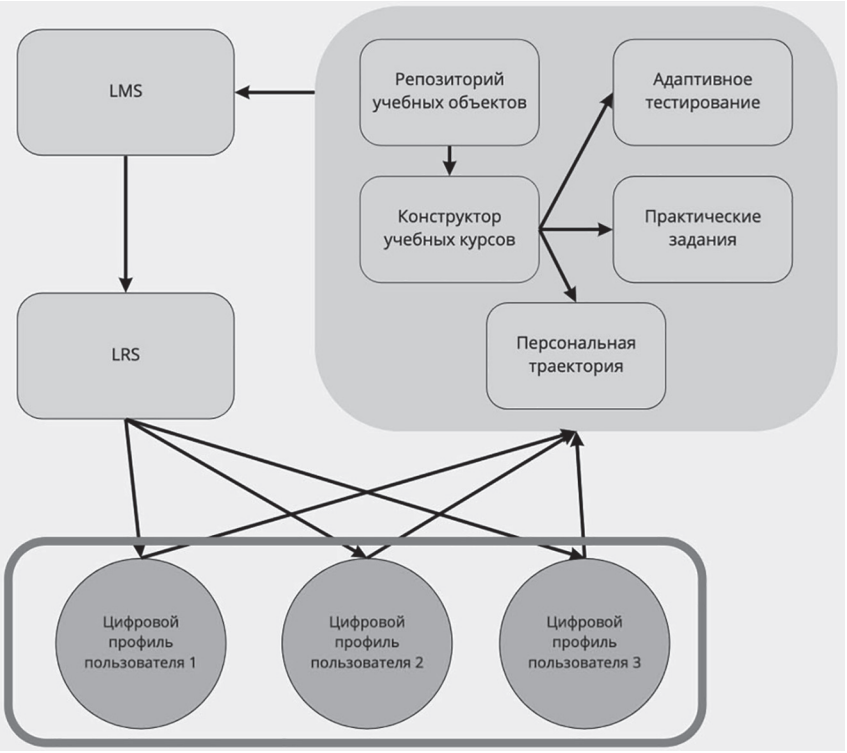

Рис. 4. Архитектура проекта «Цифровой тьютор» и взаимодействие с внешними системами

Fig. 4. Architecture of the “Digital Tutor” project and interaction with external systems

В рамках общей задачи на проектирование и разработку программного приложения – цифрового профиля компетенций – рекомендуется формулировать задачу создания децентрализованных цифровых профилей с возможностью подтверждения полученных свидетельств о прохождении онлайн-курсов или завершении обучения на различных платформах и в образовательных организациях. Для выполнения поставленной задачи необходимо спроектировать и реализовать следующие части системы:

1. Модуль проверки хранимой информации, ее раскрытия и передачи.

2. Децентрализованная система хранения криптографических ключей пользователей.

3. Протокол общения между всеми участниками: Эмитентом, Верификатором и Держателем.

При этом должны быть выполнены следующие требования:

1. Цифровой профиль компетенций должен поддерживать стандарты SCORM и xAPI.

2. Формат хранения цифровых эквивалентов дипломов, сертификатов и других подтверждающих документов должен удовлетворять критерию многовариантности.

Цифровой профиль компетенций может быть автономной частью общей архитектуры информационной системы или подсистемой, реализующей логику построения персональной траектории обучения. Разрабатывая программное приложение, необходимо учесть возможность взаимодействия цифрового профиля компетенций с другими подсистемами для передачи или получения необходимой информации.

Схема такого взаимодействия представлена на рисунке 4 и демонстрирует процесс работы цифровых профилей в рамках цифровой образовательной платформы «Цифровой тьютор», разработанной в Российском экономическом университете им. Г.В. Плеханова, для создания онлайн курсов, способных интегрироваться в среду электронного обучения организации [19].

При взаимодействии с LMS образовательной организации, обучающийся проходит авторизацию, благодаря VC подтверждается его личность и данные, переданные цифровым профилем компетенций, например, документы об обучении, история обучения. Последующие действия или результаты обучающегося в процессе прохождения онлайн-курса на платформе LMS будут аккумулированы через цифровой профиль компетенций обучающегося. В дальнейшем извлеченная из цифрового следа полезная информация может быть использована для прохождения обучения на новой программе обучения, для анализа и подбора программы обучения или образовательной организации, а также для определения ключевых компетенций и направлений их развития. Для реализации такой стратегии цифровой профиль компетенций должен не просто накапливать данные цифрового следа обучающегося, но и отвечать следующим требованиям:

- соответствие современным стандартам онлайн-образования;
- соответствие стандартам архитектуры блокчейн и модели SSI;
- удобство сопровождения;
- переносимость;
- доступность и эффективность;
- децентрализованность;
- достижение безопасности с помощью криптографических методов.

При наличии проверяемых учетных данных (VC) существует несколько методов доказательства того, что содержащиеся в них данные были выданы держателю учетных данных. К ним относятся предоставление подтверждения биометрических данных для держателя и криптографическая привязка учетных данных к держателю с использованием доказательств с нулевым разглашением (ZKP).

Доказательства с нулевым разглашением (ZKP) используются для подтверждения информации, касающейся учетных данных человека, если нет необходимости полностью раскрывать иную конфиденциальную личную информацию. Каждый сценарий, в котором нужно доказать, что человек имеет право на доступ к сервису, не раскрывая больше персональных данных, чем необходимо, является потенциальным применением для ZKP [20].

Процесс доказательства с нулевым разглашением должен обладать следующими тремя свойствами:

1. Полнота: если утверждение действительно верно, и оба человека следуют правилам, то Верификатор будет убежден без привлечения иных ресурсов Эмитента.

2. Обоснованность: в случае ложности утверждения Верификатор не будет убежден ни при каких обстоятельствах.

3. Нулевое разглашение: Верификатор в любом случае не будет знать больше той информации, которая ему предоставлена.

Свойства (1) и (2) необходимы для всех интерактивных систем проверки, таких как доказательства цифровой подписи. Свойство (3) создает доказательство с нулевым разглашением.

При использовании обычной криптографии с открытым или закрытым ключом цифровая подпись также коррелируема, как и открытый ключ. Криптографические методы с нулевым разглашением не раскрывают фактическую подпись. Вместо этого они раскрывают только криптографическое доказательство действительной подписи. Только владелец подписи имеет информацию, необходимую для представления удостоверений Верификатору. Это означает, что подписи ZKP не увеличивают риск корреляции для подписывающей стороны и автоматически защищают подписывающую сторону от выдачи себя за другое лицо.

Одним из важных преимуществ доказательства с нулевым разглашением является выборочное раскрытие [17]. Оно означает, что вам не нужно раскрывать все атрибуты, содержащиеся в учетных данных. Например, если нужно только подтвердить успешное завершение бакалавриата, то не нужно раскрывать как именно завершали обучение. Точно также Верификатору не надо собирать больше данных, чем необходимо для успешного завершения транзакции. Выборочное раскрытие информации – это не только обеспечение конфиденциальности для физических лиц. Оно также снижает ответственность Верификатора за обработку или хранение персональных данных, которые им не нужны. Криптография с нулевым разглашением позволяет Держателю учетных данных выбирать, какие атрибуты раскрывать, а какие скрывать в каждом конкретном случае – без необходимости каким-либо образом вовлекать Эмитента учетных данных.

Однако применения доказательств с нулевым разглашением не ограничиваются только выборочным раскрытием или подтверждением информации. На самом деле возможностей ZKP очень много: доказательства с несколькими учетными данными, аннулиро-

вание, конфиденциальность и личный контроль данных и т. д. Например, ZKP можно использовать для подтверждения получения научной степени или подтверждения обучения по определенной профессии для работодателя.

5. Выводы

В настоящей работе были показаны преимущества использования децентрализованного подхода к разработке цифрового профиля компетенций, а также предложены решения по формированию аппаратной и программной архитектуры разрабатываемого программного обеспечения, предназначенного для управления данными цифрового следа и формирования индивидуальной траектории обучения. Предлагаемые решения рассматриваются как методический базис для активизации роли обучающегося – владельца персональных данных – в процессах управления идентификацией, контроля персональных данных и построения траектории своего обучения.

Внедрение и масштабирование предложенных решений основаны на реализации в цифровых сетях подхода управления идентификацией, инструменты которого обеспечат децентрализованную идентификацию данных цифрового профиля компетенций. В отличие от распространенной сегодня практики централизованного управления образовательными платформами разработка и масштабирование децентрализованного приложения – цифрового профиля компетенций – не признает границ отдельных образовательных платформ и позволяет на основе сгенерированного и обработанного цифрового следа воплотить в жизнь идею персонализированного обучения.

Университеты получат реальную возможность для того, чтобы катализировать экосистему цифровых профилей компетенций, которые студенты смогут использовать во время и по завершении своей университетской карьеры. Это позволит обеспечить безопасность во взаимодействии со студентами, сотрудниками и другими организациями согласно принципам Гронингенской декларации, которая направлена на расширение возможностей учащихся на основе управления цифровыми данными.

Университеты рассматриваются в качестве ведущих эмитентов учетных данных для своих студентов, одновременно позволяя их цифровой жизни стать более безопасной, продуктивной и конфиденциальной.

Литература

1. Бандура А. Теория социального научения. СПб.: Евразия; 2000. 318 с.

2. Демин А.Н., Демина И.В. Проблема адаптации человека к скорости социальных процессов // Человеческий капитал. 2020. № 10 (142). С. 80–88. DOI: 10.25629/HC.2020.10.05.

3. Marginson S. Research on international and global higher education: Six different perspectives // Oxford Review of Education. 2022. № 48(4). С. 421–438. DOI: 10.1080/03054985.2022.2087619.

4. Fdhila W., Stifter N., Kostal K., Saglam C., Sabadello M. Methods for decentralized identities: evaluation and insights. Business process management: blockchain and robotic process automation forum. BPM 2021. Lecture Notes in Business Information Processing. 2021. DOI: 10.1007/978-3-030-85867-4_9.

5. Rek P., Podgorelec B., Turkanović M. Complexity analysis of decentralized application development using integration tools [Электрон. ресурс]. Proceedings of the SQAMIA. 2019. Режим доступа: https://ceur-ws.org/Vol-2508/paper-rek.pdf.

6. Kyun S., Yi J., Jang J. A Decentralized approach to education powered by blockchain technology // Asia-Pacific Journal of Convergent Research Interchange. FuCoS. 2021. № 7(7). С. 131–141. DOI: 10.47116/apjcri.2021.07.13.

7. Мутин Д.И., Мутина Е.И., Кравец О.Я., Сорокин С.А. Управление и инжиниринг блокчейн-технологий. Воронеж: Научная книга, 2022. 140 с.

8. Alizadeh M., Andersson K., Schelén O. Comparative analysis of decentralized identity approaches // IEEE Access. 2022. DOI: 10.1109/ACCESS.2022.3202553.

9. Shemshack A., Spector J.M. A systematic literature review of personalized learning terms // Smart Learning Environments. 2020. № 7. С. 33. DOI: 10.1186/s40561-020-00140-9.

10. Соленый, С.В., Воропаев И.А. О внедрении проверяемых учетных данных (VC) и децентрализованных идентификаторов (DID) в систему аутентификации // Завалишинские чтения 22: Сборник докладов XVII Международной конференции по электромеханике и робототехнике. (Санкт-Петербург, 12–14 апреля 2022 года). СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. С. 58–61.

11. Еськов С.С., Лебеденко Е.В., Кравец О.Я. Управление взаимным информационным согласованием в системах распределенного реестра на основе специального математического и программного обеспечения. Воронеж: Научная книга, 2021. 120 с.

12. Бахвалова Е.А., Судаков В.А. Исследование алгоритмов консенсуса для блокчейн-платформ // Препринты ИПМ им. М.В. Келдыша. 2021. № 26. С. 1–16. DOI: 10.20948/prepr-2021-26.

13. Тельнов Ю.Ф., Косоруков О.А., Тихонов С.В., Комлева Н.В. Модели и информационные технологии в экономике и образовании. М.: Российский экономический университет имени Г. В. Плеханова, 2021. 152 с.

14. Развитие отдельных высокотехнологичных направлений. Белая книга [Электрон. ресурс]. М.: Высшая школа экономики, 2022. 187 с. Режим доступа: https://issek.hse.ru/mirror/pubs/share/565446894.pdf.

15. Giannopoulou A., Wang F. Self-sovereign identity // Internet policy review. 2021. № 10 (2). DOI: 10.14763/2021.2.1550.

16. Lim S.Y., Musa O.B., Al-Rimy B.A. S., Almasri A. Trust models for blockchain-based self-sovereign identity management: a survey and research directions. In Advances in blockchain technology for cyber physical systems // Internet of things. 2022. С. 277–302. DOI: 10.1007/978-3-030-93646-4_13.

17. Wang F., Filippi P. De. Self-sovereign identity in a globalized world: credentialsbased identity systems as a driver for economic inclusion // Frontiers in blockchain. 2020. № 2(28). DOI: 10.3389/fbloc.2019.00028.

18. Queiruga-DiosA., Bullón PérezJ.J., L. Encinas H. Self-sovereign identity in university context. 31st Conference of open innovations association (FRUCT). Helsinki, Finland. 2022. С. 259–264. DOI: 10.23919/FRUCT54823.2022.9770913.

19. Комлева Н. В., Вилявин Д. А. Цифровая платформа для создания персонализированных адаптивных онлайн курсов // Открытое образование. 2020. № 24(2). С. 65–72. DOI: 10.21686/1818-4243-2020-2-65-72.

20. Blum M., Feldman P., Micali S. Non-interactive zero-knowledge and its applications. Providing sound foundations for cryptography. New York: Association for computing machinery, 2019. С. 329–349. DOI: 10.1145/3335741.3335757.

References

1. Bandura A. Teoriya sotsial'nogo naucheniya = Social learning theory. Saint Petersburg: Yevraziya; 2000. 318 p. (In Russ.)

2. Demin A.N., Demina I.V. The problem of human adaptation to the speed of social processes. Chelovecheskiy capital = Human capital. 2020; 10(142): 80–88. DOI: 10.25629/HC.2020.10.05. (In Russ.)

3. Marginson S. Research on international and global higher education: Six different perspectives. Oxford Review of Education. 2022; 48(4); 421–438. DOI: 10.1080/03054985.2022.2087619.

4. Fdhila W., Stifter N., Kostal K., Saglam C., Sabadello M. Methods for decentralized identities: evaluation and insights. Business process management: blockchain and robotic process automation forum. BPM 2021. Lecture Notes in Business Information Processing. 2021. DOI: 10.1007/978-3-030-85867-4_9.

5. Rek P., Podgorelec B., Turkanović M. Complexity analysis of decentralized application development using integration tools [Internet]. Proceedings of the SQAMIA. 2019. Available from: https://ceur-ws.org/Vol-2508/paper-rek.pdf.

6. Kyun S., Yi J., Jang J. A Decentralized approach to education powered by blockchain technology. Asia-Pacific Journal of Convergent Research Interchange. FuCoS. 2021; 7(7): 131–141. DOI: 10.47116/apjcri.2021.07.13.

7. Mutin D.I., Mutina Ye.I., Kravets O.Ya., Sorokin S.A. Upravleniye i inzhiniring blokcheyntekhnologiy = Management and engineering of blockchain technologies. Voronezh: Scientific book; 2022. 140 p. (In Russ.)

8. Alizadeh M., Andersson K., Schelén O. Comparative analysis of decentralized identity approaches. IEEE Access. 2022. DOI: 10.1109/ACCESS.2022.3202553.

9. Shemshack A., Spector J. M. A systematic literature review of personalized learning terms. Smart Learning Environments. 2020; 7: 33. DOI: 10.1186/s40561-020-00140-9.

10. Solenyy S.V., Voropayev I.A. On the implementation of verifiable credentials (VC) and decentralized identifiers (DID) in the authentication system. Zavalishinskiye chteniya 22: Sbornik dokladov XVII Mezhdunarodnoy konferentsii po elektromekhanike i robototekhnike. (Sankt-Peterburg, 12–14 aprelya 2022 goda) = Zavalishin Readings 22: Collection of reports of the XVII International Conference on Electromechanics and Robotics. (St. Petersburg, April 12–14, 2022). Saint Petersburg: St. Petersburg State University of Aerospace Instrumentation; 2022: 58–61. (In Russ.)

11. Yes'kov S.S., Lebedenko Ye.V., Kravets O.Ya. Upravleniye vzaimnym informatsionnym soglasovaniyem v sistemakh raspredelennogo reyestra na osnove spetsial'nogo matematicheskogo i programmnogo obespecheniya = Management of mutual information coordination in distributed registry systems based on special mathematical and software. Voronezh: Scientific book; 2021. 120 p. (In Russ.)

12. Bakhvalova Ye.A., Sudakov V.A. Study of consensus algorithms for blockchain platforms. Preprinty IPM im. M.V. Keldysha = Preprints of the Institute for Problems of Mathematics. M.V. Keldysh. 2021; 26: 1–16. DOI: 10.20948/prepr-2021-26. (In Russ.)

13. Tel'nov Yu.F., Kosorukov O.A., Tikhonov S.V., Komleva N.V. Modeli i informatsionnyye tekhnologii v ekonomike i obrazovanii = Models and information technologies in economics and education. Moscow: Russian Economic University named after G.V. Plekhanov; 2021. 152 p. (In Russ.)

14. Razvitiye otdel'nykh vysokotekhnologichnykh napravleniy. Belaya kniga = Development of

individual high-tech areas. White paper [Internet]. Moscow: Higher School of Economics; 2022. 187 p. Available from: https://issek.hse.ru/mirror/pubs/share/565446894.pdf. (In Russ.)

15. Giannopoulou A., Wang F. Self-sovereign identity. Internet policy review. 2021; 10(2). DOI: 10.14763/2021.2.1550.

16. Lim S.Y., Musa O.B., Al-Rimy B.A.S., Almasri A. Trust models for blockchain-based self-sovereign identity management: a survey and research directions. In Advances in blockchain technology for cyber physical systems. Internet of things. 2022: 277–302. DOI: 10.1007/978-3-030-93646-4_13.

17. Wang F., Filippi P. De. Self-sovereign identity in a globalized world: credentialsbased identity systems as a driver for economic inclusion. Frontiers in blockchain. 2020: 2(28). DOI: 10.3389/fbloc.2019.00028.

18. Queiruga-Dios A., Bullón Pérez J. J., L. Encinas H. Self-sovereign identity in university context. 31st Conference of open innovations association (FRUCT). Helsinki, Finland. 2022: 259–264. DOI: 10.23919/FRUCT54823.2022.9770913.

19. Komleva N. V., Vilyavin D. A. Digital platform for creating personalized adaptive online courses. Otkrytoye obrazovaniye = Open Education. 2020; 24(2): 65–72. DOI: 10.21686/1818-4243-2020-2-65-72. (In Russ.)

20. Blum M., Feldman P., Micali S. Non-interactive zero-knowledge and its applications. Providing sound foundations for cryptography. New York: Association for computing machinery; 2019: 329–349. DOI: 10.1145/3335741.3335757.

Сведения об авторах

Даниил Андреевич Вилявин
Team Lead Backend, ООО Сколопендра,
Москва, Россия
Эл. почта: dviliavin@skolopendra.com

Нина Викторовна Комлева
К.э.н., доцент, доцент Базовой кафедры цифровой экономики
Российский экономический университет им. Г.В. Плеханова,
Москва, Россия
Эл. почта: komleva.nv@rea.ru

Наталья Александровна Мамедова
К.э.н., доцент, ведущий научный сотрудник Базовой кафедры цифровой экономики
Российский экономический университет им. Г.В. Плеханова,
Москва, Россия
Эл. почта: mamedova.na@rea.ru

Аркадий Ильич Уринцов
Д.э.н., профессор, заведующий Базовой кафедры цифровой экономики
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: urintsov.ai@rea.ru

Information about the authors

Daniil A. Vilyavin
Team Lead Backend, Skolopendra LLC,
Moscow, Russia
E-mail: dviliavin@skolopendra.com

Nina V. Komleva
Cand. Sci. (Economics), Associate professor, Associate professor of the Basic Department of Digital Economics
Plekhanov Russian University of Economics,
Moscow, Russia
E-mail: komleva.nv@rea.ru

Natalia A. Mamedova
Cand. Sci. (Economics), Associate professor Leading Researcher of the Basic Department of Digital Economics,
Plekhanov Russian University of Economics,
Moscow, Russia
E-mail: mamedova.na@rea.ru

Arkady I. Urintsov
Dr. Sci. (Economics), Professor, Head of the Basic Department of Digital Economics,
Plekhanov Russian University of Economics,
Moscow, Russia
E-mail: urintsov.ai@rea.ru