Цифровизация в образовании

УДК 378.44 + 004.056 **DOI: 10.14529/ped200106**

РАЗВИТИЕ ЦИФРОВЫХ КОМПЕТЕНЦИЙ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ВУЗЕ

Л.В. Астахова, И.А. Сафонова

Южно-Уральский государственный университет, г. Челябинск, Россия

В условиях динамики цифровой трансформации высшее образование призвано развивать как универсальные, так и профессиональные цифровые компетенции студентов. Особенно это касается специалистов по защите информации, подготовка которых обладает ярко выраженными специфическими особенностями, чем и обусловлена актуальность настоящей статьи. Этим обусловлена ее цель – обосновать возможности развития цифровых компетенций будущих специалистов по защите информации в вузе в контексте парадигмы «Образование 4.0» и национальной программы развития цифровой экономики России. В процессе исследования использованы аналитико-синтетические методы. Теоретическая значимость исследования заключена в уточнении понятия цифровых компетенций в эпоху Образования 4.0, тенденций и возможных последствий их развития в российской и зарубежной практике. Научная новизна работы состоит в выявлении особенностей и проблем развития цифровых компетенций специалистов по защите информации, в обосновании перспективных возможностей преодоления этих проблем в процессе профессиональной подготовки будущих специалистов по защите информации в условиях вуза. Показана результативность новых подходов к организации обучения цифровым навыкам студентов в процессе обучения управлению рисками информационной безопасности, что подчеркивает практическую значимость исследования.

Ключевые слова: цифровые компетенции, цифровые технологии, специалист по защите информации, высшее образование, перевернутое обучение, социальное обучение.

Введение

Эволюция образования от Образования 1.0 к Образованию 4.0 соответствует развитию информационных технологий и производства. Образование 1.0 сравнивают с Web 1.0, где распространение информации происходит односторонне – от учителя к ученику. Это тип образования, основанного на 3 действиях: слушать учителя; отвечать на вопросы, изучая текст и делая рабочие записи; получать оценки. Образование 2.0, как и Web 2.0, основано на организации интерактивного взаимодействия между контентом и пользователем, а также между самими пользователями. Оно фиксируется на общении, содействии и сотрудничестве. В Образовании 3.0 этот набор другой: обучающиеся – это соединители, создатели, конструктивисты. Они самоопределяются в обучении, а не учатся у преподавателя. Образование 3.0 характеризуется образовательными возможностями, где сами обучающиеся играют ключевую роль в качестве создателей артефактов знания, которые становятся общими [37].

Развитие цифровых информационных технологий и нацеленность на Индустрию 4.0 естественным образом способствовали появлению современной парадигмы Образования 4.0. В настоящее время происходит усиление акцента на персонализацию обучения на основе широкого применения электронных учебников, обучающих программ, искусственных когнитивных обучающих систем. В ближайшее время могут быть востребованы технологии гибридного обучения (совместного обучения людей и интеллектуальных машин). Конвергенция искусственного интеллекта, больших данных и технологий платформ показывает, что большинство необходимых навыков в высшем образовании, которые еще предстоит развивать, – это потребность в большей активности и гибкости [40], интеграция навыков управления знаниями: этика использования информации, управление проектами, командная работа, независимое мышление и способность учиться [33], а также способность к созданию нового знания.

Названные особенности Образования 4.0 требуют анализа возможностей развития новых компетенций выпускников вузов в новых условиях. Сложность ситуации заключается в том, что в условиях динамики цифровой трансформации высшее образование должно одновременно развивать и универсальные цифровые компетенции студентов, и их профессиональные цифровые инновационные компетенции, остро требуемые всеми отраслями грядущей цифровой экономики. Особенно это касается специалистов по защите информации, подготовка которых и без того обладает ярко выраженными специфическими особенностями, чем и обусловлена актуальность настоящей статьи.

Развитие цифровых компетенций за рубежом

Образование 4.0 широко обсуждается за рубежом, где давно поняли, что после преодоления цифрового разрыва в доступности к цифровым средствам обработки и хранения информации новый цифровой разрыв связан неравенством между теми, кто способен творчески использовать цифровые технологии для выполнения нестандартных работ, таких как исследования, наблюдения, конструирования, и тех, кто способен использовать ЦТ только для рутинных операций [12].

Осознавая потребность адаптации образования к быстроизменяющимся внешним условиям, Европейский союз активно занимается цифровизацией образования и его трансформацией. Центр совместных исследований (Joint Research Centre (JRC)) Европейской комиссии начал исследования по обучению и навыкам для цифровой эры еще в 2005 году. Их целью было предоставить государствам – членам ЕС поддержку в использовании потенциала цифровых технологий для внедрения инноваций в области образования и обучения, улучшения доступа к обучению на протяжении всей жизни и развитии новых (цифровых) навыков и компетенций, необходимых для трудоустройства, развития личности и социальной интеграции. Европейская система цифровых компетенций для граждан, известная как DigComp, предлагает инструмент для повышения цифровой компетенции граждан. Впервые она была опубликована в 2013 году, а в 2016 году JRC опубликовал DigComp 2.0, где была обновлена терминология и концептуальная модель, а также продемонстрированы примеры ее реализации на европейском, национальном и региональном уровнях. Начальные три уровня квалификации были расширены до восьми уровней.

DigComp 2.0 включает 5 областей цифровых компетенций:

1. Информационная грамотность (просмотр, поиск и фильтрация данных, информации и цифрового контента; оценка данных, информации и цифрового контента; управление данными, информацией и цифровым контентом).

2. Общение и сотрудничество (взаимодействие с помощью цифровых технологий; совместное использование цифровых технологий; вовлечение в гражданство через цифровые технологии; сотрудничество с помощью цифровых технологий; сетевой этикет; управление цифровой идентификацией).

3. Создание цифрового контента (разработка цифрового контента; интеграция и переработка цифрового контента; авторские права и лицензии; программирование).

4. Безопасность (защита устройств; защита личных данных и конфиденциальности; защита здоровья и благополучия; защита окружающей среды).

5. Решение проблем (решение технических проблем; определение потребностей и технологических ответов; творческое использование цифровых технологий; выявление пробелов цифровой компетенции).

Для каждой из компетенций обоснованы 8 уровней квалификации, а также соответствующие им знания и умения: 1 и 2 – базовые уровни (решение простых задач с инструкциями с ориентацией на запоминание); 3 и 4 – промежуточные уровни (решение определенных и рутинных задач и простых (далее – нестандартных) проблем с ориентацией на понимание); 5 и 6 – продвинутые уровни (решение разных задач и проблем с ориентацией на применение знаний и умений в практике); 7 и 8 – глубокоспециализированные уровни (решение сложных проблем с помощью ограниченных (далее – множества) вариантов решений, способность внести свой вклад в профессиональную практику и направлять других, предлагать новые идеи и процессы на местах) [31].

В 2017 году государства – члены ЕС подчеркнули свою приверженность обеспечению обучающихся «лучшим образованием». Европейский совет призвал к тому, чтобы системы европейского образования и обучения были

«пригодны для цифрового века» [35]. В специальном документе [32] было изложено видение европейского образовательного пространства и объявлен специальный План действий в области цифрового образования. Этот План действий демонстрирует, как системы образования и обучения могут более эффективно использовать инновации и цифровые технологии и поддерживать развитие соответствующих цифровых компетенций, необходимых для жизни и работы в эпоху информационных технологий. Он сфокусирован на необходимости стимулировать, поддерживать и расширять целевое использование цифровых и инновационных методов обучения; на вовлечении в образовательный процесс широкого круга потенциальных работодателей. В основу Плана положены: более эффективное использование цифровых технологий для преподавания и обучения; развитие соответствующих цифровых компетенций и навыков для цифровой трансформации; улучшение образования за счет лучшего анализа данных и прогнозирования. Цифровая трансформация в Европе базируется на применении в образовательном процессе новых технологий, таких как искусственный интеллект, робототехника, облачные вычисления, блокчейн и др. [21].

Принятый план активно реализуется. Так, консорциумом европейских университетов из нескольких стран была создана инновационная образовательная платформа TIPHYS. Цели проекта TIPHYS состоят в том, чтобы создать открытую сетевую платформу для изучения тем Industry 4.0 студентами университетов путем использования современных стратегий обучения: образования в социальных сетях (SNE) и конструктивного выравнивания (CA). Они ориентированы на командную работу, построение сетей взаимодействия между студентами и преподавателями различных университетов. В рамках проекта планируется создать платформу виртуальной реальности (VR), где пользователи смогут проектировать и создавать виртуальную среду для обучения и моделирования промышленных процессов [27]. Федеральное министерство образования и науки Германии (BMBF) инициировало серию исследовательских проектов, связанных с образованием, одним из которых является совместный проект ELLI – «Отличное преподавание и обучение в инженерных науках». В нем участвуют 3 университета: Aachen University, Ruhr-Universität Bochum и TU Dortmund University. В рамках проекта разрабатываются удаленные и виртуальные лаборатории для обучения машиностроению с акцентом на технологии производства. Для их использования был создан Massive-Open-Online-Course (MOOC), который включает в себя удаленные лаборатории как часть применяемых дидактических методов. Это позволяет студентам визуально исследовать сложные процессы и экспериментировать с ними. Все эти меры в настоящее время используются на лекциях в различных учебных программах, идет работа по включению новых процессов и внедрению технологий дополненной реальности и аддитивного производства [38]. В Неапольском университете имени Федерико II образовательная деятельность по курсу «Измерительные приборы и измерения для интеллектуальной промышленности» основана на модели «обучающих фабрик» (Teaching Factory), ориентированных на инновационные процессы, и малых предприятий четвертой промышленной революции, использующих технологии Интернета вещей (IoT) и технологии аддитивного производства [26]. Парадигма Teaching Factory представляет собой недостающее звено, которое нацелено на преодоление разрыва между наукой, образованием и промышленностью. Она применяется также в учебных курсах «Компьютерное проектирование / планирование автоматизированных процессов» и «Автоматизированное производство», что обеспечивает успешное обучение студентов новым функциям и опыту работы в условиях Industry 4.0, а также сохранение актуальных учебных программ [25]. Накопленный опыт уже показывает, что использование парадигмы Teaching Factory приводит к изменению производственного образования, удовлетворяя возросшую потребность в высококвалифицированных кадрах [42].

Инновационный опыт развития цифровых компетенций накоплен и в других регионах мира. Одним из примеров новой модели университета и образования эксперты называют модель Singularity University (SU), в которой академические практики опираются на концептуальные и эмпирические эффекты цифрового преобразования, которые могут быть развернуты в компаниях и фирмах. Появляются новые платформенные технологии в образовательном пространстве (ImpactEd), которые позволяют учитывать сложные образова-

тельные потребности завтрашнего дня посредством интегрированного обучения на основе сетевых проектов [41].

Развитие цифровых компетенций в России

В России изучение проблем цифровых технологий в контексте Образования 4.0 актуализировалось после принятия национальной программы «Цифровая экономика Российской Федерации» в 2018 году [18], в которой уделено особое внимание компетенциям цифровой экономики и цифровой грамотности. Согласно Федеральному проекту «Кадры для цифровой экономики» (Раздел «Обеспечение цифровой экономики компетентными кадрами») уже в 2019 году будет разработана концепция базовой модели компетенций цифровой экономики, перечень ключевых компетенций и механизм их актуализации (п. 1.2).

Цифровые навыки, охватывающие технические знания в области ИКТ, в тесной связи с мягкими навыками и общими знаниями лежат в основе «Целевой модели компетенций 2025», подготовленной консалтинговой группой The Boston Consulting Group (BCG) на базе консенсус-мнения экспертов и анализа подходов Библиотеки компетенций Lominger, Сбербанка, RosExpert / Korn Ferry, НИУ ВШЭ, WorldSkills Russia и Global Education Futures [17], а также Working Group on Education (2017) [30].

Понятие цифровых компетенций не является строго научным понятием. Зачастую понятия технологии, грамотность, культура и компетенции (с определениями «информационная» или «цифровая») рассматриваются как синонимы. Наряду с этим наблюдается трансформация взглядов на дифференциацию и развитие профессиональных компетенций личности, связанных с существованием в информационном, цифровом и SMART-обществе. На основе анализа публикаций последних лет эксперты определяют: информационную компетенцию – как интегральную характеристику, связанную с опытом деятельности в информационной действительности, способами взаимодействия с техникой и технологиями с целью реализации общих и профессиональных информационных потребностей личности; цифровую компетенцию – как высокоуровневые метаспособности для существования в цифровом пространстве высокомобильных интеллектуальных устройств; SMART-компетенцию – как сформированность личности SMART-человека, которая в совершенстве владеет SMART-технологиями для поиска, анализа информации и создания инноваций, взаимодействует в профессиональных сетевых сообществах [22]. В Университете ИТМО для обозначения цифровых компетенций использовали термин «цифровая культура». Одноименная дисциплина включена в учебные планы всех образовательных направлений. Цифровую культуру определили как совокупности компетенций, характеризующих способность использования информационно-коммуникационных технологий для комфортной жизни в цифровой среде, для взаимодействия с обществом и решения цифровых задач в профессиональной деятельности, включая информационную безопасность и соблюдение цифровой этики [10].

Определенный опыт построения инновационных моделей обучения цифровым навыкам в России накопили также в компаниях Google, IBM, «Яндекс» и в таких известных своим новаторством образовательных институциях, как École 42/Школе 21, Национальном исследовательском университете «Высшая школа экономики» (НИУ ВШЭ) и Корпоративном университете Сбербанка. В качестве новых подходов к организации обучения стали использоваться: непрерывное обучение, обучение через опыт, адаптивное обучение, социальное обучение, перевернутое обучение, микрообучение, геймификация, искусственный интеллект и применение интеллектуальных помощников, виртуальная и дополненная реальность VR/AR. Используются и новые обучающие решения: новые форматы очного обучения, массовые открытые онлайн-курсы, адаптивные электронные курсы, VR/AR-симуляции, интерактивные дистанционные занятия (life virtual) [17]. Для интеллектуализация информационных систем образовательного назначения активно разрабатываются прототипы интеллектуальных систем обучения и контроля знаний [24], обосновывается актуальность внедрения современных средств обучения – роботов и робототехнических комплексов как цифровых помощников, приводится анализ имеющихся разработок по созданию роботов для образовательной сферы [23] и др.

Результаты исследований готовности российского высшего образования к цифровой экономике свидетельствуют о том, что создан необходимый задел по созданию ИТ-инфраструктуры, нормативно-правовому обеспече-

нию, лучших практик в области применения ИТ в учебном процессе. С одной стороны, высок уровень обеспечения вузов персональными компьютерами и доступом к Интернету, но с другой – недостаточно автоматизирован учебный процесс. Несмотря на постоянное развитие технологий и появление новых образовательных веб-сервисов, а также многолетнюю государственную политику по формированию информационного образовательного пространства, его потенциал вузами задействован частично. Только треть студентов вузов обучаются с использованием электронного обучения или дистанционных образовательных технологий [9]. По мнению ученых, информационные системы, функционирующие на базе цифровых технологий, в настоящее время не в полной мере реализуют интеллектуализацию процесса обучения, под которой понимается «обеспечение информационного интерактивного взаимодействия между субъектами процесса обучения многовариантным причинно-следственным анализом данных (информации) обо всех аспектах данного процесса с последующей обработкой, визуализацией, получением и сохранением результатов для их предоставления и совместного использования всеми заинтересованными пользователями» [19]. Идентичные проблемы наблюдаются и в области вузовской подготовки специалистов по защите информации.

Понятие цифровых компетенций специалиста по защите информации

Особенность специалиста по информационной безопасности заключается в том, что его деятельность обладает: информационно-управленческой природой; самоорганизующимся характером (он работает с объектами, которые сам создает); гуманитарно-технической сущностью; углубляющейся интеграцией с обеспечением других видов безопасности (пожарной, экономической, кадровой, информационно-психологической, социальной), а следовательно – многопредметностью и полифункциональностью [1, 6, 7].

Учитывая, что необходимость защиты информации существует во всех организациях, независимо от их масштаба, формы собственности и отраслевой принадлежности, выпускники образовательных направлений должны иметь управленческие компетенции. За рубежом трудовая функция обеспечения информационной безопасности закреплена за CISO (англ. Chief Information Security Officer) – директором по информационной безопасности. При этом сегодня CISO – это, как правило, субъект решения всех видов технических проблем, о которых никто не хочет беспокоиться [29]. Неслучайно в зарубежной науке об информационной безопасности с конца XX века распространена и активно развивается концепция ролей [36]. CISO выступает в роли стратега (адаптация стратегии безопасности к требованиям бизнеса, инициирование инновационных преобразований с целью эффективного управления рисками и инвестициями в безопасность); советника (взаимодействие с бизнесом с целью обучения, консультирования и оказания влияния на реализацию бизнес-проектов в контексте имеющихся рисков); защитника (защита активов бизнеса за счет понимания текущего профиля угроз и управления эффективностью текущей программы для безопасности); техника (оценка и внедрение новых технологий и стандартов с целью обеспечения необходимого уровня безопасности). Согласно исследованию Deloitte, CISO сегодня тратят 77 % своего времени в качестве «техников» и «защитников», т. е. на технические аспекты деятельности, и что они хотели бы сократить это время до 35 %. Это демонстрирует заметный сдвиг в их стремлении уделять больше внимания функциям «стратег» и «советник» [34]. Они обладают не только профильными знаниями по безопасности, но и понимают информационные технологии, экономику, финансы, управление персоналом и многие другие важнейшие дисциплины [15].

В России все эти функции также должен выполнять руководитель отдела информационной безопасности (IT-безопасности), директор отдела по IT-безопасности. Если в организации не имеется этой штатной единицы, все функции – и управленческие (стратег, советник), и операционные (защитник, техник) – выполняет рядовой специалист по защите информации.

Сегодня требования к специалистам в области защиты информации особенно высоки, поскольку нужны кадры нового поколения, способные быстро адаптироваться к постоянно изменяющимся угрозам информационной безопасности, обладающие высоким уровнем цифровых компетенций как частью профессиональной компетентности.

Зарубежные исследования показывают, что лидеры кибербезопасности нуждаются

в уникальном наборе атрибутов, включая способность мыслить нестандартно, глубоко вникать в вопросы, осуществлять суждения на уровне совета директоров и быть надежным деловым партнером. Они относят к числу его необходимых компетенций: стратегическое, глобальное мышление, аналитическую компетенцию, знание бизнес-процессов и движения информации в организации, способность к коммуникациям и влиянию на высшее руководство, способность обеспечить баланс конкурирующих приоритетов, способность развивать и реализовать свои таланты и др. [39]. К числу необходимых навыков XXI века относят также склонность молодых людей к многозадачности с использованием цифровых технологий [43].

Для развития названных компетенций в российских вузах предпринимаются некоторые шаги. Так, выполнение совместных проектов с другими вузами и применение сетевых технологий обучения называются в качестве педагогических условий подготовки специалистов в области ИБ [8]. Разрабатываются новые средства обучения: электронные учебные пособия, автоматизированные тренажеры и обучающие системы, средства и комплексы технической защиты информации, программные средства авторской разработки, использование которых дает возможность решить проблему малой обеспеченности реальными средствами и комплексами технической защиты информации и средствами обучения или полного их отсутствия [13, 20] и др. Однако, несмотря на определенный опыт изучения и развития цифровых компетенций будущего специалиста по защите информации, понятие и структура этих компетенций не определены, практика их развития фрагментарна.

Опираясь на европейский подход к содержанию цифровых компетенций и авторские публикации по вопросам информационной компетенции [3–5], культуры информационной безопасности [2, 16, 28], определим цифровую компетентность будущего специалиста по защите информации как его *способности к информационному взаимодействию в цифровом пространстве высокомобильных интеллектуальных устройств, умных технологий и сетевых профессиональных сообществ с целями обеспечения конфиденциальности, целостности и доступности информации в организации, а также самореализации и непрерывного инновационного полифункционального развития.* Исходя из этого определения, спектр цифровых компетенций – составляющих цифровой компетентности будущего специалиста по защите информации – должен включать следующие способности:

1) *к потреблению* цифрового контента: его поиску, отбору, пониманию, оцениванию, интерпретированию, хранению, защите;

2) *к репродуктивной деятельности* в цифровой среде: взаимодействию и сотрудничеству, взаимообмену цифровым контентом на основе норм сетевого этикета;

3) *к продуктивной деятельности* в цифровой среде: созданию, интеграции и творческой переработке цифрового контента, в том числе с использованием технологий программирования и машинного обучения, защиты авторских прав;

4) *к рефлексивной деятельности* в цифровой среде: выявлению информационных и цифровых потребностей и пробелов цифровой компетенции для реализации различных видов деятельности в этой среде (потребительской, репродуктивной и продуктивной).

Кроме многоцелевой и полифункциональной специфики деятельности специалиста по защите информации в основу структуры цифровых компетенций мы положили также видовую структуру информационной деятельности (информационно-потребительская, информационно-репродуктивная, информационно-созидательная (продуктивная)), обоснованную на базе принципа единства сознания и деятельности А.Н. Леонтьева [14]; концепцию взаимодействия сознания и информационной деятельности в процессе духовного развития личности [11]. Именно этот информационно-психологический методологический подход наиболее эвристичен сегодня, когда «в условиях экспоненциального роста знаний, лавинных потоков информации практическим измерителем духовного развития личности уже не может быть степень энциклопедизма. Им может быть только степень вовлеченности индивида в различные виды информационной деятельности» [11, с. 23].

Цифровые навыки, лежащие в основе цифровых компетенций, принято условно делить на пользовательские (общие) и профессиональные (специальные). Так, к пользовательским навыкам относят: базовые цифровые навыки, которые связаны с функциональной грамотностью в использовании электронных

устройств и приложений и необходимы для получения доступа и использования цифровых устройств и сервисов (умение работать с различными техническими устройствами, файлами, Интернетом, цифровыми сервисами (социальными сетями, мессенджерами, информационными порталами), способность создавать цифровой контент и в целом умение работать с информацией – собирать, структурировать, проверять на достоверность, хранить и защищать данные приложениями); специализированные профессиональные цифровые навыки, связанные с регулярным решением сложных профессиональных задач в цифровой среде [44].

Возможности развития цифровых компетенций будущих специалистов по защите информации в вузе

Цифровые компетенции в обоснованной выше интерпретации стали объектом развития в рамках подготовки специалистов в области информационной безопасности (специальность 10.05.03 «Информационная безопасность автоматизированных систем») на кафедре защиты информации Южно-Уральского государственного университета. Для этого мы использовали дисциплину «Управление информационной безопасностью» (8-й семестр, 144 часа). Информационно-психологический подход к развитию цифровых компетенций был апробирован на примере управления рисками информационной безопасности.

Для развития цифровых компетенций студентов и реализации всех видов информационной деятельности в цифровой среде (потребительской, репродуктивной, продуктивной и рефлексивной) в качестве новых подходов к организации обучения мы использовали перевернутое и социальное обучение.

Перевернутое обучение (flipped learning) – технология обучения, при которой прямая передача знаний из группового образовательного пространства переносится в индивидуальное образовательное пространство, а групповое пространство обучения трансформировано в динамическое, интерактивное окружение, в котором преподаватель принимает роль консультанта и помогает обучающимся применить изученную теорию на практике, выработать навыки для дальнейшего самостоятельного обучения и развития.

Для реализации этого подхода мы разработали модульную сетевую платформу на базе «Электронного ЮУрГУ». В течение семестра студенты поэтапно выполняют задание «Проект системы управления рисками информационной безопасности на предприятии N». Каждый из этапов задания осуществляется в рамках конкретного модуля.

Первый модуль – для развития потребительских цифровых компетенций. Студентам предоставляется общая теоретическая информация по проблемам управления рисками информационной безопасности в виде презентаций и видеороликов, которую они должны освоить в индивидуальном порядке. Затем студент получает задание по подготовке *библиографического списка и информационно-аналитического обзора* литературы по предложенной преподавателем теме и ему предлагается список российских и зарубежных полнотекстовых и библиографических цифровых ресурсов вузовской научной библиотеки (e-library, ЭБС Лань, Science Direct, Scopus, Web of Sciense и др.). Библиографический список создается студентом по шаблону, который императивно содержит все виды цифровой информации (правовую, научную, техническую, коммерческую, популярную) и оформляется с помощью библиографических менеджеров. В методические указания по выполнению задания встраиваются обучающие видеокурсы по работе с этими цифровыми ресурсами.

Второй модуль – для развития репродуктивных цифровых компетенций: их способностей к взаимодействию и сотрудничеству с членами студенческой группы, преподавателем и работодателями-экспертами, взаимообмену цифровым контентом об управлении рисками информационной безопасности на основе норм сетевого этикета. Студенты для развития этих компетенций делятся на команды по 3 человека, и далее взаимообмен найденным на первом этапе цифровым контентом об управлении рисками информационной безопасности происходит посредством группового общения. На этом этапе используются также элементы социального обучения (social learning) для обязательного взаимодействия студентов с экспертами – сотрудниками и руководителями предприятий (организаций). Роль ведущего инструмента играет социальная сеть, реализующая функционал микроблоггинга, обмена знаниями и интерактивных уведомлений.

Третий модуль – для развития созидательных (продуктивных) цифровых компе-

тенций: их способностей к созданию, интеграции и творческой переработке цифрового контента, в том числе с использованием технологий программирования и машинного обучения, защиты авторских прав. Команды самостоятельно выбирают предприятие (организацию) и самостоятельно моделируют угрозы и систему управления рисками информационной безопасности на выбранном предприятии, обосновывая ее особенностями решения обсужденных на втором этапе проблем, а также спецификой этого предприятия. Для оценки рисков студентам предлагается программный продукт Microsoft Security Assessment Tool (MSAT). В качестве итогового документа студенты представляют *информационно-аналитический отчет* для руководителя предприятия (организации) «Проект системы управления рисками информационной безопасности на предприятии N». Подготовленный отчет команда в полном составе представляет на сетевой платформе и на аудиторных занятиях. Для оценивания проделанной работы каждому члену команды задаются вопросы, а после коллективного обсуждения силами всех групп выставляется оценка. Преподаватель также оценивает выполнение командой законодательных норм авторского права в сети с помощью программы Антиплагиат.

Четвертый модуль – для развития рефлексивных цифровых компетенций: их способностей к выявлению информационных и цифровых потребностей и пробелов цифровой компетенции для реализации различных видов деятельности в этой среде (потребительской, репродуктивной и продуктивной). Это очень важный модуль, поскольку специалист по защите информации, согласно его функциям и нормативным документам, должен повышать осведомленность сотрудников организации о кибербезопасности. В процессе работы каждый студент индивидуально выявляет пробелы в своих цифровых умениях (в том числе по информационной безопасности), в осведомленности сотрудников предприятия об информационной безопасности и разрабатывает инновационные цифровые инструменты их развития (видеоролик, презентация с элементами мультимедиа и др.). Конкурсная оценка этих инструментов также осуществляется всеми участниками платформы. Для выявления пробелов в знаниях студентов по дисциплине проводится тестирование на базе «Электронного ЮУрГУ». Этот модуль можно объединить с третьим, так как по своей сути он является продуктивным. Однако целесообразнее выделять его как самостоятельный, поскольку он отражает специфику профессиональной деятельности специалиста по защите информации.

Благодаря «Электронному ЮУрГУ» также был автоматизирован контроль учебного процесса (контроль посещения занятий, контроль выполнения заданий обучающимися и их оценивание), общение студентов внутри команд и с преподавателем.

Заключение

Проблема разработки и использования цифровых технологий в высшем образовании весьма актуальна в условиях парадигмы «Образование 4.0» и национальной программы развития цифровой экономики России. В настоящей статье уточнено понятие цифровых компетенций в эпоху Образования 4.0, тенденции и возможные последствия их развития в российской и зарубежной практике. Выявлены особенности и проблемы развития цифровых компетенций специалистов по защите информации, показаны перспективные возможности преодоления этих проблем в процессе профессиональной подготовки будущих специалистов по защите информации в условиях вуза. Анализ разработки и внедрения в учебный процесс новых подходов к организации изучения материалов по управлению рисками информационной безопасности показал высокую результативность в усвоении дисциплины, повышение уровня общих и профессиональных цифровых компетенций будущих специалистов по защите информации.

Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г., соглашение № 02. A03.21.0011).

Литература

1. Астахова, Л.В. Информационная безопасность: герменевтический подход / Л.В. Астахова. – М.: РАН, 2010. – 185 с.

2. Астахова, Л.В. От культуры – к культурному капиталу информационной безопасности организации / Л.В. Астахова // Вестник культуры и искусств. – 2018. – № 3 (55). – С. 85–101.

3. Астахова, Л.В. От медиаинформационной грамотности – к коммуникативно-когнитивно-управленческой культурной компетенции: императивы общества знания /

Л.В. Астахова // Медиаобразование. – 2017. – № 2. – С. 14–25.

4. Астахова, Л.В. Понятие информационной компетенции специалиста: когнитивный подход / Л.В. Астахова // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». – 2013. – Т. 5. – № 4. – С. 10–16.

5. Астахова, Л.В. Развитие информационно-аналитических компетенций студентов в вузе / Л.В. Астахова, А.Е. Трофименко // Вестник Челяб. гос. пед. ун-та. – 2011. – № 12. – С. 16–23.

6. Астахова, Л.В. Развитие управленческой компетенции будущего специалиста по защите информации в вузе / Л.В. Астахова // Современные проблемы науки и образования. – 2012. – № 6. – С. 330.

7. Астахова, Л.В. Управленческая компетенция специалиста по защите информации / Л.В. Астахова. – Челябинск: Издат. центр ЮУрГУ, 2014. – 99 с.

8. Бурькова, Е.В. Профессиональная подготовка специалистов в области информационной безопасности / Е.В. Бурькова // Вестник Оренбург. гос. ун-та. – 2016. – № 2 (190). – С. 3–9.

9. Днепровская, Н.В. Оценка готовности российского высшего образования к цифровой экономике / Н.В. Днепровская // Статистика и экономика. – 2018. – № 4. – С. 16–28.

10. Егорова, О.Б. Развитие цифровой культуры в вузах (на примере университета информационных технологий, механики и оптики) / О.Б. Егорова // Современное пед. образование. – 2019. – № 4. – С. 187–192.

11. Зубов, Ю.С. Библиография и художественное развитие личности / Ю.С. Зубов. – М.: Книга, 1979. – 144 с.

12. Козлова, Н.Ш. Цифровые технологии в образовании / Н.Ш. Козлова // Вестник Майкоп. гос. технол. ун-та. – 2019. – № 1. – С. 85–93.

13. Комарова, Э.П. Проектирование автоматизированных обучающих систем как средство формирования профессиональной компетентности специалистов по технической защите информации / Э.П. Комарова, М.Д. Стадников // Экономические и гуманитарные исследования регионов. – 2016. – № 6. – С. 56–64.

14. Леонтьев, А.Н. Проблемы развития психики / А.Н. Леонтьев. – М.: Изд-во МГУ, 1972. – 575 с.

15. Лукацкий, А.В. Кто такие CISO и есть ли они в России? / А.В. Лукацкий // Защита информации. Инсайд. – 2007. – № 3. – С. 18–20.

16. Лушникова, С.С. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований / С.С. Лушникова, Л.В. Астахова // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 1 (31). – С. 37–47.

17. Обучение цифровым навыкам: глобальные вызовы и передовые практики. Аналитический отчет к III Международной конференции «Больше чем обучение: как развивать цифровые навыки» // Корпоратив. ун-т Сбербанка. – М.: АНО ДПО «Корпоративный университет Сбербанка», 2018. – 122 с.

18. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. Президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. № 16). – https://base.garant.ru/72190282/ (дата обращения: 24.12.2019).

19. Роберт, И.В. Развитие информатизации образования на основе цифровых технологий: интеллектуализация процесса обучения, возможные негативные последствия / И.В. Роберт // Наука о человеке: гуманитарные исследования. – 2017. – № 4 (30). – С. 65–71.

20. Стадников, М.Д. Модель формирования профессионально-коммуникативной компетентности специалистов по технической защите информации с применением интегрированной информационной среды / М.Д. Стадников // Мир образования – образование в мире. – 2015. – № 4 (60). – С. 259–272.

21. Сулимов, А.В. Цифровые технологии в образовании: опыт европейского союза / А.В. Сулимов, А.В. Орлов // Инновационные технологии в образовательной деятельности: материалы Всерос. науч.-метод. конф. – 2019. – С. 136–138.

22. Табачук, Н.П. Информационная, цифровая и smart-компетенции личности: трансформация взглядов / Н.П. Табачук // Науч.-пед. обозрение. – 2019. – № 4 (26). – С. 133–141.

23. Тихонова, Л.П. Об актуальности внедрения современных цифровых технологий в образование / Л.П. Тихонова // Вестник

Череповец. гос. ун-та. – 2019. – № 1 (88). – С. 203–221.

24. Шихнабиева, Т.Ш. Цифровое образование: методы, модели и технологии развития / Т.Ш. Шихнабиева // Мониторинг. Наука и технологии. – 2018. – № 2 (35). – С. 65–68.

25. Alves, C. Experiential Learning of CAD Systems Interoperability in Social Network-based Education / C. Alves, G. Putnik // Procedia CIRP. – 2019. – Vol. 84. – P. 209–214.

26. Angrisani, L.A "Learning Small Enterprise" Networked with a FabLab: An Academic Course 4.0 in Instrumentation and Measurement / L.A. Angrisani, P. Arpaia, F. Bonavolontá et al. // Measurement. – 2020. – Vol. 150. – P. 107063.

27. Antonelli, D. Tiphys: An Open Networked Platform for Higher Education on Industry 4.0 / D. Antonelli, D.M. D'Addona, A. Maffei et al. // Procedia CIRP. – 2019. – Vol. 79. – P. 706–711.

28. Astakhova, L.V. The Concept of the Information-Security Culture / L.V. Astakhova // Scientific and Technical Information Processing. – 2014. – Vol. 41. – Iss. 1. – P. 22–28.

29. Bartsch, M. Woher Nehmen, Wenn Nicht Stehlen – Oder wo Haben Sie Ihren CISO her? / M. Bartsch // Cybersecurity Best Practices. Springer Vieweg, Wiesbaden. – 2018. – P. 261–269.

30. Broadband Commission Working Group on Education. Digital Skills for Life and Work. – 2017. – http://d-russia.ru/wp-content/uploads/2017/10/Digital-skills-for-life-and-work_259013e.pdf (дата обращения: 20.12.2019).

31. Carretero, S. DigComp 2.1: The Digital Competence Framework for Citizens with Eight Proficiency Levels and Examples of Use / S. Carretero, R. Vuorikari, Y. Punie // Publications Office of the European Union. – 2017.

32. COM 673: Strengthening European Identity through Education and Culture. – https://ec.europa.eu/commission/sites/beta-political/files/communication-strengthening-european-identity-education-culture_en.pdf (дата обращения: 20.12.2019).

33. Conference Board 2019. Employability Skills: The Skills you Need to Enter, Stay in, and Progress in the World of Workdwhether you Work on your own or as a Part of a Team. – https://www.conferenceboard.ca/edu/employability-skills.aspx?AspxAutoDetectCookieSupportZ1 (дата обращения: 20.12.2019).

34. Deloitte Reveals Top Challenges Facing New Chief Information Security Officers. – http://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-reveals-top-challenges-facing-new-cisos.htm (дата обращения: 21.12.2019).

35. EUCO 14/17: European Council Conclusions of 19 October 2017. – https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf (дата обращения: 20.12.2019).

36. Fuchs, L. Roles in Information Security – a Survey and Classification of the Research Area / L. Fuchs, G. Pernul, R. Sandhu // Computers & Security. – 2011. – Vol. 30. – Iss. 8. – P. 748–769.

37. Gerstein, J. Moving from Education 1.0 through Education 2.0 towards Education 3.0 / J. Gerstein, L.M. Blaschke, C. Kenyon // Experiences in Self-Determined Learning. CreateSpace Independent Publishing Platform. – 2014. – P. 83–98.

38. Grodotzki, J. Remote and Virtual Labs for Engineering Education 4.0: Achievements of the ELLI project at the TU Dortmund University / J. Grodotzki, T.R. Ortelt, A.E. Tekkaya // Procedia Manufacturing. – 2018. – Vol. 26. – P. 1349–1360.

39. Harkins, M.W. The 21st Century CISO / M.W. Harkins // Managing Risk and Informa tion Security. Apress, Berkeley, CA. – 2016. – P. 139–153.

40. Hildebrandt, C.K. Whose interest is educational technology serving? Who is included and who is excluded? / C.K. Hildebrandt // RIED. Revista Iberoamericana de Educación a Distancia. – 2019. – Vol. 22, no. 1. – P. 207–220.

41. Jackson, N.C. Managing for competency with innovation change in higher education: Examining the pitfalls and pivots of digital transformation / N.C. Jackson // Business Horizons. – 2019. – Vol. 62. – No. 6. – P. 761–772.

42. Mourtzis, D. Cyber-physical systems and education 4.0–the teaching factory 4.0 concept / D. Mourtzis, E. Vlachou, G. Dimitrakopoulos, V. Zogopoulos // Procedia Manufacturing. – 2018. – Vol. 23. – P. 129–134.

43. Okros, A. Cognitive Capacities and Competencies / A. Okros // Harnessing the Potential of Digital Post-Millennials in the Future Workplace. – 2020. – P. 77–91.

44. UNESCO – "Working Group on Education: Digital skills for life and work", 2017. – http://unesdoc.unesco.org/images/0025/002590/259013e.pdf (дата обращения: 24.10.19).

Астахова Людмила Викторовна, доктор педагогических наук, профессор кафедры защиты информации, Южно-Уральский государственный университет, г. Челябинск, astakhovalv@susu.ru.

Сафонова Ирина Алексеевна, студентка кафедры защиты информации, Южно-Уральский государственный университет, г. Челябинск, safonovaia97@mail.ru.

Поступила в редакцию 5 декабря 2019 г.

DOI: 10.14529/ped200106

DEVELOPMENT OF DIGITAL COMPETENCES OF FUTURE SPECIALISTS IN INFORMATION SECURITY AT UNIVERSITY

***L.V. Astakhova**, astakhovalv@susu.ru,*
***I.A. Safonova**, safonovaia97@mail.ru*
South Ural State University, Chelyabinsk, Russian Federation

Digital transformation of modern society causes higher education to develop both universal and professional digital competencies of students. This is critical for the future specialists in the field of information security, as their training has some specific features, which determine the relevance of this article. The goal of the research is to justify the development of digital competencies of information security students in the context of Education 4.0 paradigm and the national program for the development of digital economy. The theoretical significance of the study is the clarification of the concept of digital competencies, trends and the possible consequences of their development in Russian and foreign practice. The scientific novelty is in identifying the features and problems of the development of digital competencies of information security specialists, as well as in substantiating the prospective possibilities of these problems overcoming in training information security students at university. The effectiveness of new approaches to the organization of digital skills training of students in the course called information security risk management is shown.

Keywords: digital competencies, digital technologies, information security specialist, higher education, flipped classroom, social education.

This article was prepared with the support of the Government of the Russian Federation (Decree No. 211 of March 16, 2013, agreement No. 02. A03.21.0011).

References

1. Astakhova L.V. *Informatsionnaya bezopasnost': germenevticheskiy podkhod* [Information Security: a Hermeneutic Approach]. Moscow, RAN Publ., 2010. 185 p.

2. Astakhova L.V. [From Culture – to the Cultural Capital of the Organization's Information security]. *Bulletin of Culture and Arts*, 2018, no. 3 (55), pp. 85–101. (in Russ.)

3. Astakhova L.V. [From Media Information Literacy to Communicative-Cognitive-Managerial Cultural Competence: Imperatives of the Knowledge Society]. *Media Education*, 2017, no. 2, pp. 14–25. (in Russ.)

4. Astakhova L.V. [The Concept of Information Competence of a Specialist: Cognitive Approach]. *Bulletin of the South Ural State University. Ser. Education. Pedagogy*, 2013, vol. 5, no. 4, pp. 10–16. (in Russ.)

5. Astakhova L.V., Trofimenko A.E. [Development of Information and Analytical Skills of Students at the University]. *Bulletin of the Chelyabinsk State Pedagogical University*, 2011, no. 12, pp. 16–23. (in Russ.)

6. Astakhova L.V. [Development of Management Competence of the Future Information Security Specialist at the University]. *Modern Problems of Science and Education*, 2012, no. 6, p. 330. (in Russ.)

7. Astakhova L.V. *Upravlencheskaja kompetencija specialista po zashhite informacii* [Management Competence of the Information Security Specialist]. Chelyabinsk, 2014. 99 p.

8. Bur'kova E.V. [Professional Training of Specialists in the Field of Information Security]. *Bulletin of the Orenburg State University*, 2016, no. 2 (190), pp. 3–9. (in Russ.)

9. Dneprovskaya N.V. [Assessment of the Readiness of Russian Higher Education for the Digital Economy]. *Statistics and Economics*, 2018, no. 4, pp. 16–28. (in Russ.)

10. Egorova O.B. [Development of Digital Culture in Higher Education Institutions (on the Example of the University of Information Technology, Mechanics and Optics)]. *Modern Pedagogical Education*, 2019, no. 4, pp. 187–192. (in Russ.)

11. Zubov Yu.S. *Bibliografiya i hudozhestvennoe razvitie lichnosti* [Bibliography and Artistic Development of Personality]. Moscow, Kniga Publ., 1979. 144 p.

12. Kozlova N.Sh. [Digital Technologies in Education]. *Bulletin of the Maikop State Technological University*, 2019, no. 1, pp. 85–93. (in Russ.)

13. Komarova E.P., Stadnikov M.D. [Design of Automated Training Systems as a Means of Formation of Professional Competence of Specialists in Technical Protection of Information]. *Economic and Humanitarian Research of Regions*, 2016, no. 6, pp. 56–64. (in Russ.)

14. Leont'ev A.N. *Problemy razvitiya psikhiki* [Problems of Mental Development]. Moscow, 1972. 575 p.

15. Lukatskiy A.V. [Who are CISO and Whether they are in Russia?]. *Information Protection*, 2007, no. 3, pp. 18–20. (in Russ.)

16. Lushnikova S.S., Astakhova L.V. [The Culture of the Enterprise Information Security: a Comparative Analysis of Foreign and Russian Studies]. *UrFU Bulletin. Security in the Information Sphere*, 2019, no. 1 (31), pp. 37–47. (in Russ.)

17. [Digital Skills Training: Global Challenges and Best Practices. Analytical Report for the III International Conference "More than Learning: how to Develop Digital Skills"]. *Korporativnyy universitet Sberbanka* [Sberbank Corporate University]. Moscow, ANO DPO "Korporativnyy universitet Sberbanka" Publ., 2018. 122 p. (in Russ.)

18. *Pasport natsional'noy programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii" (utv. Prezidiumom Soveta pri Prezidente Rossiyskoy Federatsii po strategicheskomu razvitiyu i natsional'nym proektam protokol ot 24 dekabrya 2018 g. N 16)* [Passport of the National Program "Digital Economy of the Russian Federation" (Approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, Protocol No. 16 of December 24, 2018)]. Available at: https://base.garant.ru/72190282/ (accessed 24.12.2019).

19. Robert I.V. [Development of Informatization of Education Based on Digital Technologies: Intellectualization of the Learning Process, Possible Negative Consequences]. *The Science of Man: Humanitarian Research*, 2017, no. 4 (30), pp. 65–71. DOI: 10.17238/issn1998-5320.2017.30.65

20. Stadnikov M.D. [Model of Formation of Professional and Communicative Competence of Specialists in Technical Protection of Information with the use of Integrated Information Environment]. *World of Education-Education in the World*, 2015, no. 4 (60), pp. 259–272. (in Russ.)

21. Sulimov A.V., Orlov A.V. [Digital Technologies in Education: the Experience of the European Union]. *Innovatsionnye tekhnologii v obrazovatel'noy deyatel'nosti. Materialy Vserossiyskoy nauchno-metodicheskoy konferentsii* [Innovative Technologies in Educational Activities. Materials of the all-Russian Scientific and Methodological Conference]. 2019, pp. 136–138. (in Russ.)

22. Tabachuk N.P. [Information, Digital and Smart-competence of the Individual: Transformation of Views]. *Scientific and Pedagogical Review*, 2019, no. 4 (26), pp. 133–141. (in Russ.)

23. Tikhonova L.P. [On the Relevance of the Introduction of Modern Digital Technologies in Education]. *Bulletin of the Cherepovets State University*, 2019, no. 1 (88), pp. 203–221. DOI: 10.23859/1994-0637-2019-1-88-20

24. Shikhnabieva T.Sh. [Digital Education: Methods, Models and Technologies of Development]. *Monitoring. Science and Technology*, 2018, no. 2 (35), pp. 65–68. (in Russ.)

25. Alves C., Putnik G. Experiential Learning of CAD Systems Interoperability in Social Network-based Education. *Procedia CIRP*, 2019, vol. 84, pp. 209–214. DOI: 10.1016/j.procir.2019.07.002

26. Angrisani L., Arpaia P., Bonavolontá F., Moccaldi N., Schiano Lo Moriello R.A "Learning Small Enterprise" Networked with a FabLab: An Academic Course 4.0 in Instrumentation and Measurement. *Measurement*, 2020, vol. 150, pp. 107063. DOI: 10.1016/j.measurement.2019.107063

27. Antonelli D., D'Addona D.M., Maffei A., Modrak V., Putnik G., Stadnicka D., Stylios C. Tiphys: An Open Networked Platform for Higher Education on Industry 4.0. *Procedia CIRP*, 2019, vol. 79, pp. 706–711. DOI: 10.1016/j.procir.2019.02.128

28. Astakhova L.V. The Concept of the Information-Security Culture. *Scientific and Technical Information Processing*, 2014, vol. 41, iss. 1, pp. 22–28. DOI: 10.3103/S0147688214010067

29. Bartsch M. Woher Nehmen, Wenn Nicht Stehlen – Oder wo Haben Sie Ihren CISO her? *Cybersecurity Best Practices. Springer Vieweg, Wiesbaden*, 2018, pp. 261–269. DOI: 10.1007/978-3-658-21655-9_21

30. Broadband Commission Working Group on Education. Digital Skills for Life and Work. – 2017. Available at: http://d-russia.ru/wp-content/uploads/2017/10/Digital-skills-for-life-and-work_259013e.pdf (accessed 20.12.2019). DOI: 10.18411/a-2017-023

31. Carretero S., Vuorikari R., Punie Y. DigComp 2.1: The Digital Competence Framework for Citizens with Eight Proficiency Levels and Examples of Use. *Publications Office of the European Union*, 2017.

32. COM 673: Strengthening European Identity through Education and Culture. Available at: https://ec.europa.eu/commission/sites/beta-political/files/communication-strengthening-european-identity-education-culture_en.pdf (accessed 20.12.2019).

33. Conference Board 2019. Employability Skills: The skills you Need to Enter, Stay in, and Progress in the World of Workdwhether you Work on your own or as a Part of a Team. Available at: https://www.conferenceboard.ca/edu/employability-skills.aspx?AspxAutoDetectCookieSupportZ1 (accessed 20.12.2019).

34. Deloitte Reveals Top Challenges Facing New Chief Information Security Officers. Available at: http://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-reveals-top-challenges-facing-new-cisos.htm (accessed 21.12.2019). DOI: 10.1093/ww/9780199540884.013.45187

35. EUCO 14/17: European Council Conclusions of 19 October 2017. Available at: https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf (accessed 20.12.2019).

36. Fuchs L., Pernul G., Sandhu R. Roles in Information Security – a Survey and Classification of the Research Area. *Computers & Security*, 2011, vol. 30, iss. 8, pp. 748–769. DOI: 10.1016/j.cose.2011.08.002

37. Gerstein J., Blaschke L.M., Kenyon C. Moving from Education 1.0 through Education 2.0 towards Education 3.0. Experiences in Self-Determined Learning. *CreateSpace Independent Publishing Platform*, 2014, pp. 83–98.

38. Grodotzki J., Ortelt T.R., Tekkaya A.E. Remote and Virtual Labs for Engineering Education 4.0: Achievements of the ELLI Project at the TU Dortmund University. *Procedia Manufacturing*, 2018, vol. 26, pp. 1349–1360. DOI: 10.1016/j.promfg.2018.07.126

39. Harkins M.W. The 21st Century CISO. *Managing Risk and Information Security. Apress, Berkeley, CA*, 2016, pp. 139–153. DOI: 10.1007/978-1-4842-1455-8_10

40. Hildebrandt C.K. Whose Interest is Educational Technology Serving? Who is Included and who is Excluded? *RIED. Revista Iberoamericana de Educación a Distancia*, 2019, vol. 22, iss. 1, pp. 207–220. DOI: 10.5944/ried.22.1.22293

41. Jackson N.C. Managing for Competency with Innovation Change in Higher Education: Examining the Pitfalls and Pivots of Digital Transformation. *Business Horizons*, 2019, vol. 62, iss. 6, pp. 761–772. DOI: 10.1016/j.bushor.2019.08.002

42. Mourtzis D., Vlachou E., Dimitrakopoulos G., Zogopoulos V. Cyber-physical Systems and Education 4.0 – the Teaching Factory 4.0 concept. *Procedia Manufacturing*, 2018, vol. 23, pp. 129–134. DOI: 10.1016/j.promfg.2018.04.005

43. Okros A. Cognitive Capacities and Competencies. *Harnessing the Potential of Digital Post-Millennials in the Future Workplace*, 2020, pp. 77–91. DOI: 10.1007/978-3-030-25726-2_4

44. UNESCO – "Working Group on Education: Digital skills for life and work", 2017. Available at: http://unesdoc.unesco.org/images/0025/002590/259013e.pdf (accessed 24.11.19).

Received 5 December 2019

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Астахова, Л.В. Развитие цифровых компетенций будущих специалистов по защите информации в вузе / Л.В. Астахова, И.А. Сафонова // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». – 2020. – Т. 12, № 1. – С. 61–74. DOI: 10.14529/ped200106

FOR CITATION

Astakhova L.V., Safonova I.A. Development of Digital Competences of Future Specialists in Information Security at the University. *Bulletin of the South Ural State University. Ser. Education. Educational Sciences*. 2020, vol. 12, no. 1, pp. 61–74. (in Russ.) DOI: 10.14529/ped200106