



РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ
ОТДЕЛЕНИЕ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)
ИМЕНИ И. М. ГУБКИНА

**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
ЛИЧНОСТИ СУБЪЕКТОВ
ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА
В СОВРЕМЕННОМ
ОБЩЕСТВЕ**



РОССИЙСКАЯ АКАДЕМИЯ ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)
ИМЕНИ И. М. ГУБКИНА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ СУБЪЕКТОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В СОВРЕМЕННОМ ОБЩЕСТВЕ

Москва – 2023

УДК 061.3 + 004.056: ББК 74
И 74

Авторы-составители:
В. Г. Мартынов, И. В. Роберт, И. Г. Алехина

Рецензенты:
В. И. Блинов – доктор педагогических наук,
профессор, член-корреспондент
Российской академии образования
Р. С. Бозиев – доктор педагогических наук,
профессор, член-корреспондент
Российской академии образования

Ответственный редактор – *И. Г. Алехина*

И 74 Информационная безопасность личности субъектов образовательного процесса в современном обществе: Монография / Авторы-составители: В. Г. Мартынов, И. В. Роберт, И. Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И. М. Губкина, 2023. – 254 с.

ISBN 978-5-91961-489-0

Издание посвящено вопросам информационной безопасности личности субъектов образовательного процесса, анализу проблем, возникающих в процессе цифровой трансформации общества, обоснованы варианты их решения. Представлен опыт внедрения цифровых техно-логий в образовательный процесс.

Издание адресовано научным работникам, педагогам, студентам, а также широкому кругу читателей, интересующихся проблемами современного образования.

Материалы печатаются в авторской редакции.

ISBN 978-5-91961-489-0

© Коллектив авторов, 2023
© Российская академия образования, 2023
© РГУ нефти и газа (НИУ) имени И. М. Губкина, 2023

Введение

Цифровая трансформация общества, как и любой процесс, меняющий социально-экономические отношения, производственные процессы, роль человека в системе труда, способы коммуникации, сопровождается существенными изменениями в системе ценностей общества и личности. Ни одна из технологических революций, начиная с аграрной, не сопровождалась такими сложными социально-экономическими явлениями, как четвертая, когда создание компьютера привело к развитию информационно-коммуникационных технологий, созданию гигантского ресурса интеллектуальной силы. В системе разделения труда человек перешел из категории «трудовой ресурс» в категорию «капитал», а затем и в «потенциал». В необходимые для жизни направления развития личности вошли гражданская позиция, профессиональная деятельность и личная и социальная ответственность. Существенной чертой производства стала его интеллектуализация, и компетенции специалиста, дополненные цифровыми технологиями, создали трудно измеримый ресурсный интеллектуальный потенциал будущего.

Отличительной чертой социальной жизни стала безграничная открытость информационного пространства, в полной мере реализующая право личности на свободу и доступ к информации. Однако нельзя не заметить, что любой трансформации свойственны как безусловно позитивные, так и негативные процессы. Одной из проблем цифровой трансформации является сложность обеспечения в условиях открытого информационного пространства информационной безопасности и общества в целом, и личности. Это проблеме посвящены такие документы государственного уровня как Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (2017 г.), Стратегия

национальной безопасности Российской Федерации (2021 г.), Основы государственной политики Российской Федерации в области международной информационной безопасности (2021 г.), Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей (2022 г.), Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации (2022 г.), Концепция информационной безопасности детей в Российской Федерации (2023 г.) и др.

Документы взаимодополняют друг друга и, отмечая неразрывность жизни современного человека с пребыванием в информационном пространстве, выделяют формирование культуры и обеспечение информационной безопасности в числе приоритетных государственных задач.

Так «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» устанавливает «приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий», важность обеспечения государственной защиты интересов российских граждан в информационной сфере. В «Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» анализируются источники деструктивной идеологии и также определяется необходимость защиты «от внешнего деструктивного информационно-психологического воздействия», важность развития и совершенствования «форм и методов противодействия рискам, связанным с распространением деструктивной идеологии в информационном пространстве». В «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации на 2017–2030 годы» также подчеркивается необходимость формирования культуры информационной безопасности граждан Российской Федерации.

Федерации» формирование и развитие культуры информационной безопасности рассматривается как способ защиты в информационном пространстве.

Систематическое использование в профессиональной и бытовой деятельности, в образовательной практике цифровых технологий, влияя на жизнедеятельность общества, требует серьезного анализа с целью выявления баланса положительных и негативных факторов. Динамика изменения тематики прошедших четырех конференций, посвященных вопросам информационной безопасности личности субъектов образовательного процесса и организуемых Отделением профессионального образования Российской академии образования, демонстрирует ежегодное смещение обсуждения с технологической составляющей на гуманистическую.

Представленные в данном издании материалы отражают мнение отечественного научного и педагогического сообщества о содержании и формировании информационной безопасности личности с опорой на духовно-нравственные основы отечественного образования.

Авторы подчеркивают значимость воспитательной составляющей образования в формировании социально активной личности, способной противостоять рискам социально-информационного давления, обеспечить технологический суверенитет страны. Большое внимание уделено теоретико-методическим аспектам, методическим условиям обеспечения информационной безопасности личности субъектов образовательного процесса, предложены направления дальнейших теоретических и практико-ориентированных исследований, посвященных данной проблеме, а также вопросам обеспечения информационной безопасности научных исследований, проводимых в университетах, резуль-

таты которых могут потенциально оказывать влияние на обороноспособность страны и её конкурентоспособность на мировых рынках товаров и услуг, а также порядок экспертизы тематики и результатов таких исследований. Показаны возможности цифровой информационно-образовательной среды, повышающие качество образования.

От редакции

**ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ
И СОЦИАЛЬНЫЙ АСПЕКТЫ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ
ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ**

И. В. Роберт,

*академик РАО, доктор педагогических наук, профессор,
руководитель научной школы «Информатизация образования»,
заведующий лабораторией информатики и информатизации
образования ФГБНУ «Институт стратегии развития
образования»*

**ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ПОДХОДЫ К
ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ
ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ**

Современный период развития образования характеризуется **цифровой трансформацией образования**, которая рассматривается как результат системных существенных изменений, произошедших и происходящих в сфере образования, как позитивных, так и негативных, в связи с активным и систематическим использованием цифровых технологий и реализацией в образовательной практике технологий неконтактного информационного взаимодействия, технологий отображения реальной действительности

предметной области в виртуальную (VR, AR), нейросетевых технологий, систем искусственного интеллекта. **Цифровой трансформации подверглись многие процессы сферы образования:** предоставление образовательных услуг; создание цифровых образовательных ресурсов; информационно-методическое обеспечение учебного процесса; информационно-учебная деятельность; информационное взаимодействие, как между субъектами образовательного процесса, так и с цифровым ресурсом; управление образованием; информационное обеспечение и организационное управление деятельностью образовательной организации; обеспечение информационной безопасности личности субъектов образовательного процесса [11–15; 20].

К позитивному влиянию на развитие образования процесса использования цифровых технологий можно отнести следующее [11–15; 20]:

- **интеллектуализация процесса обучения**, обеспечивающая: **свободу поиска информации** для изучения или исследования объектов, процессов, явлений, учебных сюжетов; **осуществление взаимодействия с объектами или участие в процессах, находящих свое отображение на экране**, реализация которых в реальности невозможна, но методически целесообразна; **предоставление: инструмента** исследования абстрактных образов и понятий, **инструмента моделирования** изучаемых объектов, явлений, как реальных, так и виртуальных; **инструмента имитации** на экране реальных объектов или процессов; **инструмента проектирования предметной области** адекватно определенному содержательно-методическому подходу [6];
- **мультипредметное представление учебного материала** как отображение изучаемого объекта или процесса, исходя из

разных концептуальных подходов (философский, социологический, информационный, естественно-научный и др.);

- **реализация организационных форм и методов обучения** адекватно современным научно-исследовательским методам познания изучаемых закономерностей природных явлений и социальных проявлений, как реально протекающих, так и виртуально представляющих на экране реальные или абстрактные объекты, процессы, сюжеты;
- **появление принципиально новых средств обучения, функционирующих на базе информационных и коммуникационных технологий** (цифровой или электронный образовательный ресурс, интеллектуальные информационные системы прикладного и инструментального назначения, средства автоматизации контроля и поддержки учебной деятельности и пр.), использование которых повышает мотивацию обучения и обеспечивает самостоятельность при решении учебных задач;
- **расширение видов учебной деятельности** (автоматизация поиска, обработки, представления, формализации, продуцирования, тиражирования учебной информации; создание электронного (цифрового) образовательного ресурса; управление моделями изучаемых объектов, процессов, представленных на экране; экспериментально-исследовательская деятельность на базе виртуального лабораторного оборудования и пр.).

К возможным негативным последствиям влияния на обучающегося процесса использования цифровых технологий относятся [11–15; 20]:

- **ослабление дискурсивного (рассуждающего) типа мышления** и преобладание констатирующего типа мышления,

проявляющегося в ослаблении способности обучающегося концентрировать внимание на вычленении существенных признаков отбираемой информации в связи с тем, что при поиске информации в любой поисковой системе пользователь, как правило, **запоминает не содержание информации, а ее местонахождение или путь к нужной информации;**

- **рассредоточенность внимания**, возникающая в связи с избыточностью и доступностью любых объемов информации по любой изучаемой теме, что зачастую приводит к трудностям в выявлении содержательной составляющей информации об изучаемом объекте, процессе;
- **«контентная слепота» – затруднение осознания обучающимся целевой, структурно-содержательной, морально-ценностной компоненты информации при ее восприятии и использовании**, возникающая в связи с приоритетом визуального представления информации над содержательным, что снижает уровень понимания содержания информации, но усиливает наглядно образное восприятие информации;
- **«клипово-комиксное» восприятие информации**, приводящее к поверхностному восприятию учебной информации, к непониманию ее содержательной составляющей, представленной на экране в сжатой форме (пиктограммы, схемы, диаграммы, графики, инфограммы и пр.);
- **развитие дивергентного стиля мышления** в связи с ориентацией современного обучения на поиск множества решений какой-то одной проблемы с **последующим снижением до алгоритмического стиля мышления** – точное следование заранее усвоенным алгоритмам учебной деятельности.

Вышеизложенное определяет необходимость выявления факторов (таб. 1), влияющих на жизнедеятельность пользователя, которые обусловлены вызовами и рисками современного информационного общества (столбец 1) и определения следствий их влияния на пользователя (столбец 2). Анализ выявленных факторов и следствий их влияния позволил **выделить характерные особенности современного образования**, обусловленные вызовами и рисками современного информационного общества (столбец 3) **и предложить результаты научно-педагогических исследований, реализация которых обеспечит информационную безопасность личности субъектов образовательного процесса и будет способствовать нивелированию негативного влияния** на обучающегося указанных факторов (столбец 4).

Таблица 1

Факторы, обусловленные вызовами и рисками современного информационного общества

Факторы, влияющие на жизнедеятельность пользователя	Следствия влияния факторов на пользователя	Характерные особенности современного образования	Результаты научно-педагогических исследований, реализация которых обеспечивает информационную безопасность личности и нивелирует негативное влияние на обучающегося факторов
1. «Распределенность» и анонимность пользователя при осуществлении сетевого информационного взаимодействия.	Мотивированность пользователя на возможную ответственность при создании содержательного компонента информационного взаимодействия.	Глобализация информационного взаимодействия и осуществления информационной деятельности. Конвергенция педагогической науки и информационных и коммуникационных технологий. Сетевое образование.	Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса. 2. Проектирование: <ul style="list-style-type: none"> • конвергентного содержания образования в условиях использования ИКТ; • конвергентных методик обучения с использованием ИКТ; • конвергентных средств обучения, реализующих дидактические возможности ИКТ. Разработка научно-педагогических практик как результата феномена конвергенции педагогической науки и ИКТ.
2. Доступность пользователя к выбору любой информации в сети Интернет в неограниченном объеме.	Отсутствие регламентации при поиске, выборе информации, кроме мнения или желания пользователя.	Сетевое образование.	Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса. 2. Проектирование: <ul style="list-style-type: none"> • конвергентного содержания образования в условиях использования ИКТ; • конвергентных методик обучения с использованием ИКТ;

Факторы, влияющие на жизнедеятельность пользователя	Следствия влияния факторов на пользователя	Характерные особенности современного образования	Результаты научно-педагогических исследований, реализация которых обеспечивает информационную безопасность личности и нивелирует негативное влияние на обучающегося факторов
3. Доступность пользователя к любому партнеру или к группе партнеров по сетевому информационному взаимодействию.	Свобода выбора пользователем партнера по сетевому информационному взаимодействию, возможность его сопричастности к любым сетевым группам, выбор которых обусловлен только его личным мнением или предпочтениями.	Глобализация информационного взаимодействия и осуществления информационной деятельности. Конвергенция педагогической науки и информационных и коммуникационных технологий.	<ul style="list-style-type: none"> конвергентных средств обучения, реализующих дидактические возможности ИКТ. <p>3. Использование для образования интеллектуальных методов и моделей в информационных системах.</p> <p>Проектирование:</p> <ul style="list-style-type: none"> конвергентного содержания образования в условиях использования ИКТ; конвергентных методик обучения с использованием ИКТ; конвергентных средств обучения, реализующих дидактические возможности ИКТ.
4. «Распределенность» цели сетевого информационного взаимодействия между пользователями.	Возникновение у пользователя приоритета процесса сетевого информационного взаимодействия над его целью	Глобализация информационного взаимодействия и осуществления информационной деятельности.	<p>Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса.</p> <p>2. Проектирование:</p> <ul style="list-style-type: none"> конвергентного содержания образования в условиях использования ИКТ; конвергентных методик обучения с использованием ИКТ;

Факторы, влияющие на жизнедеятельность пользователя	Следствия влияния факторов на пользователя	Характерные особенности современного образования	Результаты научно-педагогических исследований, реализация которых обеспечивает информационную безопасность личности и нивелирует негативное влияние на обучающегося факторов
5. Концентрация внимания в процессе осуществления сетевого информационного взаимодействия при полном отвлечении внимания пользователя от реальных событий.	«Потеря» пользователем временного и (или) пространственного ориентиров и, как следствие, «утрата» связи с реальной действительностью.	Глобализация информационного взаимодействия и осуществления информационной деятельности. Конвергенция педагогической науки и информационных и коммуникационных технологий.	<ul style="list-style-type: none"> конвергентных средств обучения, реализующих дидактические возможности ИКТ. <p>Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса.</p> <p>2. Проектирование:</p> <ul style="list-style-type: none"> конвергентного содержания образования в условиях использования ИКТ; конвергентных методик обучения с использованием ИКТ. конвергентных средств обучения, реализующих дидактические возможности ИКТ. <p>3. Разработка научно-педагогических практик как результата феномена конвергенции педагогической науки и ИКТ.</p>
6. «Распределенность» внимания участников сетевого информационного взаимодействия в условиях использования ими любого объема аудиовизуальной информации.	Возникновение у пользователя неадекватного восприятия содержательных аспектов сюжета (сюжетов) сетевого информационного взаимодействия.	Глобализация информационного взаимодействия и осуществления информационной деятельности.	<p>Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса.</p> <p>2. Проектирование:</p> <ul style="list-style-type: none"> конвергентного содержания образования в условиях использования ИКТ;

Факторы, влияющие на жизнедеятельность пользователя	Следствия влияния факторов на пользователя	Характерные особенности современного образования	Результаты научно-педагогических исследований, реализация которых обеспечивает информационную безопасность личности и нивелирует негативное влияние на обучающегося факторов
7. Приоритет технологических и коммуникационных решений в процессе научных исследований и изысканий.	Ослабление у пользователя аналитико-синтетических, индуктивных дедуктивных и экспериментальных методов в процессе научных исследований.	Конвергенция педагогической науки и информационных технологий. Конвергенция педагогической науки и информационных технологий.	<ul style="list-style-type: none"> • конвергентных методик обучения с использованием ИКТ; • конвергентных средств обучения, реализующих дидактические возможности ИКТ. <p>1. Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса. 2. Разработка научно-педагогических практик как результата феномена конвергенции педагогической науки и ИКТ. 3. Использование интеллектуальных методов и моделей в информационных системах для образования.</p>
8. Замещение естественных наук конструктивными науками (математика, информатика, инженерные науки), которые активно применяются возможности информационных и коммуникационных технологий.	Создание искусственных (виртуальных) объектов, уровень сложности которых сопоставим с природными.	Конвергенция педагогической науки и информационных технологий. Возникновение и развитие популизма в науке и в образовании.	<p>1. Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса. 2. Разработка научно-педагогических практик как результата феномена конвергенции педагогической науки и ИКТ. 3. Использование интеллектуальных методов и моделей в информационных системах для образования.</p>

Факторы, влияющие на жизнедеятельность пользователя	Следствия влияния факторов на пользователя	Характерные особенности современного образования	Результаты научно-педагогических исследований, реализация которых обеспечивает информационную безопасность личности и нивелирует негативное влияние на обучающегося факторов
9. Создание информационных продуктов территориально распределенными коллективами.	Реализация возможностей сетевого информационного взаимодействия при создании информационных продуктов и возникновение «сетевой информативности» у работников.	Возникновение и развитие трансфер-интегративных областей научного знания (трансфер-зон). Глобализация информационного взаимодействия и осуществления информационной деятельности. Возникновение и развитие трансфер-интегративных областей научного знания (трансфер-зон).	<p>4. Реализация возможностей трансфер-зон в педагогической науке.</p> <p>1. Разработка и применение методических рекомендаций по формированию компетентности в области информационной безопасности личности субъектов образовательного процесса. 2. Проектирование: <ul style="list-style-type: none"> • конвергентного содержания образования в условиях использования ИКТ; • конвергентных методик обучения с использованием ИКТ; • конвергентных средств обучения, реализующих дидактические возможности ИКТ. </p> <p>3. Реализация возможностей трансфер-зон в педагогической науке.</p>

Анализ методических подходов, обеспечивающих информационную безопасность личности субъектов образовательного процесса и нивелирующих негативное влияние на обучающегося факторов, обусловленных вызовами и рисками современного общества [1–5; 7], позволяет вести речь о необходимости создания **Теории информационной безопасности личности субъектов образовательного процесса**, в которой рассматриваются теоретические и методические подходы к защите личности субъектов образовательного процесса от:

- воздействия информации, запрещенной законодательством, неэтичной, агрессивной, нелегитимной, оскорбляющей моральные ценности и чувства пользователя;
- использования некачественной педагогической продукции, разработанной на базе информационных и коммуникационных технологий, не отвечающей педагогико-эргономическим требованиям;
- ситуаций, которые приводят к потере авторских прав разработчика педагогической продукции, функционирующей на базе информационных и коммуникационных технологий.

Теоретико-методологические аспекты обеспечения информационной безопасности личности субъектов образовательного процесса представляют собой содержательные позиции подготовки личности к противодействию негативным информационным воздействиям извне на основе:

- развития способности личности к блокированию негативной информации, представляемой различными источниками, и к выявлению легитимности источника информации;
- формирования у обучающегося навыков критического мышления по отношению к воспринимаемой им информации;

- формирования компетентности обучающегося в области информационной безопасности личности субъектов образовательного процесса.

Методическое обеспечение информационной безопасности личности субъектов образовательного процесса [16–17; 18] представляет собой учебно-методические материалы в следующем составе:

- методические рекомендации по защите пользователя от негативного информационного воздействия извне;
- матрица компетенций в области информационной безопасности личности субъектов образовательного процесса.

Вышеизложенное позволило **сформулировать направления, на которые следует ориентироваться при разработке методик информационной безопасности личности субъектов образовательного процесса**

➤ **философско-психологическое:**

- обманчивость природы многофункционального и информационно емкого «виртуального мира» с его ирреальными и фантазийными отображениями реальной действительности, основанными на преобладании визуализации его объектов или процессов, происходящих в нем;
- неадекватность реальности виртуальных объектов, их отношений или процессов, представленных на экране, их условность, абстрагирование от существенных признаков реальных объектов и подмена их несуществующими в реальности;
- обманчивость информационного взаимодействия с партнером по общению при анонимности и непредсказуемости интерпретации его личности;

➤ **социально-этическое:**

- агрессивность, направленность на осуществление неправомерной деятельности и (или) действий, запрещенных законодательством Российской Федерации, или неадекватность национальным традициям народов России;
- оскорбление моральных ценностей и чувств пользователя;
- преднамеренное манипулирование сознанием пользователя, выполняющего действия с информацией или участвующего в компьютерных играх, или в процессе приватного общения с пользователем (ми) в сети Интернет;
- распространение информации, ориентированной на информационное неравенство (дефицит информации, значимой для данной социальной группы, отсутствие доступа к социально значимой информации);

➤ **педагогико-технологическое:**

- несоответствие педагогической продукции, представленной в электронном виде, установленным педагогико-эргономическим требованиям и нормативным документам;
- преобладание учебной информации в виде инфограмм, пиктограмм, визуальных образов, графических интерпретаций;
- заимствование результатов интеллектуальной собственности, представленной в электронном виде.

Выявленные и сформулированные теоретико-методические аспекты обеспечения информационной безопасности личности субъектов образовательного процесса позволяют переходить к формулированию **методических условий обеспечения информационной безопасности личности субъектов образовательного процесса:**

- формирование у обучающегося критического осмысления и

оценки информации на основе традиционных российских нравственных и культурных ценностей;

- обеспечение информационного взаимодействия между обучающимся и легитимным интерактивным источником информации;
- обеспечение «перехода» от визуальных образов и процессов (ситуаций) к их текстовому описанию и обратно;
- выявление возможностей средств, представляющих на экране визуальные образы и процессы (или ситуации), на основе их содержательного описания;
- реализация в педагогической продукции, представленной в электронном виде, психолого-педагогических, содержательно-методических требований, определяющих педагогико-эргономическое качество данной продукции;
- применение оценочных листов педагогико-эргономического качества педагогической продукции, представленной в электронном виде, при ее отборе или разработке;
- реализация нормативно-правовых и методических документов, регламентирующих легитимность использования педагогической продукции, представленной в электронном виде.

При этом выделяются **меры психолого-педагогического характера при обеспечении защиты от:**

- неэтичной, противозаконной, агрессивной информации (пропаганда насилия, терроризма, суицида, нарушения норм и правил поведения человека в обществе; «очернение» человека; вовлечение в запрещенные интернет-сообщества; вымогательство; запугивание);
- предоставления недостоверной, нелегитимной информации, а также информации этически некорректной;

- вмешательства в частную жизнь человека (защищенность личной информации, персональных данных);
- «информационного насилия» со стороны источника информации, адресованного «темной стороне» его личности.

Подытоживая вышеизложенное можно предложить **направления теоретических и практико-ориентированных исследований, посвященных обеспечению информационной безопасности личности субъектов образовательного процесса:**

- формирование внутренних интеллектуальных ресурсов личности, позволяющих противостоять информационным угрозам и «сетевым» атакам;
- разработка электронных образовательных ресурсов, удовлетворяющих педагогико-эргономическим требованиям, и учебно-методического обеспечения, включающего средства информационной защиты личности в условиях глобальной массовой коммуникации современного общества;
- разработка комплексных методик формирования у обучающихся способности активно противодействовать негативным воздействиям агрессивной информации;
- создание методической системы обучения студентов педагогических вузов в области информационной безопасности личности;
- формирование компетентности в области информационной безопасности личности субъектов образовательного процесса.

Особое место в Теории информационной безопасности личности занимает формирование **компетентности субъектов образовательного процесса в области информационной безопасности личности**, под которой будем понимать владение компетенциями по следующим направлениям: философско-мировоззрен-

ческое, социально-этическое, педагогико-технологическое. При этом под **компетенциями** будем понимать совокупность **знаний** в области основного содержания по общим вопросам обеспечения информационной безопасности личности субъектов образовательного процесса; **умений** в области использования методических и технологических средств обеспечения информационной безопасности личности субъектов образовательного процесса; **опыта** реализации знаний и умений по общим вопросам в области основного содержания и реализации средств обеспечения информационной безопасности личности субъектов образовательного процесса (Таблица 2) [10; 11; 12].

Представим в Таблице 2 **в области информационной безопасности личности субъектов образовательного процесса.**

Компетенции в области информационной безопасности личности субъектов образовательного процесса

Философско-мировоззренческие	Социально-этические	Педагогико-технологические
<p>Знания в области</p> <ul style="list-style-type: none"> • «обманчивости природы» многофункционально о и информационно емкого «виртуального мира» с его ирреальными и фантазийными отоображениями реальной действительности. • особенностей виртуальных объектов, их отношений или процессов, представленных на экране (неадекватность реальности, условность признаков, абстрагирование от существенных признаков). • «обманчивости» информационного взаимодействия с партнером по 	<ul style="list-style-type: none"> • выявления в содержании информации агрессивности, направленности на осуществление неправомерной деятельности и (или) действий, запрещенных законодательством РФ; • выявления информации, оскорбляющей моральные ценности и чувства пользователя; • выявления информации образовательного назначения, не соответствующей педагогико-эргономическим требованиям к педагогической продукции, реализованной на базе ИКТ; • выявления в содержании информации замствования результатов интеллектуальной собственности, представленной в электронном виде; • выявления в содержании информации предумышленного манипулирования сознанием человека, выполняющего действия с информацией в сети Интернет; • выявления в компьютерных играх; при участвующего в компьютерных играх; при приватном общении с пользователем (ми) в сети Интернет; • критического осмысления и оценки информации на основе нравственных и культурных ценностей; 	<ul style="list-style-type: none"> • структурирования несистемных данных и их трансформации в информацию и в знание; • наличия связей между информацией (знаниями), относящейся (ихся) к элементу множества, и информацией (знаниями) об этом множестве при сохранении информации (знаний), принадлежащей (их) всем элементам множества, записанной (ых) одноактно при описании самого множества; • ситуативных отношений, определяющих ситуативную совместимость той или иной информации (тех или иных знаний), хранимой (ых) в памяти; • обеспечения информационного взаимодействия между пользователем и интерактивным источником информации; • представления информации в виде визуальных образов или графических интерпретаций • перехода от визуальных образов и процессов (ситуаций) к их текстовому описанию и обратно; • создания и использования средств, порождающих на экране визуальные образы и процессы (или ситуации) на основе их внутренних представлений;

Философско-мировоззренческие	Социально-этические	Педагогико-технологические
<p>Умения в области</p> <ul style="list-style-type: none"> • выявления и описания признаков «виртуального мира» (ирреальность, фантазийность), отличительных от реальной действительности; • выявления и описания особенностей виртуальных объектов, их 	<ul style="list-style-type: none"> • отбора (по ключевым словам) информации с агрессивными высказываниями; • выявления содержания информации, не соответствующей Государственным законодательным материалам; • выявления содержания информации, не соответствующей принятой этике (или оскорбляющей моральные ценности и чувства пользователя); • выявления контента ЭОР, не соответствующего требованиям к эргономическим требованиям к 	<ul style="list-style-type: none"> • содержания Технических требований педагогико-эргономического качества педагогической продукции, функционирующей на базе ИКТ; • содержания методик использования оценочных листов педагогико-эргономического качества педагогической продукции, функционирующей на базе ИКТ; • содержания нормативно-правовых и методических документов, регламентирующих легитимность использования педагогической продукции, разработанной с использованием ИКТ; • технологических оснований сертификации технических средств и носителей информации.

Философско-мировоззренческие	Социально-этические	Педагогико-технологические
<p>Умения в области</p> <ul style="list-style-type: none"> • выявления и описания признаков «виртуального мира» (ирреальность, фантазийность), отличительных от реальной действительности; • выявления и описания особенностей виртуальных объектов, их 	<p>педагогической продукции, реализованной на базе ИКТ;</p> <ul style="list-style-type: none"> • выявления информации образовательного назначения на предмет заимствования результатов интеллектуальной собственности, представленной в электронном виде; • выявления информации, манипулирующей сознанием человека, выполняющего действия с информацией в сети Интернет; • участия в компьютерных играх; при приватном общении с пользователем (ми) в сети Интернет. 	<ul style="list-style-type: none"> • осуществления информационного взаимодействия между пользователем и интерактивным источником информации; • визуализации информации в виде визуальных образов или графических интерпретаций; • интерпретации визуальных образов и процессов (ситуаций) в текстовое описание и обратно; • использования программных средств, представляющих на экране визуальные образы и процессы (или ситуации); • анализа нормативно-правовой, методической и технологической документации в области легитимности использования педагогической продукции, разработанной с использованием ИКТ; • использования оценочных листов педагогико-эргономического качества педагогической продукции, разработанной с использованием ИКТ; • установление соответствия оцениваемой педагогической продукции, функционирующей на базе ИКТ, техническим требованиям педагогико-эргономического качества.

Философско-мировоззренческие	Социально-этические	Педагогико-технологические
<p>Опыт реализации знаний и умений</p> <ul style="list-style-type: none"> • выявления ирреальности, неадекватности реальной действительности виртуальных объектов и их отношений или процессов, представленных на экране; • выявления партнеров по информационному взаимодействию, которые являются настоящими анонимными. 	<ul style="list-style-type: none"> • блокирования агрессивной информации или информации, склоняющей к неправомерной деятельности, запрещенной законодательством РФ или не соответствующей принятой этике; • выявления контента ЭОР, не соответствующего педагогико-эргономическим требованиям; • блокирования информации образовательного назначения на предмет заимствования результатов интеллектуальной собственности; • блокирования информации, манипулирующей сознанием человека. 	<ul style="list-style-type: none"> • информационного взаимодействия между пользователем и интерактивным источником информации при обеспечении визуализации информации о различных образах или графических интерпретаций; • представления визуальных образов и процессов (ситуаций) в текстовое описание и обратно; • использования нормативно-правовой, методической и технологической документации для установления легитимности использования педагогической продукции, разработанной с использованием ИКТ; • оценки педагогико-эргономического качества педагогической продукции, разработанной с использованием ИКТ.

Таким образом, *учебно-методическое обеспечение информационной безопасности личности субъектов образовательного процесса в условиях информатизации образования* предполагает наличие:

техничко-технологических средств информационной защиты личности субъектов образовательного процесса от нелегитимной, агрессивной, неэтичной информации в условиях глобализации информационного взаимодействия при массовой сетевой коммуникации современного общества;

методик формирования устойчивых состояний личности, обеспечивающих ее информационную безопасность;

организационных форм и методов противодействия негативным воздействиям агрессивной интернет-среды.

Литература

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) [Электронный ресурс]. – Режим доступа: <http://www.consultant.ru>, раздел IV, п.27.

2. Мухаметзянов И.Ш. Формирование здоровьесберегающей информационной образовательной среды в условиях глобальной информатизации // Казанский педагогический журнал. – 2015. – №5. – С. 239–244.

3. Поляков В.П. Педагогическое сопровождение аспектов информационной безопасности в информационной подготовке студентов вузов // Педагогическая информатика. – 2016. – № 4. – С. 37–47.

4. Поляков В.П. Развитие информационной подготовки в контексте стратегии национальной безопасности Российской Федерации // Научград: наука, производство, общество. – М.: ООО «Издательский дом «Научная библиотека». №2, 2016. С. 46–51.

5. Роберт И.В. Формирование информационной безопасности личности обучающегося в условиях интеллектуализации его деятельности // Педагогическая информатика – 2017. – № 2. – С. 42–59.

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

7. Robert I.V. Pedagogical Feasibility of Using Systems on the Web-interface for Implementating the Interdisciplinary Nature of Training // Proceedings of the International Conference on the Development of Education in Russia and the CIS Member States (ICEDER 2018) – Moscow, 2018. – p. 36–40. (WOS)

8. Роберт И.В. Конвергентное образование: истоки и перспективы Наука о человеке: гуманитарные исследования. – 2018. – № 2 (32). – С. 64–76.

9. С.А. Бешенков, Я.А. Ваграменко, В.А. Касторнова, О.А. Козлов, Э.В. Миндзаева, И.Ш. Мухаметзянов, В.П. Поляков, И.В. Роберт, В.И. Сердюков, Т.Ш. Шихнабиева, Г.Ю. Яламов Развитие информатизации образования в школе и педагогическом вузе в условиях обеспечения информационной безопасности личности: Монография. – М.: ФГБНУ «ИУО РАО», –2018. – 105 с.

10. Роберт И.В. Информационная безопасность личности субъектов образовательного процесса// Информатизация образования и науки. – 2019. – 3 (43). С. 119–127.

11. Роберт И.В. Цифровая трансформация образования: вызовы и возможности совершенствования// Информатизация образования и науки. – 2020 – № 3 (47). – С. 3–16.

12. Роберт И.В. Направления развития информатизации отечественного образования периода цифровых информационных технологий // Электронные библиотеки. – 2020. – Т. 23. – № 1–2. –С. 145–164.

13. Роберт И.В. Стратегические ориентиры развития информатизации образования в условиях цифровой трансформации // Информатизация образования – 2020 / Материалы Международной научно-практической конференции, посвященной 115-летию со дня рождения патриарха российского образования, великого педагога и математика, академика РАН С.М. Никольского (1905 – 2012 гг.) (29 – 31 октября 2020 г., г. Орёл) // под ред. А.А. Русакова. – Орёл: ОГУ имени И.С. Тургенева, 2020. – С. 42–60.

14. Роберт И.В. Цифровая трансформация образования: ценностные ориентиры, перспективы развития//Россия: Тенденции и перспективы развития. Ежегодник. Вып. 16: Материалы XX Национальной научной конференции с международным участием «Модернизация России: приоритеты, проблемы, решения» / РАН. ИНИОН. Отд. науч. сотрудничества; Отв. ред. В.И. Герасимов. – РАН. ИНИОН. – М., 2021. – Ч. 1. – С. 868–876.

15. *Robert I.V.* Formation and development of digital transformation of domestic education on the basis of systemic convergence of pedagogical science and technology // 03017 Published online: 26 April, 2021 / DOI: <https://doi.org/10.1051/shsconf/202110103017> PDF (285.1 KB) References (WOS).

16. *Robert I.V.* Development of education during digitalization in the context of the axiological approach // In A. A. Arinushkina (Ed.), *Advances in Education Research and Practice*. Cham, Switzerland: Springer. 2021 (WOS).

17. *Роберт И.В.* Подготовка педагогических кадров в области информационной безопасности личности в условиях цифровой трансформации образования // Информационная безопасность личности субъектов образовательного процесса в цифровой информационно-образовательной среде: Монография / Авторы-составители: В.Г. Мартынов, И.В. Роберт, И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2021. – С. 151–171.

18. *Роберт И.В., Шихнабиева Т.Ш., Касторнова В.А., Козлов О.А., Поляков В.П., Мухаметзянов И.Ш.* Международный опыт применения цифровых технологий в деятельности общеобразовательных организаций // Педагогическая информатика. – 2022 – № 1. – С. 75–93.

19. *Роберт И.В.* Цифровая трансформация образования: потенциал позитива и возможные риски для образовательного процесса // Информационная безопасность личности субъектов образовательного процесса в современном обществе: сб. материалов научно-практической конференции / Авторы-составители: В.Г. Мартынов, И.В. Роберт, И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2022. – С. 10–31.

20. Указ Президента Российской Федерации от 07.07.2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации [Электронный ресурс]. – Режим доступа: <http://www.kremlin.ru/acts/bank/33514>.

21. Указ Президента РФ от 09 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» [Электронный ресурс]. – Режим доступа: <http://www.kremlin.ru/acts/bank/41919>.

В. Г. Мартынов,

*доктор экономических наук, профессор,
академик Российской академии образования,
ректор Российского государственного университета нефти и
газа (национального исследовательского университета)
имени И. М. Губкина*

А. А. Туманов,

*проректор по молодежной политике и воспитательной работе
Российского государственного университета нефти и газа
(национального исследовательского университета)
имени И. М. Губкина*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АСПЕКТЕ ЦИВИЛИЗАЦИОННЫХ КУЛЬТУР

В классической теории иерархии потребностей А. Маслоу потребность в безопасности относится к числу первичных, свойственных всем без исключения. Ожидание опасности, по мнению автора «Теории человеческой мотивации», нивелирует все остальные потребности, включая психологические. В связи с размыванием границ отдельных сфер безопасности в условиях технологических преобразований бесспорность такой точки зрения становится все более очевидной. Безопасность личности приобретает все более сложную форму: опасности физического, экономического, военного, психологического, социального характера дополнились, а в ряде случаев и усилились постоянным информационным давлением. С одной стороны, человечество поднялось по ступеням интеллектуального и технологического развития, получило широчайший доступ к информации, с другой – усиливается противостояние цивилизаций,

повышается уровень конфликтности. Процесс глобализации привел к определенной зависимости стран друг от друга и к возможности оказания существенного давления технологически более развитыми локальными цивилизациями на экономическую, социальную, культурную сферы менее развитых. Информационно-коммуникационные технологии, сети, управление которыми экстерриториально, обеспечивает массированное воздействие на личность, став основным оружием геополитического противостояния. Угрозы безопасности личности и общества приобрели гибридный характер, обусловив появление термина «гибридная война», одной из сфер которой является культурно-мировоззренческая. «Отчуждение человека от культуры, в которой он укоренен, а точнее – от его культурной идентичности», «подмена и частичное разрушение основ общественной жизни и ценностных ориентаций» [7, с. 264] поддерживают геополитическое влияние эффективнее, чем все иные инструменты внешнего воздействия. Путем «информационного террора», под лозунгом либерализации общества методично рушатся культурные коды, идет трансформация ценностей [10], разрывается связь между личностью и обществом, снижается доверие к государству – «генераторы дезинформации функционируют намного эффективнее, нежели генераторы правдивой информации» [1].

Произошедшая в сфере информации революция сменила расстановку сил не только на геополитической арене, но и в понимании роли человеческого потенциала – «критически важной инфраструктуры» в технологическом прогрессе, т.к. для жизнедеятельности любого государства интеллектуальные и духовные ресурсы, их способности и стремление к технологическому развитию и готовность осознанно противостоять информационному, пропагандистскому, культурно-цивилизационному давлению становятся не менее значимыми, чем ресурсы природные. Поэтому основной

вектор информационного противодействия направлен на формирование культуры информационной безопасности как важной составляющей общей безопасности личности. Но прежде чем рассмотреть этот относительно новый феномен, следует проанализировать условия и предпосылки его зарождения.

Многие публикации и политические выступления в течение довольно длительного периода времени в качестве ближайшей перспективы для человечества определяли глобализацию. Идеология интегрированного глобального пространства, некоего космополитического сообщества, в котором растворятся нации, а главными движущими силами станут универсальные ценности и трансконтинентальное и межрегиональное взаимодействие, овладела множеством умов – началось построение единого образовательного пространства, единого глобального рынка труда, глобальной финансовой системы. В моду вошли экстерриториальность, экспатриотизм как форма мировоззрения, отрицающая значимость связи с Родиной и действий в ее благо. Анализируя трансформацию традиционных ценностей при переходе от 4-й промышленной революции к цифровой цивилизации [10], автор обращает внимание, что под видом продвижения новых экономических моделей ломается культурно-нравственная целостность целого поколения. Примером тому может служить появление экспатов – универсальных работников, ориентированных на удобное «место проживания» и финансовую выгоду, свободных от ответственности за будущее общества, отказавшихся от своих исторических и культурных корней. Такая идеология замещает сложившееся представление о доминировании национальных и территориальных принципов в установлении государства и кажется заманчивой, т.к., с одной стороны, обещает полную свободу, доступ каждому к созданным и создаваемым человечеством благам, с

другой – политическую стабильность и, как следствие, безопасность. Однако так ли все однозначно? Многие исследователи, как отечественные, так и зарубежные, обращают внимание на то, что процесс глобализации имеет многоплановый характер, различным образом отражается на разных странах, регионах, социальных группах и является вызовом государственному суверенитету (Д. Хельд, Е. А. Нарочницкая и др.).

«Глобализация» мироустройства для России пришлась на период резких социальных перемен, когда рушились устоявшиеся идентичности, ломалась социально-экономическая и политическая системы, и чрезмерно увлекшись на довольно длительный период идеями неолиберализма, мы, обладая богатой историей, уникальной культурой, вступили на путь преобразований, слепо копируя чужую идеологию и не оценивая риски и разницу политических и культурных традиций. Стратегическая идея того периода была «догоняющей», т.е. идеологией следования по тому пути, по которому уже прошли другие страны, цивилизации, общества.

Под лозунгом неизбежности глобализации и универсальности культуры, как одной из важнейших ее характеристик, «в фарватере идеологий Запада» методично нивелировалось значение основ идентификации – происхождения, языка, ценностей, истории, религии, обычаев, общественных институтов – всего того близкого социокультурного мира, который дает старт развитию личности; подверглась необоснованной критике сущность общероссийской гражданской идентичности. По сути была обесценена базовая потребность человека – коллективная идентичность, угроза которой воспринимается как одна из основных угроз безопасности [13, с. 15].

Вера в универсальность захватила все – образование, культуру, систему ценностей, рынок труда, моду. Е. А. Нарочницкая к числу факторов глобализации относит «исчезновение многих традицион-

ных границ в сфере информационного и культурного обмена; распространение унифицированной масс-культуры и этики» [11, 154].

К универсалистским можно отнести взгляд израильского военного историка-медиевиста¹ Ю. Н. Харари, который, не отрицая религиозной и национальной идентичности, полагает, что «все мы принадлежим к одной буйной глобальной цивилизации» [16, с. 141], и предлагает для определения идентичности не список общих черт, а перечень общих конфликтов и дилемм, прогнозируя глобальную унификацию и разделение в преддверии ее преддверии человечества на разные биологические касты (!).

Однако о невозможности универсализма еще в середине XIX века предупреждал основоположник отечественного мультицивилизационного подхода Н. Я. Данилевский. В труде «Россия и Европа: взгляд на культурно-исторические и политические отношения Славянского мира к Германно-Романскому», рассматривая цивилизацию в качестве главной формы организации человеческого общества, геополитик отмечал, что она определяется особенностями духовной природы народов, составляющих самобытные типы культуры. Противостояние цивилизаций – это противостояние различных систем ценностей разных культурно-исторических типов. Цивилизационное своеобразие России обусловлено, по мнению Н. Я. Данилевского, главной силой русского народа – внутренним нравственным сознанием [3, с. 163] и ведущими чертами психического строя – миролюбием и терпимостью.

Во внешнеполитической деятельности ученый призывал к разумному эгоизму, позволяющему учитывать в любом союзе, в первую очередь собственные интересы, и прогнозировал усиление антагонизма Европы и России по мере возрастания внутренних сил России [4].

¹ Специалист по истории Средних веков.

Век спустя американский социолог С. Хантингтон определил универсализм как идеологию, принятую для противостояния Не-западным культурам, подчеркивая, что мнение о тождественности современной цивилизации и западной ошибочно [15, с. 90–96]. Автор геополитического трактата «Столкновение цивилизаций» полагал, что процесс модернизации выстраивает глобальную политику в соответствии с направлением развития культуры, при этом наивысшей культурной общностью людей является цивилизация, предоставляющая личности самый широкий уровень идентификации и выделяющая человека из иных биологических видов [15, с. 51], а вся история развития человечества – это история цивилизаций [15, с. 46].

Не менее однозначно с точки зрения социально-экономических измерений о перспективах формирования «новой общечеловеческой цивилизации» высказался известный ученый Института востоковедения РАН С. И. Лунев: «К XXI в. также стало все более понятным, что биполярный и однополюсный мир не соответствует и культурно-цивилизационным реалиям, и отличиям стран мира» [9, с. 172–173].

Эффективности продвижения идеологии универсализма глобальной цивилизации во многом способствовал упор на единый социально-экономический базис в ущерб этнокультурной составляющей, несмотря на то, что во всей вариативности формулировок понятия цивилизации, в которой можно выделить шесть основных признаков (Л. С. Перепелкин, Институт Востоковедения РАН), устойчивость культуры, религии и системы ценностей занимают лидирующие позиции [12]:

- культура, устойчивая во времени на определенной территории (вне привязки к государственному устройству);
- единство языка и письменности (возможность культурной коммуникации);

- общества с государственным устройством;
- общества, исповедующие одну из мировых или локальных религий и идеологий, содержащую общую систему ценностей;
- субъекты исторического процесса (союзы государств, организованные в политической форме и принимающие самостоятельное участие в международной политической деятельности);
- общества с единым социально-экономическим базисом.

Авторы данной статьи не разделяют идеологию универсализма, склоняясь к предположению, что в ближайшем будущем предпосылок для исчезновения локальных цивилизаций и замещения их универсальной или глобальной нет, и, как показывают события, усиливающееся взаимодействие между локальными цивилизациями лишь укрепляет национальное самосознание и ведет к кризисам не столько на идеологическом, сколько на культурном уровне. Более того, нарастающее разобщение стран / локальных цивилизаций на блоки показывает несостоятельность идеологии глобализации. Любые ценностные притязания со стороны «чужих» локальных цивилизаций, социокультурных групп воспринимаются крайне негативно. Такой подход не позволяет обвинить нас в несовременности – современный не означает западный, восточный или какой иной и не предусматривает обязательность утраты идентичности. Одно из значений слова «современный» – «стоящий на уровне своего века, не отсталый, отвечающий материальным потребностям, *общественным, культурным*² запросам настоящего времени» [14]. Развитие человечества, безусловно, сопровождается экономической, гражданской и культурной интеграцией, сближая мировоззренческие основы, но нельзя не учитывать тот

² Выделено авторами статьи.

факт, что культурные запросы традиционно строятся на эмоциональных и рациональных связях, определяемых национальной идентичностью, и, как следствие, цивилизации, выстраиваясь на основании общих черт объективного порядка, не стирают границы, свойственные современному пониманию национального. Идеологическая глобализация всегда преследует интересы определенной и незначительной группы стран и крупнейшие страны принадлежат различным цивилизациям, поэтому попытки подавить национальную идентичность ведут к конфликтам и в культурно-мировоззренческой сфере, и к военным.

События последних лет продемонстрировали уязвимость трансформации принципов универсализма в стратегии внутренней и внешней политики, потребовали следования политике аутентичного развития, что, однако, не означает сползания в сторону национализма.

Отметим, что авторы статьи четко разграничивают понятия национального и национализма и видят разницу в подходах к пониманию национального: как политического единства на определенной территории (Э. Ренан) или (второй подход) как этнокультурной и языковой целостности, не связанной единым государством (И. Гердер). Представляется, что нам в современном понимании *национального* следует объединить эти подходы и опираться на «Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», т.е. как *на единство в многонациональном и многоконфессиональном суверенном государстве* [17]. Такой подход учитывает государственный, культурно-исторический, социально-экономический аспекты, аутентичное политико-цивилизационное развитие, позволяет рассматривать вопросы безопасности комплексно и в соответствии с рисками, возникающими в процессах

развития технологий, продвижения идеологии глобализации, и культурно-мировоззренческими конфликтами.

Военный дипломат А. А. Бартош в качестве одной из целей в противостоянии цивилизаций и задач информационного давления видит разрушение культурного кода – того «коллективного подсознательного» и «культурного бессознательного», что передается в виде социального опыта от поколения к поколению, идентифицируя локальную цивилизацию, предопределяя поведенческие паттерны [2]. Культурный код не менее сильно, чем экономический, военный, научный потенциал влияет на устойчивость нации к внешним вызовам и угрозам. Именно разрыв связей между историческим и культурным прошлым дестабилизирует настоящее, обрекая на зависимое будущее.

Возвращаясь к началу статьи подчеркнем, что влиянию сконструированных и поданных специальным образом с целью манипулирования сознанием информационных потоков особенно подвержено молодое поколение «цифровых аборигенов», рожденное и формирующее свое мировоззрение в цифровой среде. И это предопределяет новые риски, с которыми столкнулась система образования, и понимание особенностей современного образовательного пространства.

Проблемы современного образовательного пространства широко исследуются педагогикой. С. В. Иванова, О. Б. Иванов определяют его как «объектный мир, совокупность имеющих отношение к образованию объектов, создающих и наполняющих это пространство, и одновременно предмет субъектной деятельности, заключающийся в восприятии, действии, воздействии субъектов на это пространство» [5, с. 16], Лескова И. А. анализирует его внутреннюю форму в соответствии с фундаментальными отношениями как индивидуальное (кто), процедурно-инструментальное (как),

социальное (с кем и каким образом) и культурно-информационное (для чего) подпространства и подчеркивает, что это «зонтичный термин», «органическое единство, а не суммативная целостность своих подпространств <...> активная величина, а не бездейственная форма, фиксированное вместилище, образовательное пространство продуцируемо (конструируемо) субъектами обучения, следовательно, в актуальное состояние переводится их активностью» [8]. Традиционно существование и реализация образовательных объектов, феноменов и процессов локализовались в определенном специально организованном пространстве, объединяющем процессы воспитания и обучения и опирающимся на традиционные российские духовно-нравственные ценности. Сегодня, благодаря тренду на формирование единого мирового/глобального образовательного пространства и унификацию, открытости информационного пространства и все той же склонности к доверию всему иноземному, это пространство разомкнулось. В образовавшийся проем хлынули коучи, инфлюэнсеры, блогеры, марафоны, «успешный успех» и огромный пласт чуждой нашей идентичности западной культуры, страдающей, по мнению С. Хантингтона, тремя недугами – ошибочностью, аморальностью, опасностью [15].

И здесь следует еще раз обратиться к Н. Я. Данилевскому, который различал славянский и германо-романский миры, в том числе по ведущим чертам психического строя. Если характерные славянские черты, как было сказано выше, миролюбие и терпимость и, как следствие, коллективизм и социальная справедливость, то в качестве общей германо-романской Н. Я. Данилевский выделял насильственность, как «чрезмерно развитое чувство личности, индивидуальности, по которому человек, им обладающий, ставит свой образ мыслей, свой интерес так высоко, что всякий иной образ мыслей, всякий иной интерес необходимо должен ему уступить, волею или

неволею, как неравноправный ему» [3, с. 150]. Такая характеристика поддерживается и С. Хантингтоном, который, рассматривая подъем Запада в XIX веке, отмечал, что «Запад завоевал мир не из-за превосходства своих идей, ценностей или религии <...>, но скорее превосходством в применении организованного насилия» [15, с. 66]. А. А. Бартош, акцентируя внимание на разнице в целеполагании локальных цивилизаций, основывается на понятии культурного фокуса, введенного американским антропологом Мелвиллом Херсковичем, – преобладающей существенной черты каждой культуры, отражающей «тенденцию конкретного общества к особой сложности и изоциренности одних аспектов и институтов на фоне относительной простоты других» и способной стать центром инноваций. Культурный фокус, по мнению А. А. Бартоша, для большинства стран Западной Европы – развитие торговли и технологий, для США – наращивание экономического и военного потенциала с целью глобального доминирования (опираясь на навязанную миру финансовую систему и поп-культуру), в то время как российский фокус направлен на межнациональный мир и согласие, обороноспособность страны, сбалансированность отношений между Западом и Востоком. Такое определение культурных фокусов некоторых цивилизаций вполне коррелируется с исследованиями Н. Я. Данилевского и С. Хантингтона.

Применительно к системе образования представляет интерес отрицание С. Хантингтоном «давосской культуры» как универсальной цивилизации. На определенный период времени «давосская культура», построенная на предположениях, ценностях и доктринах, в числе которых «вера в индивидуализм, рыночную экономику и политическую демократию», провозглашаемых на Всемирном экономическом форуме в Давосе группой интеллектуалов, банкиров, бизнесменов, правительственных чиновников, журналистов

(перечень С. Хантингтона), стала доминирующей в подготовке специалистов практически во всем мире, внедрилась в отечественное образовательное пространство. Однако «давосский тип интеллектуальной культуры» нельзя считать универсальным, т.к. даже с учетом влияния данной группы (около тысячи человек) на международные институты, мировые правительства и экономику, по мнению Хедли Булла, сомнительно, что «даже на дипломатическом уровне она охватывает то, что было названо культурой общей морали или сводом общих правил, в отличие от общей интеллектуальной культуры» [15, с. 77].

В качестве одного из наиболее ярких примеров внедрения «давосской культуры» в образование можно привести изменение требований к выпускникам высшей школы. Исключительно практико-ориентированный подход и универсализация компетенций выдавили свойственную отечественному образованию фундаментальность, основанную на формировании у обучающихся научной методологии, системного мировоззрения на основе традиционных духовно-нравственных ценностей. Свойственные нашей идентичности патриотизм, коллективизм сменились нацеленностью на личный успех, воспитание отошло на второй план, гармонично выстроенная системность в образовании уступила место «лоскутному» коучингу.

Представляется, что отнесение образования к услугам – еще одно крайне опасное «давосское последствие», которое потребовало под давлением общественности в 2022 году изменений в законодательстве. И вопрос не только в желании повысить престиж преподавательской деятельности, но и в самой сути образования, как деятельности совместной и двухсторонней – и обучающихся и обучающихся – направленной на развитие личности, передачу из поколения в поколение нравственных установок, знаний, того са-

мого культурного кода, обеспечивающего стабильность общества.

Обобщая сказанное, можно выделить как минимум четыре основные угрозы процессам и феноменам образовательного пространства:

- следование «догоняющей» стратегии»;
- тренд на универсализацию и «давосскую культуру»;
- отсутствие экспертизы зарубежных образовательных онлайн-форматов;
- пренебрежение к отечественному историческому и культурному прошлому.

Следующая группа угроз относится к информационному давлению и, возможно, позиция авторов покажется спорной.

Аналитики платежной системы «Мир» провели комплексное исследование поколения в возрасте от 14 до 24 лет, что составило около 13% населения страны. Используя методы онлайн-опросов и глубинных интервью аналитики выясняли, чем увлекается поколение, как развивается, что смотрит и слушает, как реагирует на рекламу и расходует средства. Результаты показали, что более 60% или получили среднее специальное, высшее или неоконченное высшее образование, или планируют получить (14–17-летние). Каждый второй в свободное время смотрит каналы блогеров и знаменитостей, а самым часто используемым медиаканалом является YouTube. Две трети заинтересованы в дополнительном обучении, при этом более привлекательными являются иностранные языки, информационные технологии и психология; менее всего – культура и право. Практически половина опрошенных предпочитает онлайн-форматы [20].

В, казалось бы, положительном тренде – желании учиться и саморазвиваться – есть свои риски. К сожалению, инициаторы исследования «Чем живет молодежь» не заинтересовались у младшей

группы опрашиваемых (14–17-летние), какой и почему формат *профессионального* образования предпочтительнее для них – онлайн или традиционный, а они принципиально отличаются, например, в обеспечении важнейших задач образования – духовно-нравственное развитие, воспитание, содействие социализации. Не менее интересно было бы узнать, какие онлайн-курсы и сервисы в большей мере используются для дополнительного образования, т.к. спектр предоставляемых возможностей очень широк – от программ образовательных организаций, построенных в соответствии с существующими стандартами, до марафонов «инфобизнесменов», эффективно визуализирующих «успешный успех».

Широкое распространение онлайн-форматов требует ответа еще на один вопрос: участвуют ли информационные технологии в воспитательном процессе? Следуя общим принципам, которые кратко отражены в высказывании академика РАО А. А. Вербицкого: «компьютер не воспитывает», – не участвуют. Но не следует забывать, что машина не самостоятельна, за ней стоят создатели, политтехнологи, социальные инженеры, обеспечивающие поток дезинформации, пропаганды. И техническое средство, вне зависимости от того, портативное или нет, является проводником мощного информационно-психологического воздействия, оказываемого всеми доступными инструментами открытого информационного пространства, эффективность которого мы признаем. Представляется важным переосмыслить процесс трансформации образовательного пространства, степень влияния на мировоззрение личности информационно-коммуникационных технологий, чтобы разработать способы защиты с учетом «социальных, культурных, технологических процессов и явлений с опорой на традиционные ценности и накопленный культурно-исторический опыт» [17]. Да, в нашем традиционном понимании технологии не

воспитывают, но мы признаем, что влияют на личность, трансформируя ее ценностное восприятие мира и себя в этом мире.

Наверное, за все время существования человечества культурно-цивилизационный фактор впервые стал настолько значимым, и ядро, вокруг которого сегодня строится социальная стабильность государства, в большей мере состоит из двух компонент – культуры и воспитания, отводя в соответствии с нашим отечественным культурным фокусом технологической составляющей важную, но вспомогательную роль.

Такой вывод можно сделать, в том числе проанализировав ряд документов государственного уровня, принятых в конце 2022 – начале 2023 гг.: Указ Президента Российской Федерации «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», Концепцию формирования и развития культуры информационной безопасности граждан Российской Федерации и Концепцию информационной безопасности детей в Российской Федерации.

Все три документа направлены на защиту нашей локальной цивилизации от внешнего агрессивного воздействия в культурно-мировоззренческой сфере и определяют цели и задачи государства и общества в этой области. Особенно следует отметить, что в Концепции информационной безопасности детей в Российской Федерации не только перечислены риски, такие, например, как интернет-манипуляции, способные сформировать у детей и подростков неправильное восприятие традиционных российских духовно-нравственных ценностей, способствующие деструктивному поведению, но и прописана ответственность родителей (законных представителей) за воспитание и духовное и нравственное развитие своих детей. Такой подход позволяет сформировать

преемственность в формировании культурного кода по всей социальной цепочке: родители – система образования – работодатели. В главе, посвященной приоритетным задачам государственной политики в области информационной безопасности детей, данное положение усилено формулировкой: «Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий *при определяющей роли семьи*»³. К числу безусловных достоинств документа относится акцент на «воспитание объективного представления о российской культуре как неотъемлемой части мировой цивилизации» и роль цифровых технологий в этом процессе.

Отметим, обобщая содержание данных документов, что они в полной мере отражают российский культурный фокус и ценности нашей цивилизации, предполагающие «формирование на международной арене образа Российского государства как хранителя и защитника традиционных *общечеловеческих*⁴ духовно-нравственных ценностей», устанавливают права на свободу и доступ к информации и неразрывность жизни современного человека с пребыванием в информационном пространстве, содержат некоторые механизмы противодействия преступлениям с использованием информационно-коммуникационных технологий, а также, не снимая ответственности с государства за обеспечение информационной безопасности, определяют необходимость «согласованного взаимодействия семьи, главного института социализации и воспитания детей, с государством и всеми элементами современного медиарынка».

Вышесказанное позволяет сделать следующие выводы.

³ Выделено авторами.

⁴ Выделено авторами.

- Участники глобального информационного процесса подвергаются агрессивному воздействию технически оснащенных локальных цивилизаций, продвигающих свои ценности, традиции, культуру под лозунгом универсализации.
- Российской идентичности свойственен мультицивилизационный подход, который строится на восприятии нашей цивилизации как одной из многих в составе единой (определяемой периодом времени), на интеграции, уважении и понимании чужой культуры, что не должно исключать «разумного эгоизма» с приоритетом собственных интересов.
- Значимые различия в психическом строе цивилизаций и в культурном фокусе формируются последовательно наследственными накоплениями.
- Культура как действенная категория воспитывается, формируя личность в целостной и логичной последовательности, что накладывает ответственность на все поколения.
- Одной из важнейших задач государства и системы образования является заполнение идеологического и культурного вакуума в информационном пространстве.
- Основным механизмом защиты российского общества от деструктивного информационно-психологического воздействия является воспитание в непрерывном процессе передачи культурного кода, начиная с семьи.
- Трансформация современного образовательного пространства, результатом которого стало создание информационного образовательного пространства, привело к новой категории рисков, требующих детального изучения психолого-педагогическим сообществом и создания механизмов противодействия.
- Информационная безопасность личности в большей мере обеспечивается высоким уровнем культуры, в том числе ин-

формационной, проявляющейся в культуре взаимодействия человека и социума в информационной среде.

- Любые инновации в образовании необходимо оценивать с точки зрения отдаленных последствий для локальных цивилизаций, состоящих из отдельных личностей, неповторимых в границах общего целого [6, с. 5].

Литература

1. Арутюнян Г. Гибридные войны и «триады» цивилизационной безопасности. Ереван: НОФ «Нораванк». http://www.noravank.am/rus/articles/security/detail.php?ELEMENT_ID=22763
2. Бартош А. Гибридная война против культурного кода. Цивилизационная многополярность поменяет векторы в мировом развитии / Независимое военное обозрение. 2020. https://nvo.ng.ru/gpolit/2020-12-24/8_1123_gpolit.html
3. Данилевский Н.Я. Россия и Европа: взгляд на культурно-исторические и политические отношения славянского мира к германо-романскому [Текст] / Н.Я. Данилевский. – СПб.: Глаголь, 1995. – 514 с.
4. Данилевский Н.Я. Горе победителям! [Текст]: сборник статей / Н.Я. Данилевский. – М.: АЛИР, 1998 г. – 416 с.
5. Иванова С.В., Иванов О.Б. Образовательное пространство как модус образовательной политики: монография. М.: ООО «Русское слово – учебник», 2020. 160 с.
6. Ильенков Э.В. Философия и культура. – М.: Изд-во Московского психолого-социального института; Воронеж: Изд-во НПО «МОДЭК», 2010. – 808 с.
7. Кочетков В.В. Культурное измерение гибридных войн // Вестн. Моск. ун-та. Сер. 18: Социология и политология. 2015. № 4. С. 263–267. DOI: 10.24290/1029-3736-2015-0-4-263-267].
8. Лескова И.А. Топология образовательного пространства // Мир науки. Педагогика и психология, 2019 №2. <https://mir-nauki.com/PDF/38PDMN219.pdf>. (доступ свободный)
9. Лунев С.И. Индия в глобализирующемся мире // Глобализация и крупные полупериферийные страны. Научные доклады. Вып. 1. М.: Международные отношения, 2003. С. 172–184.

10. Мартынов В.Г. Транзитная зона цивилизации//Педагогика. 2021.12. № 85. С. 14–25.

11. Нарочницкая Е.А. Национальный фактор в эпоху глобализации // Процессы глобализации: экономические, социальные и культурные аспекты / РАН. ИНИОН. – М., 2000. – 232 с. – (Актуальные проблемы Европы / Редкол.: Пархалина Т.Г. (гл. ред.) и др. 2000. 4.– С. 102–155.

12. Перепелкин Л. С. Цивилизация, империя и региональная интеграция: диалектика понятий / Вопросы социальной теории. Том XI. 2019. С. 65–79.

13. Попов М. Е. Конфликты идентичностей в посттрадиционной России: общероссийский и региональный аспекты. Ставрополь: Изд-во СГУ, 2011. 321 с.

14. Толковый словарь русского языка: в 4 т. / Под ред. Д.Н. Ушакова. Т. 4. – М.: Гос. изд-во иностр. и нац. слов.: ОГИЗ, 1940. – Стб. 1503. <https://ushakovdictionary.ru/about.php>

15. Хантингтон С. Столкновение цивилизаций. Пер. с англ. Т. Велимеева, Ю. Новикова. М.: ООО «Издательство АСТ», 2003, 603 с.

16. Харари Ю.Н. 21 урок для XXI века: [пер. с англ. Ю. Гольдберга]. М.: Синдбад, 2021. 416 с.

17. Указ Президента Российской Федерации № 809 от 9 ноября 2022 года «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».

18. Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации. Утверждена 22 декабря 2022 распоряжением Правительства Российской Федерации № 4088-р.

19. Концепция информационной безопасности детей в Российской Федерации. Утверждена распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р.

20. <https://mir-young.rbc.ru/#content>

*В. М. Жураковский,
академик Российской академии образования,
доктор технических наук, профессор*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТУДЕНТОВ В ИННОВАЦИОННО-ПРЕДПРИНИМАТЕЛЬСКОЙ СРЕДЕ СОВРЕМЕННОГО ВУЗА

Важнейшим направлением развития высшей школы является усиление роли вузов в социально-экономическом и научно-технологическом развитии страны на основе вовлечения университетов в научную сферу и кооперацию с реальным бизнесом и обществом. В программе «Приоритет 2030» и национальном проекте «Наука и университеты» подчёркнута приоритетная направленность развития университетов на реализацию прорывных научных исследований и разработок, внедрение в экономику и социальную сферу высоких технологий, коммерциализацию результатов интеллектуальной деятельности и трансфер технологий, совершенствование научно-исследовательской деятельности, объединение с университетами, научными организациями и бизнесом с формированием консорциумов.

Результатом системной трансформации университетов становится формирование на их базе интегрированной инновационно-предпринимательской экосистемы, позволяющей им стать генераторами технологий и инновационно активных кадров, выполнять функции системного интегратора основных процессов технологического предпринимательства, хаба для эффективного научно-технического взаимодействия с реальным бизнесом и обеспечения технологического трансфера. Сочетание образова-

тельных, научно-инновационных и предпринимательских потенциалов множества заинтересованных участников таких экосистем открывает новые возможности для эффективного сотрудничества, при этом формируемое общее информационное пространство должно обеспечивать бесшовность информационного взаимодействия для акторов экосистемы из сферы образования, науки и профильного бизнеса.

Обеспечение взаимного доступа к информации для вузов, научных организаций и бизнеса предусмотрено утверждённой Минобрнауки РФ «Стратегией цифровой трансформации отрасли науки и высшего образования» [1] во исполнение Указа Президента Российской Федерации от 21 июля 2020 г. N 474 «О национальных целях развития Российской Федерации на период до 2030 года» [2]. Информационные системы развитых экосистем университетов, в том числе консорциумов как формы сетевого взаимодействия для решения актуальных научно-образовательных и предпринимательских задач [3], содержат и обрабатывают масштабные массивы различных данных, связанных с обеспечением учебного процесса, с научно-исследовательскими, проектно-конструкторскими разработками и бизнес-проектами, включая служебную, коммерческую и иную конфиденциальную информацию как вуза, так и его партнёров. В связи с этим возрастает актуальность и сложность проблем обеспечения информационной безопасности, растёт масштаб и ответственность за ущерб от возможных нарушений конфиденциальности, целостности и доступности информации.

Довольно часто, при создании информационной системы, организации стремятся обезопасить свои информационные активы лишь на аппаратном и программном уровнях защиты. Но такой уровень безопасности не является достаточным и должен быть подкреплён нормами и правилами в области информационной

безопасности, а для информационного взаимодействия в рамках научно-образовательных партнёрств и бизнеса – созданием условий информационного обмена между участниками для объединения усилий при создании корпоративных информационных ресурсов и гармонизации правил взаимодействия участников при использовании открытых стандартов. Современная архитектура безопасности, объединяющая сервисы для формирования и реализации согласованной бизнес-политики в масштабе всей распределенной сети партнёрства, принципиально может организационно и технически решить проблемы безопасности [4], однако необходимо учитывать специфику обеспечения защиты информационных активов университета как организации с непостоянной аудиторией и размытым периметром доступа.

В частности, особой и наиболее значительной категорией пользователей, создающих угрозы информационной безопасности, являются студенты, многие из которых достаточно свободно ориентируются в киберпространстве и путём различных, в основном, непреднамеренных поступков и манипуляций могут нанести существенный ущерб и сами подвергнуться репутационной, административной и даже уголовной ответственности. В настоящее время опасность роста угроз, ущерба и ответственности от нарушения информационной безопасности студентами существенно возрастает в связи со следующими обстоятельствами.

Во-первых, в связи с мерами по системному вовлечению обучаемых в научно-инновационную и предпринимательскую деятельность в рамках партнёрств с научными организациями и реальным бизнесом кардинально возрастает доступ студентов к конфиденциальной информации научно-технического и даже коммерческого характера.

В рамках национального проекта «Наука и университеты» и

инициатив Правительства РФ по ускоренному инновационному развитию «Платформа университетского предпринимательства», «Передовые инженерные школы», «Делаем науку в России» и «Университеты 3.0» [5] усиливается участие вузов в кооперации с бизнесом по созданию высокотехнологичных производств, создаются научно-образовательные центры мирового уровня, сеть научных и инжиниринговых центров, 900 современных молодёжных лабораторий. В части развития студенческого предпринимательства предусматривается создание платформы университетского технологического предпринимательства, массовое формирование у студентов предпринимательских компетенций, реализация акселерационных программ поддержки проектных команд, развитие акселераторов, бизнес-инкубаторов и сети стартап-студий, генерирующих технологические стартапы, формирование механизмов грантовой поддержки и привлечение инвесторов к финансированию стартапов на ранних стадиях. Получает развитие проект «Стартап как диплом», позволяющий студентам выходить на предпринимательский трек и по окончании университета продолжать заниматься предпринимательской деятельностью.

Наиболее уязвимыми объектами информационной безопасности в области науки и техники являются результаты фундаментальных, поисковых и прикладных научных исследований, незапатентованные технологии, ноу-хау, промышленные образцы, модели и программные продукты, для которых еще не определен статус конфиденциальности, а также объекты интеллектуальной собственности (открытия, патенты и пр.), которые могут быть незаконно распространены или использованы, несмотря на их правовую защиту. В связи с этим, меры по оценке уровня безопасности информации, авторских прав и других объектов интеллектуальной собственности, способствующие обеспечению защиты интеллектуальных

прав, должны соблюдаться на всех этапах исследований, разработок, публикации, экспертизы и бизнес-реализации создаваемых с участием студентов технологических процессов, технических объектов и наукоёмких производств.

Во-вторых, в последнее время значительно возросло использование смешанного обучения, ставящего студента в положение активного участника образовательного процесса, постоянного пользователя информационного научно-образовательного контента, а использование индивидуальных образовательных траекторий ещё более увеличивает долю самостоятельной работы обучаемых в информационной среде [6]. Развитие методов проектного обучения также стимулирует удалённое общение участников, требует подготовки аналитических материалов, презентаций, научных публикаций, а для прикладных исследований – бизнес-планов, заявок на целевой грант, экспертных и других материалов по созданию стартапа.

В связи с тем, что обучаемые работают удалённо, словосочетание «защита периметра» становится всё менее актуальным. При удалённом общении студенты часто используют общедоступные сети Wi-Fi и другие инструменты, которые зачастую не могут обеспечить действенную информационную безопасность. Домашние офисы менее защищены, чем централизованные, которые, как правило, имеют средства периметровой защиты, поэтому размытые границы между личной и учебной жизнью увеличивают риск потери или искажения конфиденциальной информации. На первый план выходят задачи защиты данных при их передаче по открытым каналам связи, многофакторной аутентификации при использовании личных гаджетов, обеспечения информационной безопасности с использованием аппаратно-программных средств, например, проверки пользователей, гаджетов и приложений путём использования модели «нулевого доверия» (Zero Trust Network Access).

Кроме того, рост активности участия студентов в информационном образовательном пространстве университета и его партнёров сопровождается потенциальными угрозами для безопасного функционирования информационных систем образовательного процесса, сохранения интеллектуальной собственности в виде разработанных в университете учебно-методических материалов в результате несанкционированного доступа к аппаратным объектам, неумышленного уничтожения или модификации данных, непреднамеренного раскрытия конфиденциальной информации. Необходимо отметить также новые возможности для академической нечестности студентов, которой способствует разветвлённая сеть мошеннических компаний и авторов, предлагающих свои услуги через веб-сайты, мобильные приложения и социальные сети [7].

И, наконец, третьей причиной «информационной опасности» студентов можно считать недостаточную сформированность компетентности в области информационной безопасности как компонента их общей информационной культуры [8]. Для большинства студентов, кроме обучающихся по специальностям и направлениям в сфере информационно-коммуникационных технологий, типичными нарушениями онлайн-безопасности являются использование нелегального программного обеспечения и небезопасных веб-сайтов, нерегулярное обновление операционной системы и приложений, неиспользование менеджеров паролей и мер противодействия фишингу, запуск программ, способных вызывать потерю работоспособности или необратимые изменения в информационной системе. При обращении с интеллектуальной собственностью нередко нарушаются авторские права, культура легальности цитирований и заимствований, что влечёт ответственность за плагиат.

Таким образом, в условиях развивающегося системного взаимодействия вузов с научной сферой, инновационным высокотех-

нологичным бизнесом и предпринимательской средой становится актуальным формирование у студентов и выпускников компетенций в области информационной безопасности как обязательного компонента готовности к профессиональной деятельности в современной информационной среде.

Несмотря на разработанность педагогических аспектов подготовки выпускников высшей школы в области информационной безопасности [9, 10], в практической реализации конкретной методической системы наряду с фундаментальным инвариантным содержанием [11] необходимо обеспечивать необходимую вариативность в соответствии с профессиональной направленностью подготовки, учитывать особенности корпоративных ресурсов вуза и его партнёров в части защиты информации, использовать интерактивные технологии и реальные коллективные проекты для формирования способности к безопасной профессиональной коммуникации.

Поскольку современные университеты должны быть инициаторами и полноценными участниками инновационно-предпринимательских экосистем, а также плодотворно взаимодействовать с отраслевыми, территориальными кластерами или системообразующими компаниями, подготовка студентов и выпускников в сфере информационной безопасности должна проводиться в реальных условиях создания, трансфера и коммерциализации объектов интеллектуальной собственности. В этом случае компетентность обучаемых позволит не только избежать ответственности из-за деструктивного поведения в виртуальном пространстве, но и обеспечить их готовность к безопасному использованию информационно-коммуникационных технологий для решения когнитивных, коммуникативных и организационных задач с соблюдением правовых, этических норм и требований информационной безопасности.

Литература

1. Стратегия цифровой трансформации отрасли науки и высшего образования. [Электронный ресурс]. Источник: Режим доступа: <https://minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllr6wtujw.pdf>.
2. Указ Президента Российской Федерации от 21.07.2020 года № 474 "О национальных целях развития Российской Федерации на период до 2030 года". – [Электронный ресурс]. Источник: Режим доступа: <http://www.kremlin.ru/acts/news/63728>.
3. *Лесин С.М., Махотин Д.А.* Консорциум как форма сетевого взаимодействия научных и образовательных организаций для решения масштабных научно-образовательных задач // *Интерактивное образование.* – 2020. – №5–6. – С. 31–34.
4. *Клименко И.С.* Информационная безопасность и защита информации: модели и методы управления. – Москва: ИНФРА-М, 2022. – 180 с.
5. Правительство Российской Федерации: Заседание Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 19 июля 2021 года. [Электронный ресурс]. Источник: Режим доступа: <http://www.kremlin.ru/events/president/transcripts/deliberations/66217>.
6. *Блинов В.И., Сергеев И.С.* Модели смешанного обучения в профессиональном образовании: типология, педагогическая эффективность, условия реализации // *Профессиональное образование и рынок труда.* – 2021. – №1. – С. 4–25.
7. *Иоголевич Н.И., Лободенко, Е.И.* Академическая недобросовестность студентов технического вуза: масштабы проблемы и пути решения // *Педагогика. Вопросы теории и практики.* – 2020. – Т. 5. Вып. 1. – С. 99–106.
8. *Пашков М.В., Пашкова В.М.* Проблемы и риски цифровизации высшего образования // *Высшее образование в России.* – 2022. – Т. 31. № 3. – С. 40–57.
9. *Богатырева Ю.И., Козлов О.А., Поляков В.П., Привалов А.Н.* Методическая система непрерывной подготовки педагогических и управленческих кадров в области информационной безопасности: концепция // *Теоретические и практические аспекты психологии и педагогики: коллективная монография.* Выпуск 17. – Уфа: ООО «Аэтерна», 2017. – С. 27–47.
10. Информационная безопасность личности субъектов образовательного процесса в современном обществе: сб. материалов научно-практической конференции / Авторы-составители: *В.Г. Мартынов, И.В. Роберт,*

И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2022. – 309 с.

11. *Роберт И.В.* Информационная безопасность личности субъектов образовательного процесса// Информатизация образования и науки. – 2019. – № 3 (43). – С. 119–127.

П. В. Кузьмин,

*кандидат педагогических наук,
ректор Федерального государственного автономного
образовательного учреждения дополнительного
профессионального образования
«Академия реализации государственной политики и
профессионального развития работников образования
Министерства просвещения Российской Федерации»*

В. А. Разумовский,

*кандидат педагогических наук,
начальник отдела
Федерального государственного автономного
образовательного учреждения дополнительного
профессионального образования
«Академия реализации государственной политики и
профессионального развития работников образования
Министерства просвещения Российской Федерации»*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В КОНТЕКСТЕ ГОСУДАРСТВЕННОЙ ОБРАЗОВАТЕЛЬНОЙ ПОЛИТИКИ

Образовательная политика, помимо комплекса государственных мер в отношении образования как основного социального института, включает в себя образовательные компоненты и образовательное воздействие других направлений внутренней политики (экономической, социальной, информационной и т.п.), взаимодействие образовательных отношений с основными сфе-

рами жизни общества [2].

Основной вектор современной образовательной политики направлен на достижение технологического и общественного (или мировоззренческого) суверенитета Российской Федерации. Технологический суверенитет при этом понимается как «способность государства обеспечить научно-техническое и промышленное развитие для создания и поддержания на своей территории собственных технологий и инфраструктуры, достаточных для того, чтобы гарантировать независимость своей политики, экономики и обороноспособности от иностранных технологий в критических, жизненно важных сферах» [11]. Общественный (или мировоззренческий) суверенитет – это способность общества к консолидации для решения общенациональных задач, уважение к своим истории, культуре, языку, к народам, которые проживают на территории страны [7].

Значительный вклад в достижение технологического и общественного суверенитета страны вносит российская школа. Как отмечает И. И. Калина «задача формирования и развития технологических знаний и умений школьников обязательно должна идти нога в ногу с воспитательными задачами, задачами формирования отечественно-ориентированного мировоззрения школьников» [3].

Решение основных задач государственной образовательной политики осуществляется в условиях происходящей в стране цифровой трансформации, ставшей уже, по словам заместителя Председателя Правительства Российской Федерации Д. Н. Чернышенко, естественным процессом «наполнения «цифрой» всего того, что нас окружает – дом, транспорт, поликлиника, школа. Неслучайно цифровизацию внесли в число национальных целей развития страны. Она должна сделать жизнь людей комфортнее и

безопаснее, обеспечить конкурентоспособность любой отрасли экономики» [8].

Вслед за И. В. Роберт под цифровой трансформацией образования будем понимать комплекс системных существенных изменений, произошедших и происходящих в сфере образования в связи с активным и систематическим использованием цифровых технологий и реализацией в образовательной практике результатов достижений научно-технического прогресса современного информационного общества массовой глобальной коммуникации. Цифровая трансформация образования, как подчеркивает руководитель научной школы «Информатизация образования», инициирует становление и развитие цифровой парадигмы образования как совокупности теоретико-методологических, гуманитарно-прикладных оснований и технологических решений, ориентированных на реализацию в образовании достижений научно-технического прогресса с необходимостью сохранения здоровья и обеспечения информационной безопасности личности субъектов образовательного процесса [4].

Следовательно, происходящие в общем образовании процессы, направленные на достижение технологического и общественного (мировоззренческого) суверенитета страны, необходимо рассматривать, в том числе, с точки зрения обеспечения информационной безопасности личности субъектов образовательного процесса.

Опираясь на результаты исследований в области обеспечения информационной безопасности личности, представим основные государственные меры, способствующие предотвращению возможных негативных последствий для физического и психического здоровья субъектов образовательного процесса, связанных «с воздействием на пользователя информации, запрещенной законодательством или агрессивной, нелегитимной, неэтичной

информации, или информации, оскорбляющей моральные ценности и чувства пользователя; использованием нелегитимной педагогической продукции, реализованной на базе ИКТ, не отвечающей педагогико-эргономическим требованиям; потерей авторских прав разработчика на результаты интеллектуальной собственности, представленной в электронном виде» [5].

Создание федеральной государственной информационной системы «Моя школа»

Федеральная государственная информационная система «Моя школа» (далее – ФГИС «Моя школа») создана в целях поддержки системы образования и создания благоприятных условий для функционирования системы начального общего, основного общего, среднего общего и профессионального образования [12].

Пользователями ФГИС «Моя школа» являются: обучающиеся; родители (законные представители) обучающихся; педагогические и иные работники организаций, осуществляющих образовательную деятельность; уполномоченные представители Федеральной службы по надзору в сфере образования и науки Российской Федерации (Рособрнадзор), Минпросвещения России, иных органов государственной власти, органов местного самоуправления; юридические и физические лица, в том числе индивидуальные предприниматели, обладающие правами владения, пользования и распоряжения материалами и средствами обучения и воспитания, предоставленными в цифровом виде, включая информационные ресурсы, а также средства, способствующие определению уровня знаний, умений, навыков, оценки компетенций и достижений обучающихся (далее – цифровой образовательный контент), и цифровыми решениями, предоставляющими возможность приобретения знаний, умений и навыков, в том числе

дистанционно, и обеспечивающими автоматизацию образовательной деятельности (далее – цифровые образовательные сервисы), являющиеся поставщиками цифрового образовательного контента и цифровых образовательных сервисов.

К числу задач ФГИС «Моя школа», направленных на обеспечение информационной безопасности личности, включая защиту пользователей от «несанкционированной» информации, можно отнести: обеспечение возможности создания персональных и групповых онлайн-коммуникаций пользователей, в числе которых чаты и видеоконференции; создание профильных сетевых образовательных сообществ; обеспечение возможности проведения профилактической работы с обучающимися.

Среди функций, реализацию которых обеспечивает ФГИС «Моя школа», выделим те, что направлены на сохранение физического и психического здоровья пользователя: работа с библиотекой цифрового образовательного контента (далее – Библиотека ЦОК), в том числе обеспечение возможности использования цифрового образовательного контента педагогическими работниками для подготовки и проведения уроков, а обучающимися – для осуществления самоподготовки путем изучения релевантного верифицированного цифрового образовательного контента; обеспечение защиты информации от неправомерного или непреднамеренного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации, обрабатываемой в ФГИС «Моя школа».

Библиотеку ЦОК отличают следующие особенности: соответствие содержания Федеральным государственным образовательным стандартам (далее – ФГОС) и требованиям, предъявляемым к информационной безопасности обучающихся; соответствие

разделам универсального тематического классификатора, охватывающего темы школьной программы по всем предметам; общедоступность; бесплатный доступ.

Цифровые образовательные материалы, представленные в Библиотеке ЦОК, разработаны командой российских учителей, контент по восьми предметам основного общего образования доступен уже сейчас. Материалы для всех уровней образования будут разработаны до конца 2024 года. Контент в Библиотеке ЦОК постоянно обновляется с учетом пожеланий и рекомендаций учителей, каждый педагог может прислать свое мнение, для чего необходимо выбрать соответствующий урок в Библиотеке ЦОК, нажать в конспекте урока кнопку «Замечания и предложения» и заполнить предлагаемую форму обратной связи [6].

Содержание цифрового образовательного контента проходит трехэтапную экспертизу. Критерии первого этапа: соответствие ФГОС и другим федеральным документам, регулирующим содержание образования; достоверность научных теорий, излагаемых авторами, отсутствие недостоверных, научно неподтвержденных и сфабрикованных фактов; отражение вклада российских деятелей науки, культуры, а также выдающихся изобретателей и инженеров России и др. Критерии второго этапа: отсутствие сведений, направленных на формирование неуважительного отношения к Российской Федерации, ее региональному и политическому устройству; отсутствие информации, побуждающей учащихся к девиантному поведению; отсутствие сведений, направленных на поддержку и (или) оправдание экстремизма и терроризма и т.д. На третьем этапе осуществляется экспертиза на отсутствие вредоносного программного обеспечения в разработанных образовательных материалах.

Экспертами, проводящими анализ цифрового образовательного контента, выступают высококвалифицированные сотрудники

ФГБНУ «Институт стратегии развития образования Российской академии образования», ФГБОУ ВО РГПУ им. А. И. Герцена, ФГБНУ «Федеральный институт педагогических измерений», АО «Лаборатория Касперского».

Организация дополнительного профессионального педагогического образования в области обеспечения информационной безопасности личности

Для консолидации образовательных возможностей участников системы дополнительного профессионального педагогического образования (далее – ДППО), выработки единых подходов к постдипломному педагогическому образованию и развитию профессиональных компетенций педагогов и управленческих кадров формируется Федеральный реестр дополнительных профессиональных программ педагогического образования (далее – Федеральный реестр) [10].

Концентрируя программы повышения квалификации, прошедшие общественно-профессиональную экспертизу, Федеральный реестр является своеобразной «точкой входа» для работников образования, определяющих способ реализации выбранного направления своего профессионального развития. Педагогу, заинтересованному вопросами информационной безопасности, остается только связаться с образовательной организацией, программа которой представлена в Федеральном реестре, и определиться с формой получения образования.

По согласованию с Минпросвещения России, в перечень ведущих тематик дополнительных профессиональных программ Федерального реестра на 2022 год включено направление «Здоровьесберегающие технологии и информационная безопасность обучающихся». По состоянию на 1 декабря 2022 года в Федеральном

реестре размещено 10 программ повышения квалификации в области информационной безопасности личности. Авторами программ являются коллективы организаций ДППО из 8 субъектов РФ.

Развитие предметных телеграм-каналов для педагогических работников

Развитие цифровых технологий и цифровая трансформация способствовали формированию новых механизмов работы с педагогической общественностью. Как справедливо отмечает О. В. Бондаренко, «появление функций создания отдельного канала в мессенджере «Телеграм» фактически дало жизнь новому виду узкопрофильных СМИ в телефоне» [1].

В настоящее время для учителей начальной школы, математики, химии, физики и географии с помощью телеграм-каналов обеспечен доступ к актуальному предметному содержанию, которое заведомо лишено внешней агрессии, не содержит неэтичной или оскорбляющей моральные ценности и чувства пользователей информации. С помощью телеграм-канала до учителей оперативно доводится актуальная информация, в том числе полезные прикладные материалы: новости предметного обучения, анонсы мероприятий и конкурсов, примеры заданий, опыт педагогов и методистов.

Наполнение предметных телеграм-каналов осуществляет Академия Минпросвещения России, которая обеспечивает общедоступный бесплатный доступ к ним по следующим ссылкам:

- география: https://t.me/Academy_geografiya,
- химия: https://t.me/Academy_khimiya,
- физика: https://t.me/Academy_fizika,
- начальная школа: https://t.me/Academy_nachalnaya_shkola,
- математика: https://t.me/Academy_matematika.

Информационно-методическое сопровождение педагогических работников в области обеспечения информационной безопасности обучающихся

В рамках информационно-методического сопровождения педагогов Академией Минпросвещения России разработаны презентации по актуальным угрозам информационной безопасности учащихся и студентов. Материалы включают в себя: теоретические блоки и практические задания; объяснение предмета изучения; историю возникновения, законодательное регулирование, маркеры, по которым можно судить о наличии угрозы; признаки вовлеченности ребенка в опасную информационную среду и степень этой вовлеченности, а также основные способы противодействия и профилактики, основанные на опыте школ, которые уже столкнулись с исследуемой угрозой. Профайлы в социальных сетях собраны из реальных аккаунтов школьников, столкнувшихся с описываемой угрозой и анонимизированы [9].

Материалы предназначены для учителей-предметников, классных руководителей, школьных психологов и социальных педагогов, а также управленческих команд образовательных организаций в ведении Минпросвещения России.

Цикл внеурочных занятий «Разговоры о важном»

1 сентября 2022 года в российских школах запущен масштабный проект – цикл внеурочных занятий «Разговоры о важном», посвященных различным темам, волнующим учащихся [13]. Центральные темы «Разговоров о важном» – патриотизм и гражданское воспитание, историческое просвещение, нравственность, экология и др.

Авторами комплектов методических и интерактивных материалов являются специалисты ведущих федеральных институтов.

В рамках проекта «Разговоры о важном» создан ряд информационных источников, функционирующих на базе информационных и коммуникационных технологий, которые обеспечивают единые ценностно-смысловые ориентиры воспитательной работы, единую систему информирования классных руководителей всей страны, использование единых методических материалов:

- сайт проекта: <https://razgovor.edsoo.ru/>,
- сервис для классных руководителей: <https://apkpro.ru/razgovory-o-vazhnom/>,
- телеграм-канал проекта: https://t.me/razgovory_o_vazhnom/.

Таким образом, в рамках реализации государственной образовательной политики осуществляется комплекс мер, направленный на обеспечение информационной безопасности личности субъектов образовательного процесса, выражающийся:

- в предотвращении использования информации, запрещенной законодательством или агрессивной, нелегитимной, неэтичной информации, или информации, оскорбляющей моральные ценности и чувства пользователя: Библиотека ЦОК, предметные телеграм-каналы, информационная поддержка проекта «Разговоры о важном»;
- в предотвращении использования нелегитимной педагогической продукции, реализованной на базе цифровых технологий, не отвечающей педагогико-эргономическим требованиям, и противодействию потере авторских прав разработчика на результаты интеллектуальной собственности, представленной в электронном виде: ФГИС «Моя школа»;
- в информационно-методическом сопровождении педагогических работников и управленческих кадров, обеспечении дополнительного профессионального образования в области информационной безопасности.

Литература

1. *Бондаренко О.В.* Телеграмм-каналы как новый вид коммуникации с общественностью // Век информации. – 2018. – № 2–2. – С. 170–172.
2. *Ибрагимов Е.М., Ибрагимов М.Г.* Правовое регулирование в сфере образования в контексте государственной образовательной политики // Правовая политика и правовая жизнь. – 2012. – №2. – С. 128–132.
3. *Калина И.И., Чернобай Е.В., Коверова М.И.* Вклад российской школы в формирование технологического суверенитета страны // Образовательная политика. – 2022. – № 2 (90). – С. 42–51.
4. *Роберт И.В.* Дидактика периода цифровой трансформации образования // Проблемы развития дидактики в условиях цифровой трансформации образования: Сборник научных трудов / Авторы-составители В. Г. Мартынов, В. М. Жураковский. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И. М. Губкина, 2022. – С. 30–69.
5. *Роберт И.В.* Психолого-педагогические основания информационной безопасность личности: содержательно-методический аспект // Информационная безопасность личности субъектов образовательного процесса в современном обществе. Коллективная монография/ Авторы-составители: В.Г. Мартынов, И.В. Роберт, И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) им. И.М. Губкина, – 2020. – С. 177–182.
6. Библиотека цифрового образовательного контента [Электронный ресурс] // Академия Минпросвещения России: [сайт]. URL: <https://apkpro.ru/bsook/> (дата обращения: 30.12.2022).
7. Встреча с молодыми предпринимателями, инженерами и учёными [Электронный ресурс] // Президент России: [сайт]. URL: <http://krem-lin.ru/events/president/news/68606> (дата обращения: 30.12.2022).
8. Доклад Дмитрия Чернышенко о текущей ситуации с реализацией инициатив по цифровой трансформации, спорту, а также в сфере науки и образования [Электронный ресурс] // Стратегия 24: [сайт]. URL: <https://strategy24.ru/rf/news/doklad-dmitriya-chernyshenko-o-tekushchey-situatsii-s-realizatsiey-initsiativ-po-tsifrovoy-transformatsii-sportu-a-takzhe-v-sfere-nauki-i-obrazovaniya> (дата обращения: 30.12.2022).
9. Информационно-методическое сопровождение деятельности педагогов. Совершенствование профессиональных компетенций в области цифровой грамотности и информационной безопасности [Электронный ресурс] // Академия Минпросвещения России: [сайт]. URL: https://apkpro.ru/informacionnaya-bezopasnost/?sphrase_id=37820 (дата обращения: 30.12.2022).

10. Концепция создания единой федеральной системы научно-методического сопровождения педагогических кадров: утверждена Распоряжением Минпросвещения России от 06.08.2020 № Р-76 [Электронный ресурс] // КонсультантПлюс (дата обращения: 30.12.2022).

11. Лосев А.В. Ядерная энергетика и технологический суверенитет [Электронный ресурс] // Совет по внешней и оборонной политике: [сайт]. URL: <http://svop.ru/main/26081> (дата обращения: 30.12.2022).

12. Постановление Правительства Российской Федерации от 13.07.2022 № 1241 «О федеральной государственной информационной системе «Моя школа» и внесении изменения в подпункт «а» пункта 2 Положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» [Электронный ресурс] // Официальный интернет-портал правовой информации: [сайт]. URL: <http://publication.pravo.gov.ru/Document/View/0001202207150030?index=0&rangeSize=1> (дата обращения: 30.12.2022).

13. Цикл внеурочных занятий «Разговоры о важном» // Разговоры о важном: [сайт]. URL: <https://razgovor.edsoo.ru/> (дата обращения: 30.12.2022).

Д. А. Гаврилов,

преподаватель кафедры геополитики и устойчивого развития общества Российского государственного университета нефти и

газа (национального исследовательского университета)

имени И.М. Губкина,

член Союза писателей России

ОБ УГРОЗАХ ОТЕЧЕСТВЕННОМУ ОБРАЗОВАНИЮ В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Если рассматривать цифровизацию современного образования как исторически закономерный и объективный процесс развития систем с точки зрения теории решения изобретательских задач (ТРИЗ) [1; 2], например, увидим, что благодаря внедрению цифровых технологий снижается роль вещественных ресурсов, в частности, печатных учебных изданий и помещений, и повышается роль ресурсов полевых: наличие устойчивой коммуникационной связи, электричество, Интернет, электронный видео- и аудио- контент и проч. Вещественно-полевые ресурсы (ВПР) системно развиваются по закону повышения степени вепольности систем. Одним из критериев, используемых в ТРИЗ, является логический оператор РВС («размер – время – стоимость»). Размер устройств, используемых в процессе обучения, стремится к нулю – как средств мобильной коммуникации, так и учебных экспонатов (включая целые пространства) – их заменяют собой цифровые модели и электронные муляжи. Всё это приводит к снижению затрат на время образовательного процесса, а стоимость не только устройств для участия в цифровых процессах, но и самих программ, будет падать. Но хорошо ли это для целей воспитательных?

Безусловно, воспринимать «размер» столь механистически было бы неверным – сам основатель ТРИЗ Г. С. Альтшуллер понимал под этим термином скорее «прилагаемые усилия». Цифровизация образовательных процессов создаёт у учащегося соблазн быстрого поиска и копирования готовых решений без их системного и критического осмысления, что не удивительно при наличии в его руках технологии и отсутствии того, что называется достойной целью и жизненной стратегией творческой личности [3], которой Г. С. Альтшуллер уделил последние десять лет жизни, фактически прекратив совершенствовать сервис ТРИЗ. Потребители высоких технологий словно и не обязаны иметь высокие устремления. И это серьёзная угроза!

Учащийся, как один из субъектов современного образовательного процесса, идёт по пути наименьшего сопротивления, пользуется излишними удобствами (цифровыми сервисами) там, где в прежние времена надо было затратить усилия и время (впрочем, вместе с этим получить и удовольствие от результата). Чрезмерная доступность информации с помощью цифровых технологий обесценивает её. Так и при развитости поисковых систем происходит обесценивание эрудиции, алгоритмизация приводит к купированию творческого типа мышления. Без мобильного инструментария учащийся теряет (и это воспринимается уже как норма), поскольку не может добраться технически до цифровой реальности, где считает себя и безнаказанным (самым хитрым), и всемогущим, если привык к тем или иным играм, заменяющим ему действительность, в которой он пока ничего не стоит.

Если проводить аналогии, то звучавшая в детском фильме 1970-х годов Леонида Нечаева «Про Красную Шапочку» песня Юлия Кима с приблизительно таким диалогом главной героини и избалованного ребёнка – мысленный эксперимент: «– А вдруг, ты

завтра попадёшь на остров в океане? – На остров? Вот здорово! – А как же ты там проживёшь без повара, без няни? – А я велю разжечь костёр... – Но мы-то знаем, что этот остров необитаем. – А я пойду, топор найду...» сегодня имела бы иной текст: «А я пойду, найду телефон и позвоню в службу спасения. – И как же ты проживёшь без «гаджета»?». Лишившись в какой-то момент цифровых удобств, будь то долговременное отключение электричества из-за аварии или диверсии, вспышка на солнце, иная чрезвычайная ситуация, тот, кто привык к цифровым удобствам как данности, станет беспомощным, растерянным и озлобленным, или психически больным существом, у которого отобрали любимую игрушку.

Стимул так называемого поколения Z зачастую заключается в том, чтобы быстрее отделаться от учебных заданий нахождением готовых ответов и заняться игрой или более приятными делами, и утверждение себя в сетевом мире посредством цифровых технологий – своего рода лакомство.

Добыча информации, увы, не тождественно добыче знания. Сведения? Да! Можно получать самые разные. И их обилие порождает эффект ложного обладания знанием без особых умственных усилий.

Цифровизация образования ведёт к нарушению связи между физиологией человека и его мышлением. Не следует забывать о научно обоснованной орудийной сущности языка и речи. Развивая речь и язык, мы развиваем наше мышление, и наоборот. Но неречевой характер цифровых технологий при всей их эффективности сродни феномену математического мышления. Давая личные имена вещам, мы воздействуем на мир. Этому основополагающему моменту уделялось внимание прежде [4–6] и теперь отводится существенное место в учебной дисциплине «Основы системного и критического мышления» [7].

Цифровизация давно шагнула за пределы образовательных процессов. Присваивая вещам и людям включительно инвентарные номера, мы их пересчитываем. Сама действительность руками чиновников, которые поступают по тому же принципу наименьшего сопротивления и удобства, истребляет в нас человеческое. За примером далеко ходить не надо. Названия веток московского метрополитена давно превратились в цифры. И если иной москвич под пятьдесят и старше ещё помнит, что Калужско-Рижская линия – оранжевая, а Горьковско-Замоскворецкая – зелёная, поколению Z проще запомнить именно номера...

Сиюминутность чувств, моментальность обмена смсками и сообщениями в чате в виде «смайлов», в результате – несерьёзность всяких отношений в жизни... Ценность родства, когда отец советует сыну, а мать – дочери, нивелируется влиянием сетевых манипуляторов, собравших просмотры и «лайки». И молодой человек устремляется вслед за блогером, ежечасно утверждая своё присутствие на планете сбором виртуальных поощрений, чтобы не отстать, а то и превзойти «звёзд интернет-пространства». А прежде телеграммы и письма ждали «всю жизнь» и, главное, старались быть, а не казаться!

Можно стать высококвалифицированным цифровиком, владеть всеми современными технологиями, но при этом оставаться безнравственным человеком. Нравственность воспитывается в обществе, но что может быть воспитано, если общение в виде полноценной устной и письменной речи целенаправленно сведено к нулю как по форме, так и по содержанию.

К какому идеальному конечному результату (ИКР) приходит общество в результате таких преобразований? К отсутствию человека как духовности, как нравственной личности вообще, в том числе, к отсутствию преподавателя и педагога, чьи функции

делегированы программе, в лучшем случае, они возложены на цифрового двойника, цифровую запись. Нет полной гарантии при всех ухищрениях, что и другая сторона – обучаемый – является по ту сторону образовательных дистанционных цифровых процессов той же самой личностью, чьё имя будет прописано в дипломе о высшем образовании. Цифровое пространство уравнивает преподавателя и учащегося, человека, который чего-то добился в жизни сам, и человека, который прошёл тот или иной уровень виртуальной игры в «Танки», но «не нюхал пороха» и выбрал себе университет, чтобы благодаря военной кафедре избавиться от необходимости защищать Отечество в яви.

Так является ли повальная цифровизация панацеей или это очередная продуманная антисоциальная диверсия, направленная на подрыв духовно-нравственных основ традиционного отечественного образования? Вспомним: сперва были «интернационализм» и «коллективизация», потом – «развитой социализм» с «экономной экономикой», именуемые конкурентами застоём, наконец, новое «мышление», плюрализм, гласность, перестройка, ускорение (развала страны), приватизация и рыночные реформы, атипичная пневмония, птичий и прочий грипп, информатизация и инновации, QR код и ковид, теперь наше ключевое слово «цифровизация». Модное слово становится чем-то вроде спекулятивного товара «крышка», если вспомнить многосерийный фильм «Цыган» и «божественную Тамилу», поведавшую цыганской диаспоре о хите нового сезона. Не имеем ли мы дело с очередной масштабной манипуляцией общественным сознанием?

Наличие под рукой «гаджета» избавляет от необходимости запоминать вживую не только телефоны друзей и знакомых, но и просто разрушает память пространственную. Как иностранный таксист не ориентируется в чужом городе, полагаясь на спутни-

ковый навигатор или подсказки местного пассажира, так и молодой человек беспомощен без сервиса по выстраиванию маршрута. Ему нет необходимости отягощать себя «лишними» приметами, смотреть по сторонам, держать в памяти образы зданий, скверов, бульваров, аллей, памятников культуры. Что уж думать о заблудившемся в лесу представителе поколения Z (да, похоже, и Y), не ведающем компаса? Надо дожидаться восстановления спутниковой связи или достать из подпространства «бесконечнозарядный» дрон со столь же «вечным» андроидом?

Осенью 2022 года группа преподавателей дисциплины «Основы системного и критического мышления» в ходе семинаров провела тестирование более 440 первокурсников (16 учебных групп разной специализации) на пространственное воображение. Молодым людям предлагалось за 15 минут набросать на листе бумаге максимальное число трёхмерных фигур, соответствующих заданному виду сверху. Девушки показывали лучший результат, чем юноши, как в плане аккуратности прорисовки, так и по числу предложенных вариантов. Но при подведении итогов выяснилось, что абсолютное большинство не способно сделать простейший чертёж от руки. Такое невозможно было представить несколько десятилетий назад в политехническом вузе. Конечно, можно возложить ответственность на образование школьное, также цифровизованное, приписав ему же снижение когнитивных функций. Конечно, кульман и ватман уже отошли в область архаической инженерной культуры – программа за нас всё чертит, а принтер распечатывает, но стоит ли перекладывать одну и ту же проблему с одной больной головы на другую.

Начертательная геометрия, по мнению величайшего античного учёного Платона, формировала мышление. Поэтому он и начертал пред садами своей Академии: «Пусть не входит сюда тот, кто не

знает геометрии». Похоже, сейчас эта надпись звучала бы так: «Да не войдёт в этот вуз тот, кто обходится без цифровизации». Автор считает, что диалектику Платону стоит верить, хотя формалист Аристотель, его ученик, рассуждал иначе.

Другой тест (наглядно иллюстрирующий отмеченный выше неречевой характер цифровизации) на той же аудитории показал, что учащиеся с трудом владеют даже азами родной речи. Они не в силах самостоятельно (без подглядывания в вездесущий поисковик) подобрать к понятиям хотя бы несколько синонимов и антонимов, и вроде бы нацеленные по специальности на поиск и анализ информации, не ведают о полисемантической природе языка. Хотя при клипово-комиксном характере сетевых текстов этому ведению взяться неоткуда.

Является ли «цифровизация» истиной в последней инстанции, или через пару-тройку лет появится новый спасительный рецепт и откроется очередное волшебное слово. По мнению автора, хотя переход к очередному экономическому укладу является объективным историческим процессом, это не повод для личности в частности, а для общества в целом, становиться объектом экспансии внедрённых технологий и служить их придатком, утрачивая чувство меры.

Многие из читающих эти тезисы получили прекрасное высшее образование безо всякой «цифровизации» и «информатизации» и не стали заложниками развернувшихся (или нарочно развёрнутых?) процессов. Закономерен вопрос: высшее образование мы подстраиваем под запросы и удовольствия (лакомства) поколения Z, или это поколение должно подстраиваться под неудобные ему, но выстраданные опытом поколений требования тех, кто видел в жизни что-то больше, чем экран монитора или гаджета. Конечно, играло роль и то, что высшее образование ранее не рассматрива-

лось как оказанная услуга, и то, что наши наставники по призванию оттачивали методологическое мастерство, не обладая костылями современных технологий.

Надо сохранять и активировать свою «субъектную сущность» и осмысленно управлять происходящим, не пуская цифровизацию образовательных процессов на самотёк. Нельзя ссылаться на их историческую неизбежность и объективную реальность, важно не допускать подмены самого образования – как содержания – цифровой формой ради формы, большего эффекта, впечатлений от лишённых полезного функционала электронных украшательства.

Обучение цифровым технологиям не должно предшествовать классической системе отечественного образования. Воспитание личности является более важной функцией, чем овладение навыками пользования всевозможными устройствами, базирующимися на таких технологиях. Автор не является «луддитом», но полагает, что возникшее противоречие между духовно-нравственными аспектами и техническими удобствами, к которым приучаются с юности, надо разрешать во времени и в пространстве. И это тот случай, когда следует заранее ограничивать всё, что обеспечивает привыкание к удобствам, уже хотя бы ради будущей безопасности общества и государства.

Происходящая в условиях внедрения цифровых технологий утрата прежних производственных технологий и просто полезных житейских навыков породила необходимость ремонта утраченных знаний, что уже не всегда возможно [8]. Прежде, чем поощрять использование всевозможных цифровых сервисов, следует просчитать вред, который это может нанести обществу, включая «техно-оптимизм молодёжи как идеологию скрытого технорабства» [9]. Хорошим подспорьем может стать диверсионный анализ, используемый в той же ТРИЗ.

Уравновесить вред необходимо, хотя бы изредка возвращая поколение Z в доцифровое пространство-время, погружая его в такую чрезвычайную для психики неподготовленного ситуацию, когда нет ни мобильной связи, ни Интернета, ни компьютера. Вместо насаждения и культивирования сетевых сервисов от них необходимо отучать, как наркозависимых. Например, специалистов по комплексной безопасности в целях повышения квалификации надо учить обходиться и делать своё дело без цифровых удобств, чтобы в сложный момент они не расписались в собственной беспомощности при отсутствии информационно-технологических удобств на руках.

Литература

1. *Альтиуллер Г.С.* Творчество как точная наука: Теория решения изобретательских задач. – М.: Советское радио, 1979. – 175 с.
2. *Михайлов В.А., Андреев Е.Д., Желтов В.П.* Основы теории систем и решения творческих технических задач. – Чебоксары: Чувашский университет, 2012. – 387 с.
3. *Альтиуллер Г.С., Вёрткин И.М.* Как стать гением: Жизненная стратегия творческой личности. – Мн.: Беларусь, 1994. – 479 с.
4. *Ёлкин С.В., Гаврилов Д.А.* Сильное мышление как результат диалектически выстроенного языка / Материалы IV Международной научно-практической конференции «Непознанное. Традиции и современность» 18 октября 2014 г. // Информационно-аналитический вестник «Аномалия». – 2014. – № 4. – С. 25–29.
5. *Ёлкин С.В., Гаврилов Д.А.* Как проверить гипотезу Сепира–Уорфа: приглашаем к эксперименту // Информационно-аналитический вестник «Аномалия». – 2015. – № 2. – С. 46–48.
6. *Гаврилов Д.А., Ёлкин С.В.* Избранные лекции по курсу «Начала сильного мышления». Часть 2: Алгоритмические и супероператорные методы решения изобретательских задач / Фонд содействия технологиям XXI века. – М.: Издатель Воробьёв А.В., 2018. – С. 70–87.
7. *Вассерман А.А., Гаврилов Д.А., Воробьёв А.В.* и др. Системное и кри-

тическое мышление / Под общ. ред. А.А. Вассермана; сост.: Д.А. Гаврилов, А.В. Воробьев / Факультет комплексной безопасности ТЭК РГУ нефти и газа (НИУ) имени И.М. Губкина. – М.: Центр стратегической конъюнктуры, 2021. – С. 211–228.

8. Егоров В.А. Эволюция знаний и технологий: естественный и искусственный отбор // PHILOSOPHIA. – 2022. – № 1 (13). – С. 50–58.

9. Макаренков М.А. Вы хотите быть биороботами? Технооптимизм, как идеология скрытого технорабства // EXPERIMENTUM — 2021: Сборник научных статей философского факультета МГУ / Философский факультет МГУ имени М.В. Ломоносова; под ред. А.В. Воробьева. – М., 2022. – №17. – С. 30–37.

*Ю.Д. Алашкевич,
академик Российской академии образования,
доктор технических наук, профессор*

*Л.В. Юртаева,
кандидат технических наук, доцент*

*Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева*

ОСНОВЫ ОТЕЧЕСТВЕННОГО ОБРАЗОВАНИЯ И ГУМАНИТАРНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНИЧЕСКОМ ВУЗЕ

Повсеместное использование цифровых технологий, таких как искусственный интеллект (ИИ), машинное обучение, большие данные, облачные вычисления, цифровое моделирование, дополненная реальность и т.д. приводят к тому, что личность все чаще становится не защищенной от воздействия на ее сознание и подсознание информации, причиняющей вред здоровью и (или) физическому, психическому, духовному, нравственному развитию. От наполненности информационного пространства духовно-нравственным и культурным содержанием во многом зависит передача ценностей и норм подрастающему поколению как наиболее активному потребителю информационных услуг [1]. В условиях становления цифрового общества одним из основных требований безопасности человеческой жизни и важной отраслью науки является информационная безопасность.

Существуют различные взгляды на понятие информационной безопасности, так, например:

- в ГОСТ Р ИСО/МЭК 27000:20012 это «сохранение конфиденциальности, целостности и доступности информации. Кроме того, сюда могут быть включены и другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность» [2];
- в Национальном глоссарии по обеспечению информации – это «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения с целью обеспечения конфиденциальности, целостности и доступности» (CNSS, 2010) [3];
- в глоссарии терминов ISACA – «гарантирует, что только авторизованные пользователи (конфиденциальность) имеют доступ к точной и полной информации (целостность), когда это необходимо (доступность)» (ISACA, 2008) [4];
- Д. Л. Пипкин рассматривает термин информационной безопасности как процесса защиты интеллектуальной собственности организации [5];
- с точки зрения Х. Вентера и М. Элоффа – это защита информации и минимизация риска раскрытия информации неавторизованным сторонам [6];
- С. Голд полагает, что «это междисциплинарная область обучения и профессиональной деятельности, которая связана с разработкой и внедрением механизмов безопасности всех доступных типов (технических, организационных, человеко-ориентированных и правовых) с целью сохранения информации во всех ее местах (внутри и вне периметра организации) и, следовательно, информационные системы, в которых создается, обрабатывается, хранится, передается и уничтожается информация, свободная от угроз» [7];

- согласно Федеральному закону № 436–ФЗ от 29.12.2010 «О защите детей от информации, причиняющей вред их здоровью и развитию» информационная безопасность – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [8].

Анализ рассмотренных определений показывает, что актуальный состав целей безопасности включает в себя: конфиденциальность, целостность, доступность, приватность, подлинность и надежность, неотказуемость [9]. Нельзя исключать и возможность использования изменений и деформаций информационной среды в качестве специфического информационного оружия для достижения политических, экономических, военных и других целей, влияния угроз такого характера на государственную и социальную безопасность через воздействие на менталитет людей. Все сказанное подчеркивает комплексность проблемы обеспечения информационной безопасности, при решении которой должны рассматриваться задачи:

- технологического характера: угрозы развитию отечественной информационной и коммуникационной индустрии (включая средства информатизации, телекоммуникации и связи), обеспечению потребностей внутреннего рынка и выходу на мировой рынок, а также накоплению, сохранности и эффективному использованию отечественных информационных ресурсов [10];
- правового характера: угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

- гуманитарного характера: проблемы обеспечения безопасности индивидуального, группового и массового сознания. Формирование культуры информационного общества. Социально-психологические последствия широкого использования современных информационных технологий во всех сферах жизни общества.

Обеспечить информационную безопасность можно с помощью следующих инструментов:

- всеобщая информационная грамотность;
- готовность к информационному противоборству;
- готовность к отражению информационной агрессии.
- духовно-нравственное развитие массового и индивидуального сознания граждан;
- организационно – педагогические условия создания для обучающихся гуманитарно-ориентированных ситуаций в образовательных организациях.

Так, например, для того, чтобы в процессе изучения курса «Теория и конструкция машин и оборудование отрасли» реализовать гуманитарно-ориентированные ситуации, необходимо:

- провести всесторонний анализ будущей профессиональной деятельности и исследовать смежные области. Выявить методы, подходы и приемы, применяемые к решению возникающих профессиональных задач; определить, из каких областей науки и техники заимствованы используемые приемы и понятийный аппарат;
- определить основные разделы, темы, понятия данного предмета, способы обработки информации и методы решения задач, предоставляемые данной дисциплиной. При этом тематика разработанных преподавателем заданий должна касаться

гуманитарно-ориентированных проблем;

- выделить в каждом отдельном курсе разделы, темы, понятия и методические приемы, базовые для других дисциплин и профессиональной деятельности, и организовать курс так, чтобы взаимосвязь его с другими предметами стала очевидной;
- построить взаимосвязь с гуманитарными дисциплинами, такими как инженерная психология, история, философия, иностранный язык, прикладная экология и социология и т.д.;
- направить процесс обучения не только на приобретение обучающимися умений моделировать и рассчитывать проектируемое оборудование, но и учитывать возможные последствия его функционирования, особенно отрицательные (изменение под воздействием новой техники среды и природы, изменение деятельности и инфраструктур, «антропогенные изменения»);
- сформировать освоение студентами личностно-ориентированной инженерной деятельности через моделирование различных социально-гуманитарных (экологических, правовых, этических и др.) аспектов инженерного проектирования, посредством задач, адекватное решение которых невозможно вне гуманитарной ориентировки и экспертизы;
- представить алгоритм решения гуманитарной задачи в виде последовательного проведения экспертизы предполагаемого технического решения: нормативной (соответствие технического решения социокультурным нормам), социотехнической (экспликация гуманитарного решения на техническое) и принятие обоснованного решения [11];
- активизировать познавательную деятельность студентов через решение задач прикладной направленности с целью обеспечения активной отработки и закрепления различных понятий, навыков расчетов для более осмысленного понима-

ния сути технологических процессов;

- увеличить плотность потоков информации путем отбора содержания учебного материала профессиональной направленности и внедрения в учебный процесс активных методов обучения;
- оптимизировать профессионально-творческую подготовку студентов углублением мотивации профессиональной деятельности будущих инженеров. Опираясь на мотивы познавательной деятельности студентов, педагог должен развивать их интерес к предстоящей педагогической работе, показать её значимость для будущей профессии, воспитать ответственность за успешное выполнение и решение поставленных образовательных задач.

Преподаватель должен спроектировать весь ход занятия, причем вся информация должна быть в поле зрения самого преподавателя в качестве ориентира в организации деятельности обучающихся. Ни сама проблема, ни гипотезы, ни методы исследования творческой, поисковой деятельности не должны быть предоставлены обучающимся в готовом виде. Направляя мысль обучающихся в нужное русло, преподаватель подводит их к самостоятельным выводам о правомерности выдвинутых гипотез, проблем или их ошибочности с обязательностью аргументации точки зрения доказательствами, фактами [12].

Готовность преподавателя к работе в условиях личностно-ориентированного образования предполагает [13, 14]:

- сформированность представлений о смысле и назначении инженера в современном мире;
- наличие культурного мышления, как способности к пониманию и приятию различных типов культур (технической и гуманитарной);

- наличие собственной модели гуманистической ориентации преподаваемого учебного предмета и выявления его нравственных, этических, гражданских, правовых и других гуманистических аспектов;
- знание критериев гуманизации технического образования и их использование в повседневной деятельности;
- владение современными личностно ориентированными образовательными технологиями.

Несмотря на то, что комплексность проблемы информационной безопасности предусматривает решение задач общего характера (права человека, угрозы отечественной индустрии, защита информации и локального информационного пространства, гуманитарные аспекты и т.д.), для университетов технических направлений подготовки есть своя специфика. В частности, в техническом Вузе необходимо:

- учитывать из каких областей науки и техники заимствованы приемы и понятийный аппарат;
- выстраивать взаимосвязь между гуманитарными и инженерными дисциплинами;
- оптимизировать профессионально-творческую подготовку студентов углублением мотивации к профессиональной деятельности будущих инженеров.

Литература

1. Самыгин С.И. Социальная безопасность России в условиях информационной реальности: Монография. – М.: Русайнс, 2016. – 154 с. URL: https://bstudy.net/611937/sotsiologiya/sotsialnaya_bezopasnost_rossii_usloviyah_informatsionnoy_realnosti
2. ГОСТ Р ИСО/МЭК 27000:2012. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной

безопасности. Общий обзор и терминология, 2013. – URL: <https://docs.cntd.ru/document/1200102762>

3. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

4. ISACA. (2008). Glossary of terms, 2008. Retrieved from <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>

5. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.

6. Venter, H. S.; Eloff, J. H. P. (2003). A taxonomy for information security technologies. Computers & Security. 22 (4): 299–307. doi:10.1016/S0167-4048(03)00406-1

7. Gold, S (December 2004). Threats looming beyond the perimeter. Information Security Technical Report. 9 (4): 12–14. doi:10.1016/s1363-4127(04)00047-0. ISSN 1363-4127.

8. Федеральный закон № 436–ФЗ от 29.12.2010 «О защите детей от информации, причиняющей вред их здоровью и развитию».

9. Cherdantseva Y. and Hilton J. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013).

10. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие. – М.: Гелиос АРВ, 2006. – 528 стр.

11. Петрунева, Р. М. Гуманитаризация инженерного образования: На основе моделирования социогуманитарной экспертизы технических решений. Дис. ... докт. пед. наук: 13.00.08 – Волгогр. гос. пед. ун-т., 2001. – 336 с.

12. Буракова Г.Ю. Гуманитаризация процесса обучения [Текст] / Г.Ю. Буракова. – М.: Просвещение, 2001. – 59 с.

13. Дутова А.Ю., Юртаева, Л.В., Алашкевич, Ю.Д. Развитие профессиональной культуры у студентов как фактор повышения конкурентоспособности будущего выпускника / Дутова А.Ю., Л.В. Юртаева, Ю.Д. Алашкевич. Молодые ученые в решении актуальных проблем. – ВНИПК. – Красноярск, 2012. – С. 153–155.

14. Алашкевич, Ю.Д., Кутовая, Л. В. Применение гуманитарных знаний в дисциплинах профессионального цикла / Ю.Д. Алашкевич, Л. В. Кутовая. Современное образование в условиях реформирования: инновации и перспективы: Материалы III всероссийской научно-практической конференции. – Красноярск, 2012. – С. 56–61.

А.Л. Димова,

доктор педагогических наук, доцент,

старший научный сотрудник

АНО институт непрерывного образования «Профессионал»

ПОДГОТОВКА ЛИЧНОСТИ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОХРАНЕНИЮ ЗДОРОВЬЯ В УСЛОВИЯХ СОЦИАЛЬНО- ИНФОРМАЦИОННОГО ДАВЛЕНИЯ НЕДРУЖЕСТВЕННЫХ СТРАН

События последних месяцев показывают, что проводимая нашей Родиной специальная военная операция (СВО) сопровождается беспрецедентным социально-информационным давлением недружественных нам стран на общество в целом и, в частности, на молодежь, практически функционирующую в информационной среде (в сети Интернет и т.п.).

Как отмечают специалисты в области информатизации образования (О. А. Козлов, И. Ш. Мухаметзянов, В. П. Поляков, И. В. Роберт, Г. Ю. Яламов и др.), в информационной среде молодое поколение подвергается воздействию «агрессивной информации со стороны сетевых источников информации, информации порталов, веб-ресурсов, интернет-рекламы товаров и услуг, интернет-сообществ, распространяющих запрещенную законодательством или нелегитимную информацию» [11]. В Национальной стратегии действий в интересах детей на 2012–2017 годы констатируется, что «достигнутый сегодня уровень развития высоких технологий, открытость страны мировому сообществу привели к проблеме незащищенности детей от противоправного контента в

информационно-телекоммуникационной сети интернет, усугубили проблемы, связанные с торговлей детьми, детской порнографией» [11].

В то же время следует заметить, что в условиях проведения СВО многократно усилилось воздействие негативной информации, наносящей вред здоровью, а также фейков, дестабилизирующих моральное состояние молодого человека, провоцирующих панические настроения в молодежной среде. Кроме того, уже само активное, бесконтрольное использование цифровых технологий в местах проживания и пребывания приводит к негативным последствиям психолого-педагогического и медицинского характера для здоровья пользователей. Авторы также отмечают неэффективность мер, предпринимаемых в образовательных организациях по их предотвращению и нейтрализации [9, 12].

Вышеизложенное свидетельствует о необходимости формирования личности – патриота, всесторонне подготовленного к предотвращению рисков социально-информационного давления недружественных стран. В сложившихся условиях всесторонняя подготовка обучающейся молодежи должна включать: патриотическое, военное, физкультурно-спортивное и трудовое воспитание. Учитывая, что полем военных действий становится и информационное пространство, проблема разработки комплексной программы подготовки личности к владению передовыми технологиями (индивидуальными) обеспечения информационной безопасности и обеспечения безопасности собственного здоровья в условиях использования средств ИКТ, требует незамедлительного решения на всех уровнях отечественного образования.

Анализ научных источников [1, 7, 8] показывает, что начиная с 1990-х гг. развитие отечественного образования характеризуют такие негативные процессы, как: кризис российской гражданской

идентичности; тенденция к ухудшению здоровья обучающихся, сопряженная с негативными проявлениями использования цифровых технологий и снижением мотивации студентов к занятиям физической культурой и спортом; утрата достижений отечественной педагогики советского периода (начальной военной подготовки, трудового воспитания в школах, медицинского обеспечения обучения и физиологически обоснованной организации физического воспитания в вузах) и др.

Однако следует отметить, что в последние годы активизировались исследования, посвященные вопросам обеспечения информационной безопасности личности и сохранения здоровья пользователя средствами ИКТ. Ведущие специалисты в области информатизации образования отмечают «необходимость обеспечения информационной безопасности личности субъектов образовательного процесса, использующих в своей деятельности средства ИКТ» [11]. Они указывают на тот факт, что, например, подготовка бакалавров педагогических специальностей в области информационной безопасности реализуется только в рамках дисциплины (модуля) «Безопасность жизнедеятельности», в тематическом плане которой на тему «Основы информационной безопасности» отводится всего 6 академических часов. При этом отмечается целесообразность незамедлительного включения в состав учебных планов особенно актуальной профессионально-ориентированной дисциплины «Информационная безопасность личности» [10, 11].

Так, по итогам освоения дисциплины «Информационная безопасность личности», студенты в том числе приобретают знания о «признаках агрессивной информации, информации, оскорбляющей моральные ценности и чувства пользователя, а также умения применять методы и средства защиты своей информационной

сферы (аутентификация и идентификация пользователей и технических средств, организация защиты информации в персональных компьютерах, криптографическое преобразование информации и электронная подпись)» и др. [10].

Что касается обеспечения безопасности здоровья обучающихся – пользователей средствами ИКТ, то в последние годы выделилось и активно разрабатывалось направление научных исследований «Возможные негативные последствия использования средств информационных и коммуникационных технологий» [9, 12]. В ходе теоретических исследований в Институте стратегии образования Российской академии образования (ИСРО РАО) данное направление получило дальнейшее развитие, приобрело более широкое значение и получило название «Предотвращение негативных последствий использования информационных и коммуникационных технологий для здоровья обучающихся (ПНПЗО)» [5].

При проведении исследований подготовка бакалавров педагогических специальностей в области ПНПЗО была определена в качестве наиболее эффективной меры по обеспечению безопасности и сохранности здоровья обучающихся – пользователей средствами ИКТ. Обоснована целесообразность организации предложенного нами курса подготовки будущих учителей в данной области в рамках элективных дисциплин по физической культуре и спорту, разработано его учебно-методическое обеспечение [4].

В ходе подготовки у будущих учителей формируется способность «создавать и поддерживать средствами ИКТ безопасные для здоровья пользователей условия обучения». Студенты приобретают: теоретические знания в области ПНПЗО; умения оценивать и выявлять негативные последствия использования средств ИКТ для здоровья, реализовывать общие правила и меры их

предотвращения в образовательной деятельности; навыки самостоятельной реализации средств, нейтрализующих данные негативные последствия, а также способов самоконтроля и самооценки показателей здоровья в условиях использования технического оборудования и диагностических комплексов в оздоровительно-физкультурных центрах и кабинетах здоровья; мотивы, установки: на бережное отношение к здоровью; на применение средств, способов, мер по предотвращению и нейтрализации негативных последствий использования средств ИКТ; на обогащение опыта предотвращения рисков для здоровья обучающихся с использованием самих средств ИКТ [4].

В школах, колледжах подготовку в области ПНПЗО предлагается организовывать в рамках: самостоятельного курса или теоретических занятий в данной области, встроенных в учебную дисциплину «Физическая культура» для учеников средних и старших классов, студентов колледжей; вводных теоретических занятий, бесед по дисциплинам «Технология», «Физическая культура» для учеников младших классов; школы родителей онлайн.

Вместе с тем, в силу ряда причин наиболее успешной может оказаться практика внедрения курса подготовки в области здоровьесбережения или отдельных его аспектов, которая будет реализовываться в рамках дисциплин по выбору для студентов – будущих учителей информатики.

Во-первых, вопросы, посвященные негативному влиянию средств ИКТ на здоровье обучающихся, а также мерам, реализуемым в образовательных организациях по обеспечению безопасности здоровья пользователей, беспокоят учителей информатики и привлекают их пристальное внимание. Педагоги отмечают случаи значительного ухудшения здоровья у обучающихся, связанного с использованием средств ИКТ, включая интернет-зависимость

[2, 9]. При этом недостаточное освещение данных вопросов в научно-педагогической литературе, отсутствие соответствующих методических рекомендаций заставляет учителей опираться на собственный опыт работы.

Во-вторых, учителя физической культуры, в отличие от учителей информатики, не мотивированы должным образом к проведению соответствующих занятий. Это говорит о том, что инициаторами могут стать именно учителя информатики, которые будут использовать доступный им спектр мер в области здоровьесбережения.

Разработанная нами дисциплина по выбору получила название «Здоровьесбережение», так как содержание курса включало в себя только некоторые аспекты области ПНПЗО. Объем курса составляет 24 академических часа, он реализуется на теоретических, семинарских, практических и контрольных занятиях по информатике. При отборе содержания подготовки студентов, обучающихся по программе подготовки бакалавриата «Педагогическое образование» по профилю «Учитель информатики», мы учитывали следующие условия:

1. Использование учебного материала, посвященного формированию знаний, умений, навыков создания и поддержания средствами ИКТ условий обучения, безопасных для здоровья пользователей.

К данным средствам ИКТ следует отнести диагностические комплексы и системы, применяемые, например, для контроля изменений показателей функционального состояния до и после кратковременного воздействия средств ИКТ. В этом ключе можно говорить и о приборах оздоровительного назначения, функционирующих на базе средств ИКТ (переключение режимов работы метеобарокамеры, приборов стимуляции). Медиа-курс для освоения

и проверки теоретических знаний и умений в области ПНПЗО, проводимый в электронном виде, тем не менее, также служит цели обеспечения безопасности здоровья пользователей [3].

2. Использование примерных стандартов по оснащению и функционированию кабинетов здоровья образовательной организации.

В данном контексте речь идет об использовании кабинета здоровья на базе кабинета информатики для применения оздоровительного комплекса оперативной нейтрализации [6].

Возвращаясь к подготовке студентов в области ПНПЗО, следует отметить, что при ее организации в вузе учитывался критерий междисциплинарных связей, обеспечивающий междисциплинарную интеграцию с курсом по дисциплине «Физическая культура и спорт» и последующим курсом подготовки в области ПНПЗО, реализуемым в рамках элективных дисциплин (модулей) по физической культуре и спорту, что позволяет обеспечить последовательность при формировании системы мотивов, знаний, умений, навыков в области ПНПЗО.

Если говорить о роли физической культуры и спорта в сохранении и развитии здоровья обучающихся, то авторами отмечается закономерное снижение влияния всех факторов-побудителей в мотивационной сфере студентов разных лет обучения, связанных с повышением требовательности студентов к «содержательному и функциональному аспектам занятий по физической культуре в вузе, их связи с профессиональной подготовкой» [8].

Вместе с тем предлагаемые нами содержательный и функциональный аспекты практических и контрольных занятий, осуществляемых в комфортных условиях оздоровительно-физкультурного центра, кабинетов здоровья, их доступность, а также теоретическая подготовка в области ПНПЗО мотивируют студентов к применению средств, способов, мер, направленных на нейтрализацию

и предотвращение негативных последствий, и к увеличению числа занятий оздоровительной направленности, повышающих производительность в условиях профессиональной деятельности.

Проблема сохранения и развития здоровья обучающихся должна решаться комплексно. Наряду с предлагаемыми нами мерами по предотвращению и нейтрализации негативных последствий использования средств ИКТ для здоровья обучающихся, в сложившихся условиях, требующих от будущих воинов – защитников нашей Родины необходимого уровня развития основных физических качеств, важна практика проведения обязательных 2-х разовых занятий в неделю по физической культуре в течение всего периода обучения в школах, колледжах и, особенно, в вузах, необоснованно отменяющих и сокращающих эти занятия. Процесс физического воспитания в образовательных организациях должен быть организован с учетом новых, популярных у молодежи видов физкультурно-спортивной деятельности с необходимым материально-техническим обеспечением. В рамках междисциплинарной интеграции вновь восстановленной в школах дисциплины «Начальная военная подготовка» и дисциплины «Физическая культура» востребованными становятся проведение военно-спортивных игр («Зарница» и др.) и одно-двух дневных туристических походов, организация тематических летних школ и военно-спортивных лагерей.

Заключение

Таким образом, в условиях многократно усилившегося воздействия негативной информации со стороны недружественных нам стран, а также тотального, неконтролируемого использования цифровых технологий, приносящих вред здоровью и дестабилизирующих моральное состояние детей, молодежи, необходимо незамедлительное внедрение в практику вузов, колледжей, школ уже

подготовленных ведущими специалистами теоретико-методологических основ и практических разработок с целью подготовки студентов, школьников к владению передовыми технологиями обеспечения информационной безопасности личности и безопасности здоровья обучающихся в условиях использования средств ИКТ.

Литература

1. *Виленский М.Я.* Физическая культура в гуманитарном образовательном пространстве вуза / М. Я. Виленский // Физическая культура: воспитание, образование, тренировка. – 1996. – № 1. – С. 27–32.
2. *Герова Н.В.* Теоретические и методические основания непрерывной информационной подготовки студентов гуманитарных профессий по направлению педагогического образования: монография. – Рязань, РГУ имени С.А. Есенина, 2017. – 160 с.
3. *Димова А.Л.* Базовые виды физкультурно-спортивной деятельности с методикой преподавания: учебник для вузов. – М.: Изд-во Юрайт, 2021. – 428 с. [Электронный ресурс] // ЭБС Юрайт [Сайт]. URL: <https://urait.ru/bcode/467745>.
4. *Димова А.Л.* Дисциплина «Предотвращение негативных последствий использования ИКТ для здоровья обучающихся» в программе подготовки бакалавров педагогических специальностей // Педагогическая информатика. – 2020. – № 3. – С. 125–132.
5. *Димова А.Л.* Развитие понятийного аппарата информатизации образования: здоровьесберегающий аспект / А.Л. Димова // Педагогическая информатика. – 2019. – № 3. – С. 138–144.
6. *Димова А.Л.* Методические рекомендации по оборудованию и использованию кабинета информатики для проведения оздоровительно-физкультурных занятий и тестирования показателей здоровья учащихся: метод. пособие. – М.: ИИО РАО, 2011. – 50 с.
7. *Иванова С.В.* О гражданственности, национальной идентичности, безопасности / С.В. Иванова // Ценности и смыслы. – 2012. – № 5. – С. 4–9.
8. *Мазуров Л.Е.* Формирование положительного отношения студентов к самостоятельным занятиям физическими упражнениями: дис. ... к. пед. наук: 13.00.04 // Мазуров Леонид Евгеньевич. – Тюмень, 2003. – 196 с.

9. Мухаметзянов И.Ш. Медицинские аспекты информатизации образования. 2-е изд., исп. и доп. – М.: ФГБНУ «ИУО РАО», 2017. – 168 с.

10. Поляков В.П. Информационная подготовка в вузе и аспекты информационной безопасности // Молодежный экстремизм: истоки, предупреждение, профилактика: материалы международной научно-практической конференции (23-24 мая 2014г.). Часть 1. – М.: НОУ ВПО «МПСУ», 2014. – С. 452–457.

11. Развитие информатизации образования в школе и педагогическом вузе в условиях обеспечения информационной безопасности личности // С.В. Бешенков, В.Я. Ваграменко, В.А. Касторнова, О.А. Козлов, Э.В. Минзаева, И.В. Роберт, В.И. Сердюков, Т.Ш. Шихнабиева, Г.Ю. Яламов. – М.: ФГБНУ «ИУО РАО», 2018. – 105 с.

12. Роберт И.В. Теория и методика информатизации образования: (психол.-пед. и технол. аспекты). – М.: БИНОМ, 2014. – 354 с.

М. В. Мананникова,

кандидат философских наук,

доцент кафедры геополитики и устойчивого развития общества

Российского государственного университета нефти и газа

(национального исследовательского университета)

имени И.М. Губкина

АКСИОЛОГИЧЕСКИЕ ОСНОВЫ ОБРАЗОВАНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ

Технология никогда не заменит великих учителей, но технология в руках великих учителей – это трансформация.

Джордж Курос

Текущему моменту развития цивилизации характерен процесс дальнейшего усложнения и кооперации социальных, экономических и логистических систем, основным направлением развития которых становится ускоренная интеграция все более сложных и разнообразных технологий. Данный процесс предполагает необходимость создания образовательных стандартов и профессиональных компетенций нового поколения.

Система высшего образования консервативного типа, встраиваясь в механику происходящих изменений, также признает необходимость трансформации. Вузы стремительно осваивают и внедряют в образовательный процесс новые модели, подходы, технологии и методы. Необходимости в одинаковых, «типовых» специалистах больше не наблюдается, а востребованность на рынке труда определяется обладанием не только профессиональных, но и системой гибких навыков и умений.

По оценке генерального директора City Business School Юлии Будишевской, важнейшими навыками современного специалиста стали адаптивность и универсальность, умение работать в команде, используя минимально доступные ресурсы, умение действовать в состоянии неопределенности, в условиях конкуренции, а также способность к постоянному обучению.

Данная оценка коррелирует с результатами масштабного исследования, проведенного компанией LinkedIn Learning в 2020 году. Согласно полученным данным, работодатели ждут от будущих специалистов следующих умений: креативного подхода к решению задач, умения работать в команде, убедительно и репрезентативно доносить свою точку зрения, адаптироваться к быстроизменяющейся среде, обладать развитым эмоциональным интеллектом. К востребованным умениям относят также способность работать с информацией, критическое и предпринимательское мышление, готовность к быстрому освоению новых знаний и способность быстро принимать решения.

Анализ ситуации глобального технологического обновления позволяет констатировать возникновение системы новых, т.н. «цифровых ценностей», часто именуемых ценностями «цифрового гуманизма». К ним относят прежде всего скорость, стандартизацию, многофункциональность, прозрачность, мобильность, информацию и другие.

Традиционные ценности в образовании условно можно соотнести со знаниевой образовательной моделью, предполагающей в первую очередь приоритет знания и направленной на воспроизведение знаний в действии, верное их отражение в мышлении с целью передачи новому поколению.

«Цифровые ценности» также условно ассоциируются с компетентностной моделью образования, предполагающей способность

и готовность использовать знания, умения и навыки, внутренние ресурсы индивида и внешние материальные ресурсы для самореализации в сложных меняющихся условиях реальности.

В настоящее время в цифровом пространстве практически во всех его сферах наблюдается переход от традиционных ценностей к посттрадиционным, к ценностям «цифрового гуманизма». Это существенным образом меняет и отношение к образовательной модели современной системы высшего образования, в которой студент – это будущий специалист и ученый, который должен обладать навыками успешного применения технологий искусственного интеллекта, виртуальной и дополненной реальности (VR и AR), работы с нейросетью, а также владеть навыками обработки больших данных.

Актуальность данных требований обуславливает необходимость внедрения цифровых технологий в процесс образования. Однако, на наш взгляд, содержание и механизм данного процесса должны быть всесторонне осмыслены, с учетом как положительных, так и отрицательных его последствий.

К последним можно отнести, во-первых, формирование нового языка. Возникновение и активное использование разнообразных мемов, англицизмов, гиков приводит к существенным изменениям в языковой картине мира современного молодого человека. В условиях возрастания роли интернет-коммуникаций происходит активное развитие жанров естественной письменной речи (пост, смс-сообщений, комментариев), близких к разговорной речи, не требующих нормирования. Возникают тексты, имеющие гибридную структуру (гипертексты, креолизованные форматы), позволяющие синтезировать информацию разных типов – аудиальную, визуальную, текстовую (эмотиконы, демотиваторы, интернет-мемы и другие). Данные процессы оказывают существенное влияние на

языковую среду, угрожая чистоте и нормативности языка.

Одним из возможных способов решения данной проблемы может стать наполнение курса родного языка ценностной языковой составляющей, подробный анализ связи родного языка и родной культуры.

Следующей проблемой, возникающей вследствие внедрения цифровых технологий, становится изменение способа мышления и восприятия реальности. Распад относительно устойчивых традиционных общностей является признаком «современности», согласно Э. Гидденсу. Вместо реальных социальных отношений возникает система отношений виртуальных, интегрирующих личность в модели интернет-сообществ.

Современный социальный эскапизм – это редукция «живых» взаимодействий к сетевым коммуникациям, формирование цифровой личности, обладающей ценностной свободой, а точнее отсутствием ценностных критериев, что порождает эгоизм и агрессию. Жизнь в условиях сверхнасыщенного информационного поля способствует формированию хаотичности мышления. Разрозненная противоречивая информация мешает формированию правильных ценностных установок, анализу ситуации и принятию взвешенных решений. Одним из вариантов решения данной проблемы может стать обучение информационному отбору, формированию т.н. «информационного фильтра», «информационной гигиене», способам анализа и гармонизации разнообразных информационных потоков.

Изменение форм коммуникаций, детерминированное развитием социальных сетей, приводит к трансформации общества и личности. В настоящее время происходит непрерывный рост числа коммуникационных каналов, при этом содержательно-качественная часть их постоянно сужается. Данные процессы приводят

к необходимости постоянной адаптации человека к новым формам самопрезентации, что существенным образом влияет на мировоззрение и привычки личности.

Объективно обусловленная смена форматов и способов обучения приводит к тому, что современные студенты ориентированы на результат обучения, а не на сам процесс. Если затраты времени на изучение материала окажутся слишком велики, студенты, вероятнее всего, проигнорируют данную информацию. Эрудиция и знания, таким образом, лишаются ценностного значения.

Еще одной важной характеристикой цифровой реальности становится изменение процесса социализации. Усвоение правил и норм социальной коммуникации сегодня подразумевает прежде всего умение общаться посредством мессенджеров и социальных сетей, «существование» в виртуальном пространстве. Значимость приобретают связи и статус личности в фэндомных сообществах. Интернет стал не только основным источником информации, но и важнейшим коммуникационным инструментом, обеспечивающим возможности оперативного и бесплатного общения. Всемирная сеть приобретает статус самостоятельной альтернативной реальности, «герменевтической» формы бытия, создающей иллюзию превосходства над реальностью «обычной». Психологическая литература вводит термин, обозначающий ситуацию размывания границ между «онлайн» и «офлайн» – реальностью – «игрализация общества». Данное понятие характеризует процесс внедрения принципов игровой деятельности в стратегию реального поведения, что позволяет говорить о важности анализа данной проблемы.

Цифровая культура в России еще находится в процессе становления, обретения соответствующих ее развитию ценностей. Несмотря на то, что традиционные базовые ценности, такие как здоровье, жизнь, карьера, семья, материальное благополучие, любовь

претерпевают серьезную трансформацию, а человек все активнее вовлекается в сферу виртуальной реальности, необходимо помнить, что основой процесса изменения культуры и образования должны оставаться такие ценности как безопасность личности, ее самоактуализация, свобода, развитие, творчество, этика, уважение к жизни.

Основной проблемой педагогики становится необходимость включения в процесс образования цифровых технологий и сохранение при этом всей глубины его содержания. Цифровизация процесса образования вне содержательного наполнения ее нравственными ценностями и смыслами ведет к разрыву с реальным миром, утрате культурного кода и национальной идентичности.

Особое значение в нашем обществе приобретает «нравственное воспитание», так как технологии сами по себе это только инструмент, их ценность определяется характером использования. Педагог, применяя цифровые технологии и инструменты, способен формировать личность, развивать культурно-социальные навыки, укреплять духовно-нравственные основы личности и ее национальную идентичность. В связи с этим возникает необходимость глубокого и всестороннего исследования данного процесса, целенаправленной его регуляции в соответствии с потребностями цифровой экономики и стратегии развития России.

Цифровая аксиология призвана сыграть роль инструмента «мягкой силы» в процессе образования. Фундаментальной основой нашей системы ценностей должны оставаться ценности классического гуманизма и антропоцентризма, только тогда цифровой мир будет обладать человеческим измерением, вниманием к личности и ее духовным потребностям и запросам.

Литература

1. *Баева, Л.В.* Качество жизни и ценности человека / Л.В. Баева // Вестник Волгоградского государственного университета. – 2015. – № 3 (29) – С. 108–114.
2. *Игнатова, Н.Ю.* Образование в цифровую эпоху: монография / Н.Ю. Игнатова. – Нижний Тагил: НТИ (филиал) УрФУ. – 2017. – 128 с.
3. *Ильин, Г.Л.* Об особенностях развития современного мышления / Г.Л. Ильин // Школьные технологии. – 2013. – №1. – С. 10–13.
4. *Ионова, С.В.* Лингвистика нового языкового сознания и информационных технологий / С.В. Ионова // Вестник Волгоградского государственного университета. – 2016. – Т.15. – № 3. – С. 6–16.
5. *Калмыкова, Е.И.* Актуальные проблемы русского языка в современной языковой ситуации / Е.И. Калмыкова // Международный электронный журнал. Устойчивое развитие: наука и практика. – 2014. – № 1(12). – С. 77–81.
6. *Литинская, Д.Г.* Типы современного эскапизма и феномен экзистенциального эскапизма / Д.Г. Литинская // Ярославский педагогический вестник. – 2012. – № 1. – С. 308–311.
7. *Ронжина, Н.В.* Обучающаяся личность в мире цифровизации и (или) гуманизации образования / Н.В. Ронжина // Ноосферные исследования. – 2020. – Вып. 3. – С. 69–75.
8. *Седов, Д.Н.* Аксиологический анализ цифровизации российского образования / Д.Н. Седов // Вестник Бурятского государственного университета. Серия философия. – 2020. – Вып.4. – С. 24–30.
9. *Стариченко, Б.Е.* Цифровизация образования: реалии и проблемы / Б.Е. Стариченко // Педагогическое образование в России. – 2020. – № 4. – С. 16–26.
10. *Цветкова, И.В.* Симулякры цифрового гуманизма в современном образовании / И.В. Цветкова // Вестник ВГУ. Серия Философия. – 2021. – № 2. – С. 88–97.

В. Вл. Чекмарев,
доктор экономических наук, профессор

Вл. В. Чекмарев,
кандидат экономических наук, доцент

Костромской государственной университет

НООСФЕРНАЯ БЕЗОПАСНОСТЬ: МАКРОСХЕМА КРИСТАЛЛА РОСТА

Существенным инфраструктурным элементом обеспечения стратегической безопасности будущего России и её граждан является ноосферная безопасность. В связи с этим рассуждения об утрате смысла обеспечения экономической безопасности в процессах жизнедеятельности общества под лозунгом «скрытые угрозы: две – я и моя тень как одна ложь на двоих», а также аксиоматизация *ноосферной безопасности* как школы окна, в котором видится знание об угрозах, опасностях, возможных рисках, как *посоха жизни для каждого*, чтобы действовать не только в ответ, но и на упреждение, чтобы не случайно угадывать, а точно знать смысл энергетического отравления ноосферного будущего, вызывают возражения.

Рассмотрение проблем обеспечения безопасности государства и суверенитета стран традиционно осуществляется через военную, политическую, экономическую (в том числе продовольственную и энергетическую) виды безопасности. Но в последнее время появились публикации, раскрывающие вопросы стратегии народосбережения в Российской Федерации [3, 4, 6, 8], с выделением целей стратегий, приоритетов, принципов, задач и механизмов реализации стратегии.

Но обобщая эти вопросы в едином блоке нельзя не подчеркнуть, что в их основу положено ноосферное будущее развития мира.

Выделим в общих вопросах три основных направления и рассмотрим их тезисно.

Первое. Новое время – Новый человек.

Второе. Анализ, синтез и планирование долгосрочных решений в экономике.

Третье. Выделение ноономики в рамках глобального кризиса.

Во-первых – на планете происходят новые процессы и изменения, и это не только глобализация и цифровизация, но и преобразование биосферы, а гармоничному существованию человека соответствует появление ноономики и ноосферы. И самое, наверное, главное то, что ожидает человечество – это увеличение Любви к себе. Иллюзии прошлого будут уступать новой энергоорганизации взаимного действия с Новым временем, использованием человеческой физико-химической энергии и т.п.

Во-вторых – экономические взаимодействия структурно и уровнево усложнились. Появились не только экономические субъекты нано-, номо-, микро-, меза-, макро- и т.п. уровней, но и *агенты* экономических систем, действующие в разных институциональных условиях и иерархических уровнях, на горизонтах нескольких интервалов времени.

Важно подчеркнуть появление ещё и *акторов*, действующих в экономическом пространстве с разной степенью воздействия на исход взаимодействий, то есть на потенциальное состояние экономических взаимодействий. Дело в том, что в случае долгосрочных стратегий обобщённый исход позволяет интегрировать значение отдельных исходов для оценки последствий планируемых решений. Появляется понятие «вектор приоритетов». Представление процесса планирования в виде иерархии высокопрофессионально

изложено А. Андрейчиковым и О. Андрейчиковой [Андрейчиков и др., 2002]. Вышеотмеченное имеет принципиальное значение при определении методологических принципов, методов и категориального аппарата при развитии нооэкономики.

Как изложено выдающимися учёными в книге «По ту сторону глобального кризиса: ноономика, креативность, геополитэкономия», производство остаётся материальным, но становится знаниеинтенсивным [2, с. 25]. Однако у человечества не только появляются новые возможности индустриального развития, но и происходит нарастание угроз. Защита от них – в ноосферной безопасности, содержательно определяющаяся в изменении критериев культуры и современного экономического пространства.

Как следствие, возникает вопрос, есть ли границы вмешательства в природу человека и изменение биосферы?

Противоположные теоретические характеристики ноосферной безопасности представляют собой стороны типичного логического противоречия – антиномии. Для его решения, согласно марксистской методологии, необходимо ввести в анализ условие, неизвестное на прежней его ступени. Раскрытие этого условия является содержанием характеристики ноосферной безопасности.

Литература

1. Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. – М.: Финансы и статистика, 2002. – 365 с.
2. Бодрунов С., Десаи Р., Фриман А. По ту сторону глобального кризиса: ноономика, креативность, геополитэкономия. – СПб.: ИНИР им. С.Ю. Витте, 2022. – 368 с.
3. Галушко Н.С., Ниязметов А.К., Окулов М.О. Кристалл роста. К русскому экономическому чуду. – М., 2021. – 360 с.
4. Глобальные социально-экономические трансформации: будущее России / под общ. ред. С.Д. Бодрунова. – М., 2022. – 640 с.

5. Новая-Костубаева С.В. Новое Время – Новый Человек – Новые Возможности. – М., 2016. – 192 с.

6. Российский разворот / под ред. Ю.М. Осипова и др. – М.; Тамбов, 2020. – 260 с.

7. Чекмарев В.В. Ноономика: гипотеза становится теорией // Ноосферные исследования. – 2022. – № 1. – С. 5–11.

8. Шнуренко И. Человек взломанный. – М.: Изд-во «Наше завтра», 2021. – 456 с.

*Н.Д. Подуфалов,
доктор физико-математических наук, профессор,
заслуженный деятель науки РФ,
академик Российской академии образования,
Российская академия образования*

О ЗАДАЧАХ ОБЕСПЕЧЕНИЯ НЕОБХОДИМОГО УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ НАУЧНЫХ ИССЛЕДОВАНИЙ В УНИВЕРСИТЕТАХ

Решение поставленной руководством страны задачи превращения университетов в один из основных локомотивов научно-технологического развития Российской Федерации и её регионов потребует существенного расширения участия вузов в научных исследованиях, формирования вокруг них пояса инновационных структур, занимающихся технологическими разработками. В условиях значительного ужесточения конкурентной борьбы на мировых рынках товаров и услуг, а также усиления военных угроз по отношению к России и дружественным ей государствам важное значение приобретает глубокий анализ и корректировка действующей системы работы с научно-технической информацией в научных коллективах высшей школы с целью повышения в необходимых случаях уровня защиты информации о тематике и результатах проводимых исследований и, в целом, обеспечения необходимого уровня информационной безопасности в сфере научной деятельности.

С одной стороны, фактическое упразднение на первоначальном этапе российских реформ созданной в условиях «железного занавеса» системы контроля за движением и использованием

научно-технической информации, когда публикация результатов исследований и фундаментального, и прикладного характера в открытых источниках информации была возможна только после проведения экспертизы и получения соответствующего разрешения, позволило создать более комфортные условия для исследователей, ускорить обращение информации и тем самым активизировать многие направления исследований, ускорить научно-технический прогресс.

С другой стороны, это привело к значительной неконтролируемой утечке научной и технологической информации за рубеж, негативно повлияв на уровень обороноспособности страны и способствуя снижению конкурентоспособности ряда отраслей российской экономики на международных рынках.

Для решения возникших проблем в последнее десятилетие сделано немало – усилен контроль за проведением исследований оборонного и военного характера, разработан и утвержден указами Президента Российской Федерации ряд документов, определяющих стратегию национальной и информационной безопасности, стратегию научно-технологического развития страны. Обновляется с учетом развития новых технологий и изменений на международной арене законодательство, регулирующее отношения, связанные с производством, обращением и использованием информации, а также охраной результатов интеллектуальной деятельности, государственной и коммерческой тайн и защитой конфиденциальной информации. Общие подходы к решению задач обеспечения информационной безопасности и роль вузов в этом процессе можно найти, например, в [5].

Вместе с этим, планируемое расширение объемов и тематики «университетских» исследований и повышение их роли в развитии страны приведут к увеличению объемов исследований, нахо-

дящихся на стыке фундаментальной и прикладной науки, включая поисковые и инициативные исследования, научно-технологические разработки инновационных университетских структур, открытые диссертационные исследования и т.д., то есть исследований, не имеющих прямого отношения к гособоронзаказу или к различному виду тайн, но потенциально способных оказать определенное влияние на обороноспособность и конкурентоспособность страны.

Данная категория научных исследований и обращение информации, используемой и получаемой в результате этих исследований, сейчас регулируются, главным образом, нормами законодательства и других нормативных документов в областях науки, интеллектуальной собственности и информационных технологий, связанными с регулированием исследований, имеющих открытый, «гражданский» характер, допускающими достаточно свободный обмен и использование информации. Как правило, ограничения на информационный обмен в этом случае связаны с защитой авторских прав и результатов интеллектуальной деятельности, а также, в отдельных случаях, с охраной коммерческой тайны. Как следствие, возникают большие риски неконтролируемого распространения научно-технических знаний, полученных в российских университетах и являющихся потенциально способными обеспечить усиление конкурентоспособности или военного потенциала наших зарубежных оппонентов.

Не менее серьезной проблемой является использование и передача научно-технической информации исследователем, выезжающим за рубеж или переходящим на работу в иностранные компании. Причем наиболее сложная ситуация возникает тогда, когда исследования или разработки выполнялись научным коллективом и невозможно достаточно четко определить вклад в полученные

результаты каждого члена коллектива. Понятно, что в данном случае следует опираться на уточнение соответствующих положений и норм законодательства в области интеллектуальной собственности и в области защиты конфиденциальной информации, а также руководствоваться механизмами регистрации результатов интеллектуальной деятельности и методами пресечения нарушений законодательства. Несмотря на то, что данная проблематика выходит за рамки настоящего исследования, позволим два замечания. Во-первых, без решения вышеуказанной проблемы эффективность рассматриваемой деятельности может быть значительно снижена. Во-вторых, нужны разработка и внесение в законодательство требований и обязательств, которые должны выполняться физическим лицом при выезде за рубеж или при переходе на работу в иностранные компании в том случае, если это лицо принимало участие в исследованиях и разработках с каким-либо уровнем ограничений на распространение информации.

В целом, развитие и расширение научных исследований и разработок в университетах требует более эффективного регулирования в области информационной безопасности. В общем случае необходимо искать «золотую середину» – регуляторы не должны негативно влиять на темпы исследований и необоснованно сужать их тематику и в тоже время создавать условия для выявления и защиты от несанкционированного распространения методов и результатов интеллектуальной деятельности, потенциально способных повысить обороноспособность страны и конкурентоспособность на международных рынках товаров и услуг в условиях «новой индустриализации» и формирования «технологического суверенитета».

Технологии защиты информации, содержащей сведения, составляющие государственную тайну или применяемые при выполнении

гособоронзаказа, для рассматриваемых видов научных исследований использовать в полном объеме нецелесообразно, поскольку это может негативно повлиять на темпы исследований и «отвратить» часть научной молодежи от участия в поисковых и инициативных исследованиях по некоторым актуальным тематикам. Поэтому важна разработка методологии и методов формирования системы информационной безопасности для этой сферы исследований и поиск оптимальных и эффективных методик обеспечения её защиты.

По сути, ряд методологических положений, которые необходимо учитывать при создании вышеуказанной системы, уже упомянуты ранее. Дополнительно к таким положениям можно отнести следующие требования к методам регулирования этих исследований и обеспечения защиты информации при их проведении:

- методы регулирования не должны приводить к снижению темпов исследований и необоснованно сужать тематику исследований;
- область регулирования должна включать поисковые и инициативные исследования, открытые диссертационные исследования, исследования и разработки структур, входящих в «инновационный пояс» университета, а также исследования, проводимые в рамках открытых научных и научно-технических программ, разрабатываемых и реализуемых университетами;
- методы регулирования должны включать методики, позволяющие прогнозировать потенциальную возможность использования результатов проводимых исследований в решении задач повышения обороноспособности и конкурентоспособности страны, а также оценивать необходимый уровень ограничений на использование информации, получаемой при проведении этих исследований, и риски, связанные с несанкционированным распространением информации;

- уровень регуляторных ограничений и методики их установления должны учитывать вышеуказанные риски, а сами ограничения должны быть минимально необходимыми для купирования рисков;
- экспертный анализ и оценка тематики проводимых исследований и прогнозируемых результатов должны проводиться на регулярной основе поскольку «охраноспособные» результаты могут появиться на любом этапе исследований;
- формирование и утверждение перечня тематик (направлений) исследований и разработок, в отношении которых должна проводиться обязательная экспертиза, необходимо осуществлять только на том уровне системы административного управления, который позволяет это сделать содержательно и эффективно, но на основе методик (или других нормативных документов), утвержденных соответствующим уполномоченным федеральным органом исполнительной власти (министерством, ФСТЭК и др.);
- при регулировании должен соблюдаться принцип «презумпции невиновности» – ограничения устанавливаются только тогда, когда обоснована необходимость их установления и имеется прогноз возможных рисков;
- правовая, нормативная и методическая база рассматриваемой деятельности должна постоянно обновляться с учетом динамики изменения характера этой деятельности.

Как было отмечено, параллельно следует заниматься методологией и методами определения и реализации требований и обязательств, которые должны выполняться физическим лицом при выезде за рубеж или при переходе на работу в иностранные компании в том случае, если это лицо принимало участие в исследованиях и разработках с каким-либо уровнем ограничений на

распространение информации, а также разработкой методик, обеспечивающих реализацию ограничений на новом месте работы.

Инфраструктура, обеспечивающая информационную безопасность проведения научных исследований

Существует широкий круг аппаратных и программных средств обеспечения информационной безопасности, в том числе средств защиты информации, предназначенных для работы с информацией различной степени секретности. Поэтому, оценив уровень необходимых ограничений на работу с информацией при проведении рассматриваемого вида научных исследований, по-видимому, не составит особого труда подобрать или разработать нужные средства защиты.

Вначале рассмотрим основные типы информационных систем и сетей, используемых при проведении «вузовских» научных исследований, в которых, в необходимых случаях, должен быть обеспечен соответствующий уровень защиты информации.

Прежде всего к ним относятся компьютеры, компьютерные классы и серверы, на которых находится и обрабатывается используемая и получаемая в исследованиях информация.

Если они не подключены к глобальным информационным сетям, а используются либо локально, либо в составе закрытых (защищенных) корпоративных сетей, например, защищенных сетей университета, то защита информации в данном случае не будет представлять особых проблем.

Наибольшую сложность представляет защита информации при работе с использованием глобальных информационных сетей. Основной объем научных исследований университетов укладывается в рамки данного случая.

Прежде всего отметим, что при обработке и распространении

научной и технологической информации, как правило, используются следующие сетевые технологии, которые могут привести к неконтролируемому распространению информации:

- проведение конференций, совещаний и других научных мероприятий в режиме ВКС (видеоконференцсвязи) на базе различных информационных платформ;
- использование и хранение информации в различных информационных базах данных;
- публикация результатов исследований в открытой печати, размещение их в электронных библиотеках или других базах данных;
- использование электронной почты и телефонии;
- удаленные обработка данных и вычисления, в том числе, с использованием облачных технологий.

Также, одним из факторов несанкционированного распространения информации может стать использование несертифицированного программного обеспечения, программного обеспечения и аппаратуры, произведенных зарубежными фирмами.

В ряде случаев защита информации может быть обеспечена на основе криптографических методов и средств, в основном, при передаче и хранении информации. В связи с тем, что проведение исследований в областях естественнонаучного, математического и инженерного знания, как правило, требует проведения различного рода вычислений, использования специализированных пакетов программ, скорее всего, применение криптографии в этих случаях будет существенно ограничено.

Поэтому, например, широкое использование облачных вычислений представляется маловероятным и возможно только при создании частного облака (private cloud) – инфраструктуры, предназначенной для использования, как правило, одной организацией, и

находящейся в собственности, управлении и эксплуатации этой организации.

Понятно, что необходимый уровень информационной безопасности научных исследований при работе в открытых сетях можно обеспечить только за счет выделения информации, требующей установленного уровня защиты, и организация распространения, обработки и хранения этой информации в защищенных информационных системах и сетях или в их защищенных сегментах, либо, если это позволяет характер исследовательской задачи, за счет использования криптографических методов и средств защиты.

Учитывая, что в университетах исследования проводятся по широкому спектру направлений, необходимый уровень их информационной безопасности во многих случаях без создания университетских защищенных информационных сетей, либо включения в корпоративные (отраслевые) защищенные информационные сети, невозможен. Также необходимо учесть, что результаты научных исследований могут использоваться при обучении студентов, т.е. рассматриваемые задачи будут важны и для образовательного процесса – если в университете будет создана информационная среда, обеспечивающая необходимый уровень информационной безопасности научных исследований, практически будет создана основа информационной безопасности образовательного процесса.

Обсуждаемые задачи будут актуальными для многих университетов и решать их целесообразно централизованно, в том числе и на основе создания единой защищённой федеральной университетской сети.

Таким образом, становится всё более актуальным анализ существующей практики обеспечения информационной безопасности при проведении научных исследований в университетах, выявления проблемных ситуаций, характерных для большинства

университетов, и на основании единой методологии разработка методов и методик их разрешения.

Основные проблемы, решение которых, как правило, будет опираться на совершенствование или разработку соответствующего программного и аппаратного обеспечения рассмотрены выше. Наиболее эффективным способом представляется централизованный заказ на разработку и создание необходимых аппаратно-программных продуктов и методик их использования, в том числе, для формирования при решении ряда научных задач защищенных корпоративных информационных сетей, либо создание объединённой защищенной университетской сети. Также потребуется защищенная информационная платформа для проведения различных совещаний, конференций и других мероприятий.

Понятно, что ограничиваться только созданием защищенных корпоративных сетей отдельных университетов нельзя. Для эффективного развития научных исследований необходимо создание условий для беспрепятственного межвузовского обмена научной информацией и создание объединенных (общих) баз научно-технической данных (электронных библиотек). Более того, целесообразна интеграция вузовских и академических сетей и баз данных.

Не вызывает сомнений, что многие ведущие университеты будут вынуждены индивидуально обеспечивать защиту своих информационных сетей, а, в перспективе, создавать либо сети, имеющие достаточно высокую степень защиты, либо хорошо защищенные сегменты имеющихся сетей. Конечно, при проведении некоторых исследований можно с согласия заказчиков использовать и корпоративные отраслевые сети. Но это не решит общей задачи – обеспечение оптимального уровня информационной безопасности для университетских исследований, требующих не такого высокого

уровня защиты информации, как, например, при выполнении гособоронзаказа или защите гостайны.

Следовательно, актуальной является разработка достаточно детальной концепции построения защищенной отраслевой (либо для высшего образования, либо для высшего образования и академической науки) информационной сети с тем, чтобы формируемые университетами защищенные сети можно было в перспективе без особых проблем интегрировать в общую отраслевую защищенную сеть.

Для эффективного решения перечисленных выше задач требуется разработка отраслевой программы, направленной на обеспечение в высшей школе информационной безопасности проведения научных исследований, технологических разработок и образовательного процесса, использующего результаты таких исследований и разработок, а также определение источников необходимых инвестиций. Либо, если будет разрабатываться общая программа цифровой трансформации системы образования, то она должна включать подпрограмму обеспечения информационной безопасности.

Большой опыт обеспечения информационной безопасности на основе создания защищенных корпоративных сетей накоплен в военных высших учебных заведениях (например, см. [1, 2, 3, 4]). В широком спектре научных статей, посвященных этой проблематике, разрабатывается необходимый понятийный аппарат, определяются назначение, принципы формирования и реализации цифровой информационно-образовательной среды, организационно-методические и технологические требования к организации учебного процесса в условиях использования информационной системы образовательного назначения, обосновываются структура и содержание цифрового образовательного контента в области обеспечения

национальной безопасности как компонента цифровой информационно-образовательной среды и т.д.

В [4] отмечается, что: «В научных трудах военных политологов, социологов, психологов и педагогов подчеркивается, что Министерство обороны РФ предпринимает шаги, направленные на минимизацию негативных последствий цифровизации за счет создания внутренней защищенной информационно-телекоммуникационной инфраструктуры и ограничения доступа военнослужащих к глобальному Интернету и использованию личных цифровых устройств. Одним из направлений противостояния критическим для обороноспособности страны угрозам безопасности становится принятие нормативно-правовых актов, введение административных и технических запретительных мер в отношении использования цифровых технологий во время исполнения служебных обязанностей и интернет-активности военнослужащих».

В некоторых работах акцентируется внимание на необходимости формирования культуры работы с информацией, требующей защиты. Например, в [4] отмечается, что важную роль в формировании такой культуры в военных вузах играют: «установление строгих регламентов, различных форм допуска и прав доступа, средств контроля и ответственности постоянного и переменного составов за обеспечением безопасности и конфиденциальности информации; ограничения на использование цифровых гаджетов, способных служить каналами утечки данных, проникновения злоумышленников или вредоносных программ; запрет использования технологии Wi-Fi, повышающей опасность неконтролируемого воздействия на внутренние сети и информационные ресурсы образовательной организации; подготовка к обучению в информационно-образовательной среде и повышение квалификации преподавателей и обслуживающего персонала».

В ряде случаев опыт военных вузов будет полезен и для гражданских вузов, но в полном объеме его целесообразно применять только при проведении исследований в рамках гособоронзаказа или других закрытых исследовательских программ.

В первую очередь, данный опыт можно использовать при создании защищенных корпоративных и отраслевой информационных сетей или их защищенных сегментов. Например, в [3] отмечается, что информационная система военного вуза должна быть сегментирована следующим образом: «При сегментировании ИОС должна быть обеспечена защита периметров сегментов информационной системы в соответствии с требованиями по защите информации. ИОС должна обеспечивать функционирование трех сегментов: открытого (общедоступного), конфиденциального и закрытого. Открытый (общедоступный) сегмент предназначен для работы с материалами, не содержащими информацию ограниченного доступа и служебную информацию ограниченного распространения. Конфиденциальный сегмент предназначен для работы с материалами, содержащими информацию ограниченного доступа и служебную информацию ограниченного распространения (за исключением сведений, составляющих государственную тайну). Конфиденциальный сегмент должен обеспечить разграничение доступа к конфиденциальной информации пользователей ИОС. Конфиденциальный сегмент ИОС должен иметь возможность передавать служебную информацию посредством конфиденциального сегмента сети передачи данных Министерства обороны. Закрытый сегмент предназначен для работы с материалами, содержащими сведения, составляющие государственную тайну. Закрытый сегмент ИОС должен иметь возможность передавать служебную информацию посредством закрытого сегмента сети передачи данных Министерства обороны».

По-видимому, для обеспечения информационной безопасности рассматриваемой области научных исследований основной целью является создание в университетских сетях аналогов конфиденциальных сегментов.

Подчеркнем, что важную роль в данных случаях играют правовое и нормативное регулирование процессов работы с информацией, требующей различных уровней защиты.

Определение необходимого уровня защиты и регулирование информационной составляющей процесса научных исследований

Параллельно формированию защищенной информационной инфраструктуры должна решаться задача создания соответствующей экспертной системы – системы организации и проведения экспертизы тематики и результатов научных исследований, которая позволила бы определять необходимый уровень защиты научно-технической информации, получаемой в ходе исследований и способной усилить позиции наших зарубежных конкурентов во вред Российской Федерации, а также предотвращать её несанкционированное распространение.

В целом, экспертиза должна обеспечивать объективную оценку направления, тематики и возможных результатов исследования с точки зрения определения нужного уровня защиты информации. Эксперт или экспертная комиссия должны оценить потенциальную возможность использования результатов исследований и разработок для усиления обороноспособности страны, потенциальный эффект масштабного внедрения в производство и коммерческого использования, потенциальную возможность нанесения вреда природе и человеку. Результаты исследований в области гуманитарного знания необходимо оценивать также с точки зрения потенци-

альной возможность нанесения вреда обществу (общественным отношениям) и личности. Должны быть определены требования к опубликованию научно-технической информации в открытой печати или к обращению в открытых информационных сетях.

Как уже отмечалось, необходимо сформировать законодательную и нормативную базу, позволяющую эффективно проводить экспертизу и устанавливать в необходимых случаях оптимальные ограничения на использование и обращение научно-технической информации, разработать соответствующие методики.

По-видимому, нецелесообразно возвращаться к старой системе, когда осуществлялась общевузовская экспертиза всех научных работ с целью определения возможности их публикации в открытых научных изданиях. Для большинства работ, проводимых по открытым тематикам исследований, эта процедура, как правило, была пустой формальностью. Поэтому нужен более гибкий механизм, позволяющий исключить неэффективные затраты времени исследователей и экспертов и требующий привлечения высококвалифицированных экспертов только для экспертизы работ, имеющих большой внедренческий потенциал.

Одним из возможных вариантов создания такой экспертной системы в университете может стать организация трехуровневой экспертизы:

- первый уровень – предварительные анализ и оценка необходимого уровня защиты научно-технической информации, получаемой при проведении исследования самим исследователем или совместно с научным руководителем, если таковой имеется;
- второй уровень – экспертиза, проводимая кафедрой или научным подразделением университета, в котором работает исследователь;

- третий уровень – экспертиза, проводимая комиссией университетского уровня, создаваемой в необходимых случаях руководством университета.

Первые два уровня экспертизы характерны, в основном, для инициативных, поисковых и открытых диссертационных исследований, для них должны быть разработаны соответствующие методики.

Третий уровень экспертизы предполагает наличие научных или научно-технических программ (не обязательно в данном университете), тематика которых связана с тематикой экспертируемого исследования и для которых установлены определенные ограничения использования и распространения научно-технической информации. Естественно, в этом случае необходимо опираться на методики, которые обеспечивают защиту информации, получаемой или используемой при реализации данных программ.

Процесс экспертизы завершается на первом уровне, если исследователь (научный руководитель) убеждены в обоснованности принимаемых мер по защите информации или в отсутствии необходимости защиты, а также готовы нести в установленном порядке ответственность за свой выбор способа защиты информации.

В противном случае проводится экспертиза кафедральной комиссией (комиссией научного подразделения). Если кафедральная комиссия затрудняется принять обоснованное решение, то работа рассматривается университетской комиссией. Если и эта комиссия затрудняется принять окончательное решение, то на первых этапах исследования устанавливаются ограничения на использование информации по аналогии с грифом «для служебного пользования» – т.е. минимально необходимые ограничения.

Для организации экспертной деятельности Минобрнауки России должно принять положение о проведении экспертизы и

утвердить необходимые методики. В положении должны быть определены уровни защиты информации и ответственность за принимаемые решения на каждом уровне экспертизы.

Понятно, что сейчас наиболее актуальной является организация экспертизы фундаментальных и прикладных исследований в области математических, естественных и технических наук.

Также представляется целесообразным рассмотреть по аналогии с используемой в практической деятельности оценкой террористической опасности на основе «цветовой шкалы» соответствующую шкалу уровней информационной опасности с оценками рисков реализации опасных событий и исходя из неё разработать методику определения, оценки и формирования необходимого уровня информационной безопасности научных исследований и технологических разработок.

В перспективе, рассматриваемые в настоящей статье задачи и методы их решения целесообразно соотнести с аналогичной деятельностью, проводимой в государствах, входящих в дружественные политические и экономические международные организации (такие, как СНГ, ЕВРАЗЭС, ШОС, БРИКС и др.) с целью расширения межгосударственного и межвузовского сотрудничества в области образования, науки и технологического развития. Естественно, это потребует гармонизации соответствующих направлений законодательного и нормативного регулирования отмеченных направлений деятельности.

Заключение

Для формирования оптимальной и эффективной системы обеспечения информационной безопасности научных исследований в организациях высшего образования необходимо разработать методологические подходы к решению задач повышения

уровня информационной безопасности при проведении научных исследований и осуществлении технологических разработок, методы и методики анализа и регулирования исследовательского процесса, позволяющие оценивать потенциальную возможность использования результатов проводимых исследований для повышения обороноспособности страны и конкурентоспособности на зарубежных рынках товаров и услуг, а также риски, связанные с несанкционированным распространением информации и знаний, получаемых при проведении таких исследований. С учетом этого, определить механизмы и степень регуляторных ограничений, минимально необходимую для купирования рисков. Разработать методики экспертизы тематики и прогнозируемых результатов проводимых исследований с целью установления в необходимых случаях ограничений на использование и распространение информации, не приводящих к замедлению темпов научных исследований и необоснованному сужению их тематики, особенно в части поисковых и инициативных исследований.

Автор глубоко благодарен доктору технических наук, декану Факультета комплексной безопасности ТЭК Губкинского университета Сергею Николаевичу Гриняеву за полезные обсуждения проблем и задач, рассмотренных в настоящей работе.

Литература

1. Галушкин А.В., Косенок Ю.Н., Однокопытный В.Н. Проблемные вопросы автоматизации мероприятий научной (научно-исследовательской) деятельности военной образовательной организации Министерства обороны Российской Федерации. В сборнике: Информационные технологии: актуальные проблемы подготовки специалистов с учетом реализации требований ФГОС. Материалы VIII Всероссийской научно-практической конференции. – Омск, 2021. – С. 125–129.

2. Раецкая О.В. Информационная среда современного военного вуза // Интернет-журнал «Мир науки». – 2017. – Том 5, – № 5. – С. 2–4.

3. Сычёв Ю.В. Анализ построения информационно-образовательной среды в военной образовательной организации МО РФ. В книге: Развитие военной педагогики в XXI веке. Материалы VI Межвузовской научно-практической конференции, 100-летию Военной академии связи посвящается. – 2019. – С. 107–113.

4. Ундозерова А.Н. Информационная культура как основа безопасности военнослужащих в учебно-профессиональной деятельности и интернет-коммуникациях. Информационная безопасность личности субъектов образовательного процесса в современном обществе: сб. материалов научно-практической конференции / Авторы-составители: В.Г. Мартынов, И.В. Роберт, И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2022. – С. 245–252.

5. Шерстюк В.П. МГУ: Научные исследования в области информационной безопасности. Информационное общество. – 2005. – № 1. – С. 7–12.

Р.З. Сафиева,

*доктор технических наук, профессор
Российский государственный университет нефти и газа
(национальный исследовательский университет)
имени И. М. Губкина*

КУЛЬТУРНЫЙ КОД КАК ВЫСОКОЭФФЕКТИВНОЕ СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

Цифровая трансформация образования, отличительные черты которой – генерация больших объемов информации и ее доступность в любое время и в любом месте всем участникам педагогического процесса, предполагает изменения основных положений педагогической науки [1]. Следуя предложенному в статье [2] определению педагогики эпохи 4.0 как совместной интеллектуальной деятельности педагога и обучающихся по постижению феноменов природы, социума и техномира, обратим внимание с позиций семиотики на особенности характеризующих эти феномены знаковых систем и, соответственно, различия их кодов. Российский ученый-гуманитарий Ю. М. Лотман – как один из основоположников семиотики [3], выделял различные знаковые системы: разговорные языки как продукт развития человеческой коммуникации, а также искусственные языки, в первую очередь, естественно-научных фундаментальных наук (математики, физики, химии, биологии и др.). Следуя логике семиотики, можно говорить об искусственных языках, возникших как результат инженерной деятельности человека и реализующихся в виде символов и понятий в технических системах в овеществленном мире [4]. В таблице представлена сравнительная характеристика феноменов природы,

социума и техномира по ряду признаков.

Таблица

Характеристика различных феноменов и их кодов

Феномен(ы)	природный(ые)	культурный	
		социальный(ые)	техномира
<i>Сравнительный анализ по ряду признаков</i>			
Источник – результат	эволюции природы	развития социальных институтов, в т. ч. образовательных	инженерной деятельности человека путем применения ТРИЗ ⁵ как средства поиска «идеальных» решений
Знаковая система	искусственные языки естественно-научных дисциплин	разговорные языки	искусственные технические языки инженерных дисциплин
Способ реализации	биологический (самоорганизация)	надбиологический (различные виды коммуникации)	внедрение перспективных технологий
<i>Виды кода</i>			
Пример кода феномена	биологический	культурный	
	ДНК, маркеры чувств (запах, осязание, вкус, слух, зрение)	генетический код профессии	патенты, технические регламенты, стандарты, требования, инструкции

Из высказывания основателя кибернетики А. А. Ляпунова: «Если представить себе, что письмо написано некоторым шифрованным образом, то содержание письма может узнать только человек, владеющий соответствующим шифром» [5], логически вытекает следующее. Постижение содержания «письма» независимо от его типа возможно при владении человека соответствующим языком и кодом, позволяющим известную или неизвестную / непознанную информацию зашифровать / дешифровать. Очевидно, что способ шифрования «письма» – код, который обеспечивает надежный безопасный канал своевременной передачи, усвоения

⁵ ТРИЗ – теория решения изобретательских задач [4].

и применения информации. Для характеристики социальных феноменов и феноменов техномира можно пользоваться термином культурный код в отличие от природных явлений, для которых можно говорить о биологическом коде. Поскольку рассматриваемые явления реализуются в открытых системах, то поиск и расшифровку культурного кода следует проводить в рамках синергетического подхода, прибегая к анализу больших данных, что невозможно без применения информационных технологий [6]. Успешность такого подхода можно проиллюстрировать яркими примерами биологического и культурного кода – это расшифровка генома человека и гипотеза о длинных циклах экономической конъюнктуры, впервые предложенная русским ученым-экономистом Н. Д. Кондратьевым, который связал циклы со сменой технологических укладов [7].

Изначально код выступает в качестве высокоэффективного защитного средства для шифрования / дешифрования любой информации и предохранения ее от искажения и нежелательного дублирования. Эффективность защиты и передачи таких кодов обеспечивается в природе, обществе и техномире совершенно различными механизмами. Ожидаемо, что выявление кода знаковой системы нередко представляет собой чрезвычайно сложную задачу, о чем свидетельствует вся история развития человеческой цивилизации и научного знания – от открытия гелиоцентрической системы мира до постижения тайн строения материи, создания материалов, обладающих уникальными свойствами и др. Система научного и педагогического знания как образовательный социальный институт призвана гарантировать эффективность постижения и передачи культурных кодов в педагогическом процессе. В таком контексте роль педагогики в информационную эпоху 4.0 неизмеримо возрастает, фигура педагога становится центральной как

генератора научно-педагогических идей и организатора образовательного процесса по постижению культурных и природных кодов с целью их передачи новому поколению и сохранности их как феноменов культурного опыта человечества и познания природных явлений. Уместно привести столь актуальное в современной реальности нетривиальное высказывание Отто фон Бисмарка: «Войны выигрывают не генералы, войны выигрывают школьные учителя и приходские священники».

В отношении природных феноменов биологический генетический код – наглядный пример постижения и применения культурного кода как результата человеческой деятельности в знаковой системе биологических наук, который был бы невозможен и в отсутствие другой знаковой системы, такой как разговорная речь. Этот пример шифрования/дешифрования культурного кода в области искусственных языков ярко иллюстрирует путь от развития фундаментального научного результата до технологии возможного редактирования генома и демонстрирует возможности появления новых научных междисциплинарных направлений (молекулярная генетика, биоинформатика, медицинская педагогика и др.), оказывая тем самым мощное влияние на качественное изменение педагогического процесса.

Постижение механизма передачи, усвоения и использования биологической информации показывает, что природой в процессе долгой эволюции выработаны надежные механизмы защиты генетической информации, передаваемой из поколения в поколение различными видами живых существ, благодаря которым многие из них дошли до нас в неизменном виде, а не исчезли в пучине времени, поскольку в природе безопасность – главное условие выживания особи и сохранности биологического вида, к которому она относится.

В педагогическом процессе функцию передачи успешного опыта от старшего поколения младшему осуществляет педагог (учитель), академик РАО В. А. Сластенин, подчеркивая его роль, ввел понятие «генетический код профессии (ГКП)» учителя [8]. Развивая эту мысль, отметим, что ГКП современного преподавателя неразрывно связан с применением информационных технологий как важного инструмента в его педагогической деятельности, существо которой заключается в распознавании культурных и природных кодов, которыми зашифрованы закономерности различных явлений и эффективная их передача младшему поколению. Воспитательная функция как главная составляющая педагогического процесса, конечно, при этом видоизменяется на фоне существенных мощных изменений в коммуникации его участников в цифровом мире, что ставит новые задачи при реализации этой функции педагогического процесса. Любые достижения, как правило, – это результат работы команды, особенно в современных условиях, когда перед страной стоит задача достижения технологического суверенитета при беспрецедентном санкционном давлении внешних сил. Умение работать в команде, организовывать поиск новых инженерных решений с реализацией их на стадии опытно-конструкторской разработки в опытном образце для последующего внедрения в серию и практику предполагает наличие не только профессиональных, но и управленческих и коммуникативных навыков, так необходимых для создания атмосферы продуктивного общения на базе соблюдения принципов инженерной этики и знания особенностей психологии инженерной деятельности. Поэтому подготовка преподавателей высшей школы, имеющих базовое профессиональное образование, как наставников, руководителей проектных команд и воспитателей студентов в стенах вуза, предполагает различные формы

обучения в системе ДПО: от краткосрочного повышения квалификации как в предметной области, так и в области психолого-педагогических дисциплин до получения второго высшего педагогического образования. Курс «Ключевые компетенции преподавателя высшей школы», который в этом году кафедра инженерной педагогики провела для преподавателей Губкинского университета, включает разделы, посвященные трансформации педагогики в эпоху 4.0, вопросам правовой грамотности преподавателя, публикационной активности, проектированию педагогической деятельности. Эти компоненты педагогической деятельности можно рассматривать как составные элементы генетического кода профессии (ГКП) преподавателя. Продолжая эту идею, еще раз отметим, что ГКП современного преподавателя неразрывно связан с активным внедрением информационных технологий как важного инструмента в его педагогическую деятельность, существо которой, как уже было отмечено ранее, – распознавание культурных кодов, которыми зашифрованы закономерности природных и социальных явлений. Еще одна важнейшая составляющая ГКП преподавателя в инженерном вузе состоит в создании новых ранее неизвестных кодов, характерных для техномира, и эффективная их передача – знания по их созданию (знания о знании) младшему поколению, а, возможно, и создание самого знания как результата сотворчества при совместной работе над проектом. Так возникали научно-педагогические школы, составляющие базовую ценность российского образования [9]. Миссия преподавателя как наставника и его воспитательная функция при этом реализуются в процессе профессиональной коммуникации участников и работе над проектом. Таким образом, главная задача перестройки образовательного процесса – усиление роли наставничества путем организации совместной

проектной деятельности в различных формах, традиционной среди которых является вовлечение студентов младших курсов в русло будущей профессии под руководством преподавателей-наставников. Это и есть самое главное мощное воспитательное средство, мотивирующее и стимулирующее студента к инженерной деятельности. Такой подход имеет исторические корни и ведет к высокой самоорганизации студентов, росту коллективной ответственности преподавателей, роль которой трудно переоценить: в масштабном метаисследовании установлено, что это второй по значимости фактор, влияющий на успешность педагогического процесса после первого – правильности оценивания результатов обучения [10]. Можно заключить, что главное в ГКП преподавателя – наставничество, возникшее в русской и советской системе образования, способствующее формированию профессиональных компетенций студентов. Лучшие практики наставничества – предмет обсуждения в рамках курсов повышения квалификации педагогических работников с целью их последующей реализации в непосредственной педагогической деятельности, что кратно повышает шансы воспитания у студентов чувства самоуважения из-за принадлежности к корпусу профессионалов, способных решать сложные инженерные задачи по достижению национального технологического суверенитета, и гордости за профессию инженера.

Литература

1. *Роберт И.В.* Развитие понятийного аппарата педагогики: цифровые информационные технологии образования // Педагогическая информатика. – 2019. – №. 1. – С. 108–121.
2. *Сафиева Р.З.* Культурный код: философско-педагогический аспект // Педагогика. – 2022. – Т. 86. – №. 8. – С. 5–11.

3. Лотман Ю.М. Семиосфера / Ю.М. Лотман. – СПб.: Искусство-СПб., 2000. – С. 395.

4. Альтшуллер Г.С. Творчество как точная наука. – М.: Сов. радио, 1979. – Кибернетика. 105 с.

5. <https://pqm-online.com/assets/files/lib/books/altshuller.pdf> (Дата обращения 24 мая 2023)

6. Ляпунов А.А. О соотношении понятий материя, энергия и информация / А.А. Ляпунов // Алексей Андреевич Ляпунов. 100 лет со дня рождения / Редакторы-составители: Н.А. Ляпунова, А.М. Федотов, Я.И. Фет; отв. ред. Ю.И. Шокин. – Новосибирск: Академическое изд-во «Гео», 2011. – С. 163–167.

7. Малинецкий Г.Г. Синергетика и наука о человеке // Человек. – Изд-во ФГУП «Издательство «Наука», 2018. – №. 3. – С. 5–17.

8. Глазьев С. Ю. Современная теория длинных волн в развитии экономики // Экономическая наука современной России. – 2012. – №. 2 (57). – С. 27–42.

9. Слостенин В.А., Асадуллин Р.М. Формирование личности учителя как субъекта педагогической деятельности // Сибирский педагогический журнал. – 2005. – №. 5. – С. 3–19.

10. Кравченко М.Н., Сафиева Р.З. Научно-педагогическая школа как базовая ценность Российского образования (на примере школы нефтегазовой и подземной гидромеханики Губксинского университета) // Вестник УГНТУ. Наука, образования. экономика; Серия: Экономика. – 2023 – Т. 1, выпуск 43. – с. 133–145.

11. Хэтти Д. Видимое обучение для учителей: как повысить эффективность педагогической работы. – М.: Национальное образование, 2021. – 322 с.

Е. А. Носков,

Частная образовательная организация высшего образования

«Омская гуманитарная академия»

ОПРЕДЕЛЕНИЕ КОМПЕТЕНЦИЙ ПЕДАГОГОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК КОМПОНЕНТА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Использование субъектами образовательного процесса из различных источников распределенного ресурса Интернет в условиях применения технологических средств глобального масштаба неизбежно возникают определенные угрозы и риски для личности, общества и государства. При этом национальная безопасность в сфере образования определяется многими факторами, к которым, прежде всего, следует отнести реализацию стратегических целей, представленных в ряде Государственных документов [1], [2]; [3 и др.]. В разделе 5 Указа Указ Президента Российской Федерации от 12 мая 2009 г. N 537 «Наука, технологии и образование» сформулированы **стратегические цели, в том числе и в сфере образования, реализация которых является одним из основных условий обеспечения национальной безопасности в сфере образования.**

Существенным фактором, влияющим на национальную безопасность в сфере образования, является повсеместное увеличение интенсивности восприятия обучающимися информационных потоков при активизации информационного взаимодействия, включая социальные сети, при использовании интеллектуальных информационных систем и различных технических средств в образовательном процессе. Многие исследователи (А. Л. Димова,

И. Ш. Мухаметзянов, В. П. Поляков, И. В. Роберт и др.) констатируют *возникновение негативного воздействия на социальные отношения между обучающимися, которые значительное время тратят на виртуальное общение в Интернете*, заменяя им реальное общение [4, 5, 6, 7].

Ряд исследователей (А. Л. Димова, И. Ш. Музаметзянов, О. В. Писарь и др.) указывают на то, что на состояние физического и психического здоровья обучающихся влияют: длительное пребывание за компьютером; эмоциональные нагрузки при работе с большими объемами информации, в том числе и учебной; нарушение режимов работы за компьютером, установленных СанПин Минздрава РФ. Анализ позволил также выявить некоторые концептуальные положения *в области здоровьесформирующего образования* [8] и *здоровьесберегающих компонент современного образования* [9]; [10], *которые также составляют содержательную основу национальной безопасности в сфере образования.*

Многие исследователи (С. А. Бешенков, О. А. Козлов, И. Ш. Мухаметзянов, В. П. Поляков, И. В. Роберт, Т. Ш. Шихнабиева и др.) посвящают свои работы выявлению и предотвращению отрицательного воздействия на личность: ярких виртуальных информационных взаимодействий с объектами, представленными на экране; от агрессивной информации порталов, веб-ресурсов, интернет-рекламы товаров и услуг, упорно навязывающих свое мнение или услугу; от различного рода интернет-сообществ, распространяющих нелегитимную или даже запрещенную законодательством информацию. В данном контексте речь идет *об информационной безопасности личности субъектов образовательного процесса, что также является компонентом национальной безопасности в сфере образования* [11,12, 13, 14, 15, 16, 17].

Анализ исследований показал, что при бессистемной, не регламентированной содержательными целями работе с информацией у пользователя возникает так называемая *информационная перенасыщенность, приводящая к ослаблению осознания индивидуумом целевой, структурно-содержательной и морально-ценностной компоненты информации* [18; 19].

Как показывают многие исследования ([20; 21; 22] и др.), позитивную роль для предотвращения возможного негативного воздействия ИКТ на обучающегося играет *ориентация на интеллектуализацию образовательной деятельности*, что также является условием обеспечения национальной безопасности в сфере образования.

В ряде исследований показана необходимость использования обучающимися только легитимной и методически грамотно разработанной педагогической продукции, функционирующей на базе информационных и коммуникационных технологий для обеспечения безопасности ее содержательно-методического уровня и психолого-педагогического назначения [23; 24; 25].

Теоретические подходы к содержанию компетенций будущих педагогов в области информационной безопасности позволяют заключить, что цели подготовки должны включать в себя формирование теоретических знаний и умений, необходимых для будущей профессиональной деятельности, и опыт их практической реализации, необходимый для применения полученных теоретических знаний и умений в профессиональной практике. При этом теоретическая компонента подготовки более устойчива, так как развитие средств ИКТ происходит в существенно быстрее, чем вызванные этим развитием изменения в теоретических аспектах подготовки любых специалистов.

Основываясь на вышеизложенном, сформулируем *цель подго-*

товки студентов в области национальной безопасности в сфере образования как формирование знаний, умений и опыта их реализации в своей практической образовательной и будущей профессиональной деятельности. Реализация вышеозначенной цели основывается на *конвергентном подходе*, который предполагает *эволюционное сближение, частичное совпадение каких-то признаков или свойств независимых друг от друга объектов, процессов, явлений* [26; 27]. При этом *цель подготовки студентов в области национальной безопасности в сфере образования рассматривается* как характеризующаяся конвергенцией следующих *независимых друг от друга компонент*: реализация стратегических целей воспитания индивидуума в духе соблюдения и уважения традиций своей страны, гражданского долга и патриотизма, любви к Родине; обеспечение информационной безопасности субъектов образовательного процесса; реализация условий сохранения физического и психического здоровья обучающихся-пользователей ИКТ; интеллектуализация образовательной деятельности субъектов образовательного процесса; использование обучающимися легитимной педагогической продукции, функционирующей на базе ИКТ, удовлетворяющей педагогико-эргономическим требованиям.

Представим содержание компетенций в области информационной безопасности личности в условиях сохранения здоровья субъектов образовательного процесса.

Знания в области содержательных аспектов обеспечения информационной безопасности личности в условиях сохранения здоровья субъектов образовательного процесса:

- противоправной деятельности в сфере высоких технологий и глобального информационного противоборства;
- возможных угроз информационной безопасности и мер по их

предотвращению, условий безопасности функционирования информационных и телекоммуникационных систем важных объектов инфраструктуры образовательной организации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, функционирования систем информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Знания в области специфики современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней:

- развития науки, технологий и образования на базе индустрии информационных и телекоммуникационных технологий, средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;
- обеспечения и реализации условий для государственно-правового регулирования в области интеграции науки, образования и высокотехнологичной промышленности;
- конкурентоспособных технологий и образцов наукоемкой продукции, организации наукоемкого производства.

Знания в области обеспечения экологической безопасности личности в современном обществе массовой сетевой коммуникации и глобализации:

- стратегических целей обеспечения экологической безопасности и рационального природопользования для сохранения окружающей природной среды и обеспечение ее защиты;
- существующих угроз в сфере экологической безопасности и рационального природопользования и мер по их предотвращению.

Знания в области сохранения здоровья субъектов образовательного процесса и обеспечения здоровьесберегающих компонент сферы образования:

- содержания нормативного, правового, санитарно-гигиенического, методического регулирования обеспечения здоровьесбережения в сфере образования.

Знания в области профилактики терроризма, экстремизма, наркомании и радикальной идеологии:

- содержания основных положений Государственной политики в области противодействия наркопреступности, терроризму и экстремизму и обеспечения координации федеральных органов исполнительной власти и органов государственной власти субъектов Российской Федерации в соответствующих сферах;
- правоохранительных мер по выявлению, предупреждению, пресечению и раскрытию актов терроризма, экстремизма, других преступных посягательств на права и свободы человека и гражданина, собственность, общественный порядок и общественную безопасность, конституционный строй Российской Федерации.

Умения в области реализации основных мер по обеспечению информационной безопасности личности субъектов образовательного процесса, по сохранению физического и психического здоровья обучающихся – пользователей ИКТ:

- использования информационных и коммуникационных технологий для развития и взаимодействия образовательных организаций с научно-исследовательскими центрами, предприятиями и другими заинтересованными субъектами в условиях обеспечения здоровьесбережения в сфере образования;

- применения нормативно-правового, санитарно-гигиенического, методического регулирования обеспечения здоровьесбережения в сфере образования.

Опыт реализации знаний и умений в области выполнения мер по обеспечению информационной безопасности личности, сохранения физического и психического здоровья субъектов образовательного процесса:

- обеспечения информационной безопасности личности в обществе массовой сетевой коммуникации и глобализации;
- применения нормативно-правового регулирования в сфере экологии;
- применения нормативно-правового, санитарно-гигиенического и методического регулирования обеспечения здоровьесбережения в сфере образования;
- разработки и реализации программ обучения в области профилактики наркопреступности, терроризма, экстремизма и радикальной идеологии;
- разработки проектов взаимодействия образовательных организаций с научно-исследовательскими центрами, предприятиями и другими заинтересованными субъектами в условиях обеспечения здоровьесбережения в сфере образования.

Представленное содержание объединяет общекультурная компетенция как способность к реализации информационного направления национальной безопасности в условиях глубокой информатизации всех сфер жизнедеятельности, информационной открытости и глобализации.

Таким образом, под компетентностью педагога в области обеспечения информационной безопасности в сфере образования понимается владение компетенциями как совокупностью знаний в

области основ обеспечения информационной безопасности (понятие информационной безопасности как оставляющей национальной безопасности в условиях глубокой информатизации всех сфер жизнедеятельности, информационной открытости и глобализации; условия обеспечения защищенности персональных данных индивидуума; незаконные действия и деятельность в Интернете; условия и меры по предотвращению возможных угроз распространения лживой информации о российском обществе; основы правового обеспечения информационной безопасности; меры по обеспечению информационной безопасности субъектов образовательного процесса); умений в области реализации средств обеспечения информационной безопасности в образовании (реализации условий обеспечения информационной безопасности в обществе массовой коммуникации и глобализации; обеспечения условий и мер по предотвращению возможных угроз незаконных действий и деятельности в Интернете; выполнения мер по обеспечению информационной безопасности субъектов образовательного процесса, по предотвращению возможных угроз распространения лживой информации о российском обществе); опыта реализации знаний и умений в области основного содержания и реализации средств обеспечения информационной безопасности (противодействия агрессивной информации манипулятивного характера, насаждающей деструктивное асоциальное поведение молодежи; применения основ правового обеспечения информационной безопасности; выполнения мер по обеспечению информационной и технологической безопасности субъектов образовательного процесса; предотвращения возможных рисков, связанных с распространением западными СМИ идей общества потребления, агрессивной, негативной информации, порочащей национальные традиции народов России, ценности отечественного образования).

Литература

1. Концепция национальной безопасности Российской Федерации: [Электронный ресурс] Режим доступа: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkV6BZ29/content/id/589768
2. Стратегия национальной безопасности Российской Федерации до 2020 года: указ Президента РФ [от 31 декабря 2015 г. № 683]. URL: <http://base.garant.ru/195521>
3. Указ Президента Российской Федерации от 12 мая 2009 г. N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»
4. Димова А.Л. Подготовка студентов в области предотвращения негативных последствий использования информационных и коммуникационных технологий в условиях физической культуры // Человек и образование. – 2017. – № 1. – С. 59–63.
5. Мухаметзянов И.Ш. Методические рекомендации по предотвращению негативных медицинских последствий использования ИКТ в образовании. – М.: ИИО РАО, 2012. – 56 с.
6. Поляков В.П. Развитие информационной подготовки в контексте стратегии национальной безопасности Российской Федерации // Научноград наука производство общество. – 2016. – № 2. – С. 46–51.
7. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надежность и качество». – Пенза: Пензенский государственный университет, 2018. – Т.1. – С. 68–71.
8. Писарь О.В. Формирование личной безопасности студентов на основе компетентностного подхода: Дисс. ...доктора пед.наук. Казань, 2009. – С. 448
9. Мухаметзянов И.Ш. Медицинские аспекты здоровьесберегающей информационно-образовательной среды // Казанский педагогический журнал. – 2016. – № 1. – С. 36–45.
10. Мухаметзянов И.Ш. Структура и содержание информационно-образовательного пространства обучаемого. Здоровьесберегающая направленность. // Педагогическая информатика. – 2018. – № 3. – С. 143–156.
11. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надежность и качество». – Пенза: Пензенский государственный университет, 2018. – Т.1. – С. 68–71.
12. Бешенков, С.А., Шутикова, М.И. Образовательные риски современного информационного социума и информационно-когнитивные технологии / С. А. Бешенков, М. И. Шутикова // Информатика и образование. – 2015. – № 8. – С. 19–21.

13. *Козлов, О.А., Поляков, В.П.* Информационная безопасность личности: актуальные педагогические аспекты / О.А. Козлов, В.П. Поляков // Наука о человеке: гуманитарные исследования. – 2018. – № 3 (33). – С. 105–112.

14. *Мухаметзянов И.Ш.* Сохранение здоровья в условиях систематического использования цифровых технологий / Цифровая трансформация образования: теория и практика: монография. – Омск: Изд-во ОмГА, 2022. – С. 28–55.

15. *Поляков В.П.* Цифровая трансформация образования и актуальные аспекты информационной безопасности личности // Человеческий капитал. 2021. – № S5–3 (149). – С. 86–91.

16. *Роберт И.В.* Формирование информационной безопасности личности обучающегося в условиях интеллектуализации его деятельности // Педагогическая информатика. – 2017. – № 2. – С. 42–59.

17. *Шихнабиева Т.Ш.* О некоторых направлениях интеллектуализации информационных систем образовательного назначения // Наука о человеке: гуманитарные исследования. – 2018. – Выпуск 3 (33). – С. 98–104.

18. *Роберт И.В.* Дидактика эпохи цифровых информационных технологий // Профессиональное образование. – 2019. – № 3 – С. 16–26.

19. *Роберт И.В.* Формирование информационной безопасности личности обучающегося в условиях интеллектуализации его деятельности // Педагогическая информатика. – 2017. – № 2. – С. 42–59.

20. *Роберт И.В.* Интеллектуализация интерактивного взаимодействия обучающегося и обучающего со средствами информатизации (на примере алгоритмизации обучения) // Ученые записки ИИО РАО. – М.: ИИО РАО, 2015. – № 56. – С. 5–25.

21. *Robert I.V., Polyakov V.P., Kozlov O.A.* Information security of the personality of the subjects of the educational process // SHS Web of Conferences. 2018. Vol. 55. P. 03011. doi:10.1051/shsconf/20185503011

22. *Шихнабиева, Т.Ш.* Автоматизация процесса обучения и контроля знаний с использованием интеллектуальных моделей образовательного контента // Педагогическая информатика. – 2011. – Вып. 5. – С. 27–31.

23. *Роберт И.В.* Идеализированные модели педагогической продукции, функционирующей на базе информационных и коммуникационных технологий // Ученые записки ИИО РАО. – М.: ИИО РАО, 2013. – Вып. 46. – С. 5–19.

24. *Роберт И.В., Ваграменко Я.А., Граб В.П.* Рекомендации по рецензированию электронных изданий образовательного назначения, используемых в образовательном процессе образовательных учреждений начального

общего, основного общего, общего среднего образования. 2-е изд., испр. и доп. – М.: ИИО РАО, 2013. – 25 с.

25. *Касторнова, В.А.* Методические особенности использования интеллектуальных программных средств для систематизации и контроля знаний / В.А. Касторнова // Педагогическая информатика. – 2019. – № 1. – С. 92–102.

26. *Роберт И.В.* Конвергенция наук об образовании и информационных технологий как эволюционное сближение наук и технологий (для научных сотрудников и преподавателей учреждений профессионального образования): Концепция. – М.: ИИО РАО, 2014. – 54 с.

27. *Роберт И.В.* Конвергентное образование: истоки и перспективы // Наука о человеке: гуманитарные исследования. – 2018. – № 2 (32). – С. 64–76.

Е. В. Никульчев,
доктор технических наук,
профессор кафедры «Интеллектуальные системы
информационной безопасности»,
профессор Российской академии образования

П. Ю. Пушкин,
кандидат технических наук,
заведующий кафедрой «Защита информации»

Е. О. Карамышева,
старший преподаватель кафедры «Защита информации»
МИРЭА – Российский технологический университет

АНАЛИЗ ИНЦИДЕНТОВ С ПЕРСОНАЛЬНЫМИ ДАНЫМИ В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ: 2020 – 2022

В 2022 году законодательство в области обработки и защиты персональных данных претерпело существенные дополнения. Так, например, в Федеральном законе «О персональных данных» появились требования об уведомлении оператором уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) в течение 24 часов о произошедшем инциденте с обрабатываемыми персональными данными. К таким инцидентам, в частности, относятся случаи обнаружения копии баз персональных данных в открытых источниках или получения сообщения об угрозе раскрытия таких баз данных неограниченному кругу лиц [1]. Кроме того, законом предписано в течение 72 часов провести внутреннее расследование случая утечки персональных данных и сообщить о его результатах в Роскомнадзор. Указанные

нормы вступили в силу в марте 2023 года и подчеркнули актуальность своевременного выявления фактов утечки персональных данных, а также причин, способствующих возникновению таких инцидентов.

Для обзора произошедших инцидентов авторами выбрана образовательная сфера, как отдельная отраслевая область, обладающая своими особенностями обработки персональных данных [2]. Образование и наука с 2022 года произвели резкий переход на новый этап развития в связи с новыми вызовами обществу, что потребовало использования современных информационных технологий для сбора и защиты персональных данных. Однако сбор и обработка данных пользователей всегда связаны с угрозами безопасности таких данных.

Рассмотрим случаи утечки персональных данных образовательных организаций, нашедшие отражение в новостных лентах веб-ресурсов и сообщениях тематических телеграмм-каналов.

В соответствии с принятой методикой поиск по веб-ресурсам производился группой экспертов в количестве 30 человек в общедоступных поисковых системах, таких как «Google», «Яндекс», «Mail.ru» по простым и сложным запросам, например, «персональные данные», «утечка данных» и «инцидент / утечка персональные данные университет / школа / колледж». Включение в исследование поисковых систем различных компаний иностранного и российского происхождения позволило увеличить охват новостных сообщений по тематике запросов.

В мессенджере «Телеграмм» определялись каналы, содержащие сведения об инцидентах с персональными данными и их причинах, затем производился поиск по ключевым словам и фразам, аналогичным запросам в поисковых системах.

Полученные данные систематизировались авторами в итоговую таблицу. Анализировались категории и объем базы утекших персональных данных, а также возможные причины возникновения инцидентов. Дополнительно проверялось подтверждение оператором факта произошедшего инцидента с обрабатываемыми персональными данными.

В таблице 1 представлены основные инциденты с персональными данными в образовательных учреждениях за 2020–2022 годы, выявленные экспертной группой. Анализ представленных в таблице инцидентов показывает, что наиболее уязвимыми являются сервисы, реализующие дистанционный доступ пользователей к ресурсам оператора. Основной целью злоумышленников являются контактные сведения субъекта персональных данных, а также реквизиты его доступа к информационным ресурсам оператора.

Таблица 1

№ п/п	Наименование оператора / наличие оператора в реестре	Дата утечки / ссылка на источник	Категория ПДН (ФИО, номер телефона и тд)	Объем базы данных	Примечание
1	«GeekBrains» – Образование в ИТ / Отсутствует в реестре операторов	01.06.2022/[3]	ФИО, адреса электронной почты, номера телефонов	105,8 тыс. строк	Компания подтвердила данные об утечке информации [3]
2	«Яндекс.Практикум» / Присутствует в реестре операторов	14.06.2022/[4]	Яндекс ID; username в системе; ФИО клиента сервиса; адреса электронной почты, номера телефонов	300 тыс. строк	Компания подтвердила данные об утечке информации [4]

Продолжение табл. 1

№ п/п	Наименование оператора / наличие оператора в реестре	Дата утечки / ссылка на источник	Категория ПДН (ФИО, номер телефона и тд)	Объем базы данных	Примечание
3	Уральский институт управления (УИУ) РАН-ХиГС при президенте РФ в Екатеринбурге / Присутствует в реестре операторов	08.05.2022/[5]	ФИО, должность, сведения о доходах	350 строк	Институт подтвердил данные об утечке информации [5]
4	Школа управления «Сколково» / Присутствует в реестре операторов	17.05.2022/[6]	ФИО обучающихся, номера телефонов, места работы и должности, хешированные пароли для входа в систему	420 тыс. строк	Компания подтвердила данные об утечке информации [6]
5	Образовательный интернет-ресурс «Якласс» / Присутствует в реестре операторов	18.02.2022/[7]	ФИО, номера телефонов, адреса электронной почты, логин, хешированный пароль, пол, дата создания и модификации профиля	102 тыс. строк	Компания не подтвердила данные об утечке информации [7]
6	«Skyeng» / Присутствует в реестре операторов	27.07.2020/[8]	ФИО, номера телефонов, адреса электронной почты, ник в Skype	5 млн. строк	Компания не подтвердила данные об утечке информации [8]

Окончание табл. 1

№ п/п	Наименование оператора / наличие оператора в реестре	Дата утечки / ссылка на источник	Категория ПДН (ФИО, номер телефона и тд)	Объем базы данных	Примечание
7	«Навигатор дополнительного образования Нижегородской области» / Присутствует в реестре операторов	14.09.2021/[9]	ФИО, дата рождения, номера телефонов, адреса электронной. почты родителей	более 48 тыс. строк	Нижегородское правительство подтвердило данные об утечке информации [9]
8	«UpStudy» – образовательный онлайн-сервис для поиска репетиторов и тренеров / Присутствует в реестре операторов	12.03.2020/[10]	Стоимость, описание и дата заказа, (ФИО, дата рождения, пол, телефон, почтовый адрес, адрес эл. почты) репетитора и студента, дата регистрации и последнего входа в систему	175,5 тыс. строк	Компания не подтвердила данные об утечке информации [10]
9	НАНО ВО «Институт мировых цивилизаций» / Отсутствует в реестре операторов	31.10.2020/[11]	ФИО, даты рождения, полные паспортные данные, адреса, номера телефонов	5,8 тыс. строк	Институт не подтвердил данные об утечке информации [11]

Ряд операторов подтвердил факт инцидента или заявил о проведении расследования причин утечки данных. Два оператора осуществляли обработку персональных данных без уведомления об этом Роскомнадзора, что может являться нарушением установленного законом [1] порядка обработки персональных данных.

В заключение отметим, что результаты представленного исследования показывают, что в настоящее время операторами не принимаются достаточные меры по защите обрабатываемых ими персональных данных, что особенно чувствительно для образовательной сферы, как одной из наиболее востребованных в постковидный период. Атаки злоумышленников с целью получения персональных данных для их дальнейшего незаконного использования приводят к утечке больших массивов информации, в том числе о несовершеннолетних. Новые изменения в законодательстве о персональных данных требуют разработки отдельных рекомендаций по проведению внутренних расследований выявляемых инцидентов в образовательном операторском сообществе. Кроме того, повышению уровня безопасности обрабатываемых персональных данных будет способствовать создание системы выявления утечек персональных данных в различных сегментах сети Интернет.

Литература

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». – Режим доступа: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261>, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 16.12.2022).
2. Пушкин П.Ю., Русаков А.М. Результаты автоматического интеллектуального анализа отдельных полей реестра операторов персональных данных // International Journal of Open Information Technologies. – 2021. – Т. 9. – № 1. – С. 37–47.
3. Утечка данных в GeekBrains. [Электронный ресурс]. – Режим доступа: <https://tass.ru/obschestvo/14795845> (дата обращения: 16.11.2022).
4. Утечка данных «Яндекс.Практикум». [Электронный ресурс]. – Режим доступа: <https://www.kommersant.ru/doc/5410288> (дата обращения: 16.11.2022).
5. Утечка данных в президентском вузе на Урале. [Электронный ресурс]. – Режим доступа: <https://ura.news/articles/1036284527> (дата обращения: 16.11.2022).

6. Утечка данных бизнес-школы «Сколково». [Электронный ресурс]. – Режим доступа: <https://iz.ru/1336502/2022-05-18/it-kompanii-zaiavili-ob-utechke-dannykh-biznes-shkoly-skolkovo> (дата обращения: 16.11.2022).

7. Телеграмм-канал «Утечки информации». [Электронный ресурс]. – Режим доступа: <https://t.me/dataleak/2508> (дата обращения: 16.11.2022).

8. Телеграмм-канал «Утечки информации». [Электронный ресурс]. – Режим доступа: <https://t.me/dataleak/1741> (дата обращения: 16.11.2022).

9. Утечка данных «Навигатор дополнительного образования Нижегородской области». [Электронный ресурс]. – Режим доступа: <https://www.kommersant.ru/doc/4986303> (дата обращения: 16.11.2022).

10. Телеграмм-канал «Утечки информации». [Электронный ресурс]. – Режим доступа: <https://t.me/dataleak/1877> (дата обращения: 16.11.2022).

11. Телеграмм-канал «Утечки информации». [Электронный ресурс]. – Режим доступа: <https://t.me/dataleak/1929> (дата обращения: 16.11.2022).

РЕАЛИЗАЦИЯ ВОЗМОЖНОСТЕЙ ЦИФРОВОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ДЛЯ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБРАЗОВАНИЯ

Е. В. Лопанова,

доктор педагогических наук, доцент

Частная образовательная организация высшего образования

«Омская гуманитарная академия»

Н. В. Савина,

кандидат педагогических наук, доцент

*Федеральное государственное бюджетное образовательное
учреждение высшего образования «Омский государственный пе-*

дагогический университет»,

Частная образовательная организация высшего образования

«Омская гуманитарная академия»

ГОТОВНОСТЬ ПРЕПОДАВАТЕЛЕЙ ВУЗА К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ

Безопасность как феномен в общем смысле является базовой потребностью человека. Ранее говорилось только о физической и психологической безопасности личности. В настоящее время особое значение приобретает безопасность информационная, являющаяся одной из составляющих национальной безопасности Российской

Федерации и оказывающая влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства [2]. Следует отметить, что надежная информационная безопасность возможна только тогда, когда она строится на совокупности научных принципов [18].

Современное развитие общества необходимо рассматривать, в том числе, через технологические изменения, которые характеризуют четвертую промышленную революцию. Происходит активная цифровая трансформация всех сфер общественной жизни. Под цифровой трансформацией образования будем понимать «...результат процесса возникновения существенных изменений, произошедших в сфере образования (как позитивных, так и негативных), при активном и систематическом использовании цифровых технологий в образовательных целях» [12, с. 10].

В 2018 году сотрудники Высшей школы экономики представили аналитический доклад, в котором обозначили основные проблемы и перспективы цифровой трансформации образования [17]. Авторы разделяют мнение С. В. Куликовой о том, что «...на первом месте здесь должен оказаться аксиологический подход, который позволит в новых технологических условиях сохранить гуманистическую составляющую человека и общества» [7, с. 134].

Аксиологическому подходу в условиях цифровой парадигмы образования посвящен ряд работ академика И. В. Роберт [11, 12, 13]. В них, в частности, представлен достаточно широкий перечень ценностей образования, среди которых новыми ценностями выступают конвергентные (значимость для индивида цифровых технологий) и ценность информационной безопасности личности. Такой подход предопределяет важность изучения мнения различных субъектов образовательного процесса о ценности, понимании и готовности к действиям по защите от информационной опасности.

Обратимся к нормативным документам, регулирующим информационную безопасность на государственном уровне. В Доктрине информационной безопасности Российской Федерации она определяется как «...состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [5].

В этом случае понятие информационной безопасности следует рассматривать в двух сторон [6, с. 31].

1. Как безопасность содержательной части (смысла) – побуждения человека к негативным действиям.

2. Как защищенность информации от внешних воздействий – копирования, уничтожения и др.

Следовательно, можно считать, что информационная безопасность состоит из безопасности информации и защиты информации. То есть, чтобы чувствовать себя безопасным в информационном обществе, необходимо получать безопасную информацию и не бояться, что информация субъекта будет искажена либо использована без должного разрешения. В узком смысле информационная безопасность личности – это «состояние, при котором отсутствует возможность причинения человеку какого-нибудь вреда сведениями из внешнего мира» [18, с. 265]. Некоторые исследователи расширяют структурный состав изучаемого феномена, включая технический, идеологический, психологический, правовой компоненты (Баринов С. В.) [2]. Возникают и новые термины – «духовная безопасность» (А. А. Соколова, С. Н. Соколова) [20], «гуманитарная безопасность» (С. А. Дементьев) [4].

Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, в том числе, основывается на принципе обеспечения государственной защиты интересов российских граждан в информационной сфере. Так, в п. 31 указаны меры для защиты, включая обеспечение баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, учитывая право на личную и семейную тайну [14].

Анализируя указанные исследования в обозначенном проблемном поле, выделим риски обеспечения информационной безопасности, с которыми столкнется личность и в системе образования, и в других сферах жизни в условиях цифровой трансформации. Это обилие разнообразной информации, что затрудняет определение общих ориентиров; воздействие недостоверной, фейковой, агрессивной информации, что приводит к изменению установок личности, девиантному поведению; «утечка» личных данных в общее информационное поле с последующим использованием их другими людьми в криминальных целях; угроза психическому здоровью личности и другие. Отдельно следует выделить цифровой след студента в электронной образовательной среде вуза. Кто может получить доступ к информации о том, как проходит обучение студент? Является ли цифровой след личной информацией студента или эта информация принадлежит образовательной организации?

Возникает вопрос, насколько готовы преподаватели вуза обеспечить информационную безопасность студентов? Под таким обеспечением мы понимаем не распространение преподавателем личной информации о студенте (считаем это недопустимым), а помощь, обучение студентов возможности защитить себя и свои личные данные. Это мнение высказывают многие авторы. Развивать способность к рефлексии и аргументации, критическое

мышление и др. [16], «...формировать и развивать культуру информационной безопасности, трактуемой исследователями и как информационная культура человека, информационная этика, и как культура взаимодействия человека и социума в информационной среде» [9, с. 340]. «Информационная безопасность личности в интернет-пространстве должна базироваться на высоком уровне информационной культуры, которая закладывается на всех уровнях обучения и воспитания в многоуровневой системе отечественного образования, начиная со ступени общеобразовательной школы» [1, с. 290].

Представим промежуточные результаты нашего эмпирического исследования мнений преподавателей вузов по вопросу информационной безопасности (декабрь 2022). Цель исследования: выявить, как преподаватели вузов понимают информационную безопасность и ее источники, а также, насколько они готовы помочь студентам в ее обеспечении.

В исследовании приняли участие преподаватели психолого-педагогических и социальных наук трех вузов города Омска: Омской гуманитарной академии, Омского государственного педагогического университета, Сибирского автомобильно-дорожного университета (n=35). Средний педагогический стаж испытуемых составляет 24,9 лет. Среди них доцентов – 82,9%, профессоров – 5,7%, преподавателей без ученой степени – 11,4%. Приведем основные результаты опроса.

1. 65,7 % респондентов считают, что информационная безопасность – это защита личности от разного рода информации, 74,3% – защита личных данных человека, 2,8% затруднились ответить.

2. На вопрос: «Есть сейчас потребность обучать студентов навыкам информационной безопасности в вузе?», – 91,4% ответили положительно.

3. Только 38,2 % опрошенных выразили личную готовность обучать навыкам информационной безопасности. Наиболее популярным был ответ, что это обязанность преподавателей компьютерных наук (рисунок 1). Результаты отразили узкое понимание преподавателями источников такой опасности, слабое представление о том, что угрозы формирует не только цифровая среда, но иные сферы жизни человека, погружающие его в информационное поле. Из определения информационного общества – «информационное общество – общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан» [14, п. 4], – не следует, что цифровые технологий не являются основным источником информации, хотя, безусловно, основным.

3. Если Вы считаете, что нужно обучать, то кто это должен делать?

34 ответа

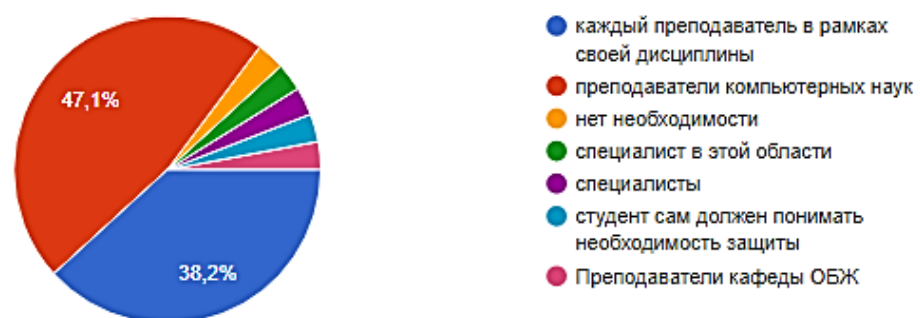


Рис. 1. Обучение студентов навыкам информационной безопасности

4. Преподаватели в основном не считают себя информационно защищенными (рис. 2). Это тревожный факт, т.к. уровень образования респондентов, и не только профессионального, высокий.

4. Считаете ли Вы себя информационно защищенным?

35 ответов

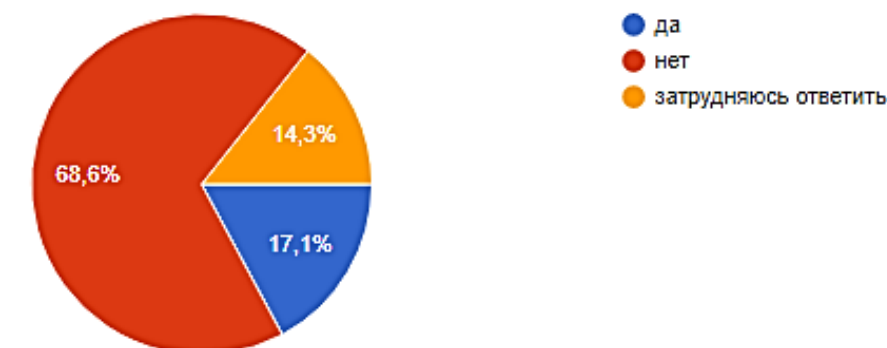


Рис. 2. Информационная защищенность преподавателей

5. Примечательно, что защита личных данных оказывается важнее защиты от негативной информации (рис. 3). В комментариях опрошенные писали, что они в состоянии отличить негативное информационное воздействие самостоятельно, но защиту личных данных сами обеспечить не всегда могут.

5. Что для Вас важнее

35 ответов

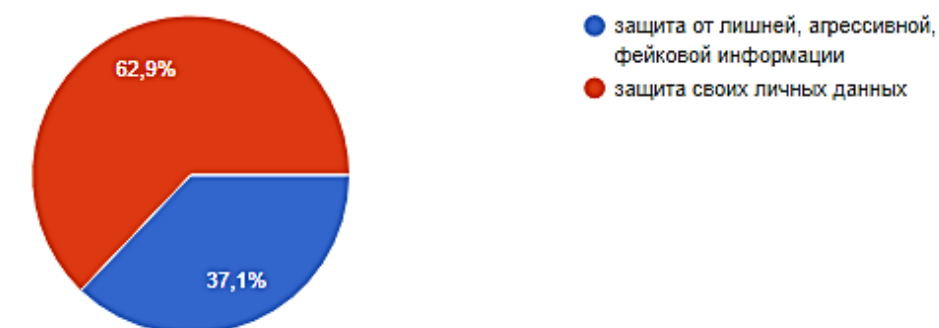


Рис. 3. Значимость аспектов информационной безопасности

6. Самый важный вопрос, касающийся готовности помочь студентам в вопросе информационной безопасности, показал, что только 25,7% могут это сделать, что соотносится с результатами рис. 2, где всего 17,1% респондентов считают себя защищенными.

Другими словами, неуверенный в этом вопросе преподаватель не может помочь другим, что естественно.

6. Вы лично готовы сейчас обучать студентов навыкам информационной безопасности?

35 ответов

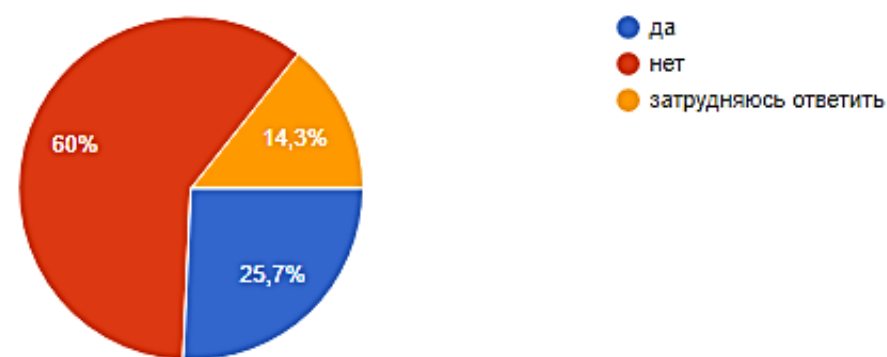


Рис. 4. Готовность к обучению студентов

7. Но уже большее количество преподавателей (51,4%) выразили готовность повысить свою квалификацию в этой области знаний (рис. 7), что показывает необходимость организации такой работы в вузах.

7. Вы хотите пройти курсы повышения квалификации по вопросам информационной безопасности?

35 ответов

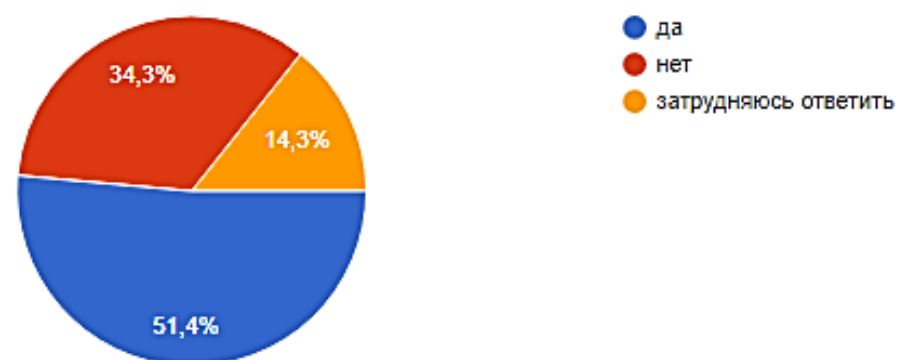


Рис. 5. Желание повысить квалификацию

8. Интерес представляют ответы на вопросы, касающиеся источников информационной опасности (рис. 6, 7).

8. Укажите источники информационной опасности для Вас?

35 ответов

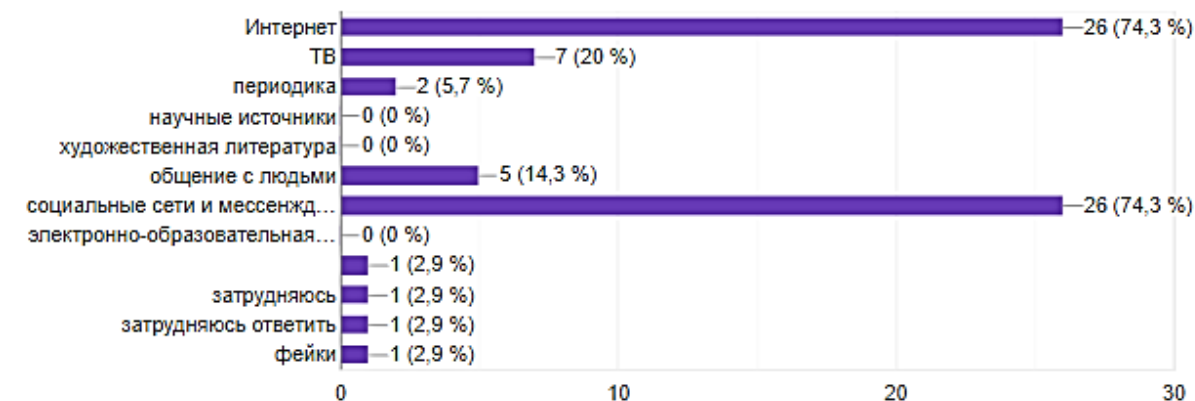


Рис. 6. Источники информационной опасности для преподавателей

9. Укажите источники информационной опасности для студентов?

35 ответов

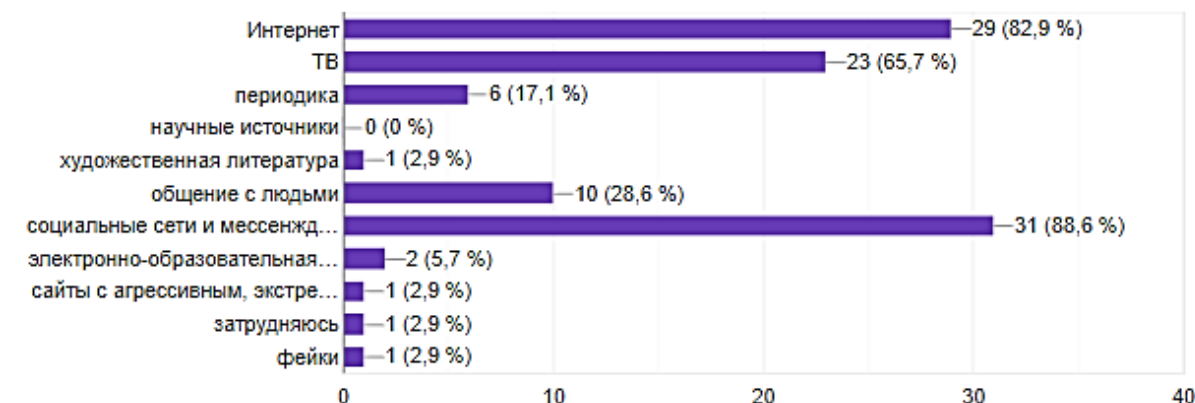


Рис. 7. Источники информационной опасности для студентов

Значительной разницы между угрозами для преподавателей и студентов нет. Однако в два раза больше преподавателей считают, что телевидение влияет на студентов сильнее, чем на преподавателей. Данная разница статистически достоверна ($\phi^*_{эмп} = 3.745$ при $\phi^*_{кр} = 2,31$). Это интересный факт, который можно проанализировать с двух сторон. Во-первых, молодежь как социальная группа

реже смотрит телевизор, основным источником информации для них является Интернет. Вероятно, даже незначительное потребление телевизионной информации считается преподавателями вредной для молодежи. Во-вторых, неизвестно, кто подвержен больше влиянию информации – взрослые, образованные, но уже достаточно консервативные люди или молодые студенты с не совсем сформировавшимися убеждениями, зачастую нигилисты. И та, и другая социальная группа обладает определенным «отторжением» нового, нежеланием подчиняться мнению другого. Но вместе с тем, они зависимы от авторитетов в отдельных значимых для них областях. В научном сообществе ценится мнение признанных ученых, в молодежной среде – публичных выразителей молодежных ценностей, в частности блогеров.

Результаты позволяют выделить два основных источника опасности: Интернет и социальные сети и мессенджеры. Именно они способны генерить возможные риски для личности. В частности, П. С. Пухно, М. В. Лапсарь предупреждают: «... информация и информационные технологии могут использоваться как мощнейший инструмент оказания воздействия на личность человека, проникновения в неё в целях трансформации. Манипуляция сознанием, как отдельного человека, так и большой массы людей является общепризнанным инструментом политики, маркетинга, идеологии. Посредством подачи информации в определённой форме, виде, различными инструментами личность может незаметно попадать под влияние и трансформироваться так, как необходимо актору такого воздействия» [10, с. 89].

Аналогичное мнение высказывает А. С. Горбунов: «... помимо возможности воздействия со стороны средств массовой коммуникации на личность (на её сознательную, волевою, потребностную составляющие, на её индивидуальность и свободу, на её мировоз-

зренческие основы) – помимо этого состоявшийся уровень развития массово-коммуникационных технологий и цифровой обработки Больших данных предоставляет возможность контролирования личности. В первую очередь её поведения» [3, с. 14].

Ранжирование источников информационной опасности представлено в таблице 1, где разница рангов наглядно показывает отличия между субъектами образовательного процесса.

Таблица 1

Ранги значимости источников информационной опасности у студентов и преподавателей

Ранг значимости у студентов	Источники информационной опасности	Ранг значимости у преподавателей	Разница рангов
1	социальные сети и мессенджеры	1,5	-0,5
2	Интернет	1,5	0,5
3	ТВ	3	0
4	общение с людьми	4	0
5	периодика	5	0
6	электронно-образовательная среда вуза	8	-2
7,5	художественная литература	8	0,5
7,5	другое	6	1,5
9	научная литература	8	1

Для студентов выше угрозы, чем для преподавателей, от социальных сетей и мессенджеров, а также электронной образовательной среды вуза, хотя ее упоминание незначительно. Такая среда вуза должна быть безопасной, тем не менее ряд исследователей видят в ней некоторую угрозу, как конфликт между «планом выражения и планом содержания» контента [19, с. 28]. Для преподавателей несколько выше риск опасности, идущих от отдельных источников, упомянутых в разделе «другой ответ»: фейки, сайт с агрессивным, экстремистским контентом, а также научной литературы.

9. Отметим как важный факт, что основные источники угрозы информации для личности связаны с цифровой трансформацией

общества и образования. Здесь приведем точку зрения Т. В. Закупень, которая утверждает, что информационная безопасность представляет собой социальное, а не чисто техническое явление. Ее нельзя отождествлять с применением специальных технических средств и методов для защиты информации от несанкционированного доступа, похищения, уничтожения и т.д. [6, с. 31]. Эту же мысль высказывают М. И. Шутикова, Н. В. Шелковникова, И. И. Мамаев: «...проблема обеспечения информационной безопасности личности тесно связана с общим кризисом культуры и ее подменой во всех проявлениях технологиями» [19, с. 29]. Наши прошлые исследования показывают, что преподаватели вузов согласны с тем, что цифровая трансформация общества и образования изменила нравственный идеал российского общества [8]. Здесь можно говорить о риске воспитания нравственного идеала студента, если он находится в зависимости не столько от качества техники, сколько от содержания контента, хотя качество цифровых технологий позволяет распространять нежелательный контент практически повсеместно. Однако, прежде всего такой контент (агрессивный, экстремистский, унижающий и т.п.) создают и распространяют люди, которые не отличаются высокой нравственностью. Также заметим, что Стратегия цифровой трансформации отрасли науки и высшего образования указывает на низкий уровень цифровых компетенций ППС и обучающихся [15, с. 217], что также подтверждает необходимость специального тематического обучения преподавателей вузов.

Обобщим эмпирические результаты на примере усредненного респондента. Отвечал на вопросы анкеты провинциальный преподаватель дисциплин гуманитарного блока высшей школы РФ с педагогическим стажем 25 лет, который считает себя информационно незащищенным, особенно в области защиты личных данных.

Он уверен, что необходимо обучать навыкам информационной безопасности студентов, но делать это должны преподаватели компьютерных наук. Лично он сейчас это делать не в состоянии, но готов пройти курсы повышения квалификации. Среди источников информационной безопасности наиболее влиятельными, по его мнению, являются Интернет и социальные сети и мессенджеры (как для него, так и для студентов). Примечательно, что воздействие телевидения на студентов он оценивает намного выше, чем на себя. Возможное негативное воздействие электронной информационно-образовательной среды вуза отмечает незначительное количество преподавателей, хотя вопрос требует рассмотрения на уровне как высококачественного образовательного контента, так и на уровне рассогласования формы и содержания.

В качестве выводов можно отметить, что информационная безопасность достаточно давно стала предметом рассмотрения ученых различных направлений, находит отражение в многочисленных документах государственного уровня. На личностном уровне в общем виде она представляет собой сочетание безопасной информации, которой пользуется человек, и защиты его личных данных. Цифровая трансформация общества в целом и системы образования в частности усилила риски незащищенности субъектов. Среди них выделяются: трудности определения общих ориентиров; изменение установок личности, девиантное поведение; использование личных данных другими людьми в криминальных целях; угроза психическому здоровью личности; снижение уровня нравственной воспитанности и другие. Мы считаем, что несмотря на то, что фиксируется отсутствие необходимых компетенций у преподавателей вузов, каждый преподаватель может обеспечить формирование и развитие навыков информационной безопасности, также согласны с мнением коллектива авторов, что «основы информационной

безопасности личности должны обязательно отражаться в требованиях Федеральных государственных образовательных и Профессиональных стандартов, начиная с первых уровней образовательной системы (дошкольной и школьной), закладываться в основу учебных планов и программ обучения на всех ступенях многоуровневой системы отечественного образования» [1, с. 291].

На основании вышеизложенного считаем необходимым целенаправленное изучение информационной безопасности личности всех субъектов образовательного процесса вуза с целью формирования и развития навыков и информационной культуры.

Литература

1. Астапенко Ю.В., Поляков В.П., Романенко Ю.А. Информационная безопасность личности на современном этапе трансформации образования // Труды международного симпозиума «Надежность и качество». – 2021. – Т. 1. – С. 288–291.
2. Баринов С.В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. 2016;(4):97–105. <https://doi.org/10.17803/1994-1471.2016.65.4.097-104>.
3. Горбунов А.С. Личность и цифровые технологии в информационном массовом обществе / А.С. Горбунов // Вестник МГОУ. Серия: Философские науки. – 2018. – № 4. URL: <https://cyberleninka.ru/article/n/lichnost-i-tsifrovye-tehnologii-v-informatsionnom-massovom-obschestve>.
4. Дементьев С.А. Гуманитарная сущность информационной безопасности личности // Общество и право. – 2017. – №1(59). – С 182–185. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/gumanitarnaya-suschnostinformatsionnoy-bezopasnosti-lichnosti>
5. Доктрина информационной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646). Российская газета. – [Электронный ресурс] Режим доступа: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html>
6. Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности РФ // Инфор-

мационные ресурсы России. – 2009. – № 4. – С. 28–34.

7. Куликова С.В. Базовые ценности воспитания молодежи в информационном обществе: теоретико-методологический аспект // Сборник научных трудов Международной научно-практической конференции «Воспитание и социализация молодежи: потенциал историко-педагогического познания в контексте вызовов современности» под редакцией М.В. Богуславского, С.В. Куликовой, К.Ю. Милованова. – Волгоград: Издательство: ГАУ ДПО «Волгоградская государственная академия последипломного образования», 2018. – С. 129–134.

8. Лопанова Е.В., Савина Н.В. Динамика ценностей воспитания в условиях цифровой трансформации образования // Информационная безопасность личности субъектов образовательного процесса в современном обществе: сб. материалов научно-практической конференции / Авторы-составители: В.Г. Мартынов, И.В. Роберт, И.Г. Алехина. – М.: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2022. – С. 75–84.

9. Матвеева Е.Ю., Матвеев И.И. Информационная безопасность личности: когнитивный и гуманитарный аспект // Сборник трудов Всероссийской научной конференции «Этологический аспект информационных гражданских войн: история и современность». Под научной редакцией В.Ш. Сабирова. – 2020. – С. 332–342.

10. Пухно П.С., Лансарь М.В. Влияние информации и информационного общества на личность. К вопросу об актуальности психологического исследования // Гуманитарные, социально-экономические и общественные науки. – 2022. – № 10. – С. 87–90.

11. Роберт И.В. Аксиологический подход к развитию образования в условиях цифровой парадигмы // Педагогическая информатика. – 2020. – № 2. – С. 89–113.

12. Роберт И.В. Развитие аксиологии образования периода цифровой трансформации // Человеческий капитал. – 2021. – Т.2. № 12 (156). – С. 9–14.

13. Роберт И.В. Цифровая трансформация образования: вызовы и возможности совершенствования. // Информатизация образования и науки. – 2020 – № 3 (47) – С. 3–16.

14. Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы – [Электронный ресурс] Режим доступа: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687>

15. Стратегия цифровой трансформации отрасли науки и высшего образования – [Электронный ресурс] Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_390417/.

16. Тимошенко Т.В. Когнитивные аспекты информационно-психологической безопасности личности // Известия ЮФУ. Технические науки. – 2010. – № 9. – С. 185 – 188. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/kognitivnye-aspektyinformatsionno-psihologicheskoy-bezopasnosti-lichnosti>

17. Трудности и перспективы цифровой трансформации образования / А.Ю. Уваров, Э. Гейбл, И.В. Дворецкая и др.; под ред. А.Ю. Уварова, И.Д. Фрумина; Нац. исслед. ун-т «Высшая школа экономики», Ин-т образования. – М.: Изд. дом Высшей школы экономики, 2019. – 343 с.

18. Усачев А.В. Информационная безопасность личности в историко-философской перспективе // Сборник материалов Всероссийской научно-практической конференции. «Россия в XXI веке в условиях глобальных вызовов: проблемы управления рисками и обеспечения безопасности социально-экономических и социально-политических систем и природно-техногенных комплексов». Российская академия наук, Международный независимый эколого-политологический университет, Государственный университет управления. – Москва, 2022. – С. 264–268.

19. Шутикова М.И., Шелковникова Н.В., Мамаев И.И. Информационная безопасность личности в цифровой образовательной среде: общие проблемы и конкретные решения // Вестник МГПУ. Серия: Информатика и информатизация образования. – 2020. – № 2 (52). – С. 28–34.

20. Sokolova A.A., Sokolova S.N. Spiritual security of society: information culture of the individual and cultural universals // Bulletin of Polessky State University. Series in Social Sciences and Humanities. 2020. № 1. С. 78–83.

В. А. Касторнова,

кандидат педагогических наук, доктор философии в области информатизации образования, доцент

Федеральное государственное бюджетное научное учреждение «Институт стратегии развития образования Российской академии образования»

КОНЦЕПТУАЛЬНЫЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ С СОБЛЮДЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Цифровые технологии, получая все большее распространение, во многом определяют развитие общества, существенно влияют на экономические, социальные и культурные аспекты. Очевидно, что и образовательные процессы должны проистекать в русле современных и перспективных направлений развития цифровых технологий, предлагая новые способы обучения, общения, обмена и сотрудничества, привнося новые содержательные и методические подходы в образование, адекватные сложившимся вызовам технологического общества. Наметившийся «цифровой сдвиг» предполагает продуманное применение цифровых технологий в школах, позволяющее повысить цифровую грамотность учащихся при обязательном соблюдении информационной безопасности личности и сформировать понимание ими гражданской ответственности в современную эпоху.

Игнорировать общественные преобразования и новые возможности, которые цифровые технологии предлагают образованию, недопустимо, как и оставаться равнодушным к той роли, которую

начинает играть во всех сферах нашего общества искусственный интеллект. Искусственный интеллект нашел отражение в школьной программе [2] и в содержании подготовки студентов [1], в том числе – будущих учителей, чтобы подготовить их к школе завтрашнего дня [13] с учетом всех аспектов соблюдения информационной безопасности личности.

Вклад ИИ в образование далеко не определен. Однако следует отметить, что речь идет не о полной замене традиционных педагогических технологий некими математическими алгоритмами, реализующими возможности ИИ, а об их потенциальных преимуществах в сфере преподавания и обучения. Педагогическая триада, включающая в себя учителя, ученика и знания, а также отношения между ними (дидактические, педагогические и обучающие), потенциально могут быть затронуты ИИ [20]. Рассмотрим элементы триады и отношения между ними в аспекте возможного влияния на них ИИ с учетом обеспечения информационной безопасности личности.

Учитель. Наиболее сложным является вопрос: сможет ли ИИ заменить учителя? С точки зрения стремительного технологического прогресса – нет. В современных отечественных и зарубежных педагогических исследованиях отмечается, что воспитатели дошкольных учреждений, учителя начальной и средней школы входят в число пяти профессий, на которые автоматизация повлияет меньше всего [17]. Использование ИИ естественным образом ведет к развитию нескольких технологий, которые, вероятно, заменят повторяющиеся и относительно предсказуемые задачи учителей. Однако, работа учителя XXI века выходит далеко за рамки автоматизируемых задач. Человек обладает качествами, которые трудно воспроизвести в ИИ. В их числе сочувствие, доброжелательность, критическое суждение, когнитивная гибкость и другие

навыки общения. Таким образом, рабочие места, связанные с человеческими отношениями, будут защищены от гипотетической замены человека роботом с развитым ИИ. Это верно и по причинам технологических ограничений, присущих ИИ, а также потому, что человек потенциально может предпочесть взаимодействие с равным себе, а не с ИИ. В этом случае, помимо замены определенных повторяющихся и относительно предсказуемых задач, ИИ может оказать значительное влияние на педагогическую практику с помощью множества дидактических инструментов, которые помогают автоматизации построения суждений и, как следствие, влияют на педагогический выбор.

Учащийся. Разработчики программного обеспечения уже давно создают продукты, дополненные инструментарием ИИ, которые могут помочь процессу обучения. Например, MOOC (массовые открытые онлайн-курсы) [3] пользуются заслуженным успехом. С их помощью учащиеся могут постигать то, что они хотят, когда хотят, и, самое главное, в удобном темпе. Однако это изобилие возможностей и свободы может создавать некоторую путаницу в отношении того, что изучать и в каком порядке действовать. Зачастую учащиеся не знают, что они хотят изучать – у них нет опыта учителя, который может структурировать и оптимизировать этапы обучения. Кроме того, учащиеся не осознают важности обеспечения информационной безопасности своей личности. Все сказанное часто приводит к демотивации и отказу от самого процесса обучения. ИИ может помочь предотвратить это явление. Используя данные, собранные в личном кабинете учащегося, ИИ может предложить последовательность уроков или упражнений, которые наиболее актуальны для ученика. Кроме того, чтобы противостоять возможному падению мотивации, встроенные интеллектуальные помощники могут предска-

зывать, когда ученик начинает терять интерес и уведомлять об этом учителей.

Знания. С позиции накапливаемого личностью интеллектуального багажа не делается различия между знаниями, навыками или любой другой классификацией его составляющих. Влияние ИИ обуславливает определенный набор знаний, который учащиеся должны освоить, чтобы понять и использовать ИИ. Этот аспект не часто упоминается, когда речь идет о влиянии ИИ на образование, но, безусловно, ставит вопросы о содержании учебных программ по различным предметам, напрямую или косвенно затрагивающих область ИИ. Независимо цели – удовлетворение потребности в знаниях или развитие критического мышления учащихся при использовании этой технологии – важно, чтобы программы обучения были адаптированы. Несмотря на то, что многим понимание того, как работает ИИ, кажется очень сложным и предназначенным для небольшой группы специалистов, некоторые понятия, связанные с ИИ, уже преподаются, хотя в ряде случаев их включение в учебные программы вызывает сомнения.

Что касается отношений между учеником, учителем и знаниями, возможно, некоторые задачи, выполняемые учениками, можно автоматизировать или по крайней мере оптимизировать с помощью ИИ. Однако речь должна идти об осознанном выборе на каждом определенном уровне образования, чтобы, как и любая технология, ИИ приносил пользу и при этом соблюдалась информационная безопасность личности. Помимо инструментов мониторинга учащихся ИИ может привести или усовершенствовать определенные инструменты для производства и обработки информации на всех уровнях реализации информационных процессов. Рассмотрим пример автоматической проверки орфографии текста как рабочего инструмента, который со временем совершенствовался. В ранних

версиях возникала ситуация, когда некоторые варианты исправления текста не очень согласовывались с намерениями автора. Сбор и анализ большого количества текстов с использованием науки о данных позволили повысить его эффективность. Сегодня мы пользуемся инструментом автоматической коррекции, который уже удовлетворяет многим образовательным потребностям. Некоторые инструменты даже нацелены на оценку содержания текста на основе predetermined тегов [24]. Потенциал инструментов обратной связи в лингвистической сфере становится очевидным с появлением искусственного интеллекта, т.е. ИИ смог выйти далеко за рамки простого исправления предложений.

Еще одним важным трендом в использовании искусственного интеллекта является адаптивное обучение. При адаптивном обучении технологии, прежде всего, позволяют легко и динамично адаптировать траектории обучения в соответствии с потребностями и характеристиками учащихся. Таким образом, адаптивное обучение – это образовательный метод, использующий ИИ для организации обучения в соответствии с индивидуальными навыками или потребностями каждого учащегося [16]. Система может не только варьировать контент по степени сложности, но и добавлять или удалять его. Концепция проста: траектории обучения постоянно развиваются в соответствии с ответами учащихся, их потребностями, характеристиками и т.д. (например, так называемые умные цифровые книги от Pearson [12] или McGraw-Hill [18]). Платформа Classcraft [7] позволяет учителям организовать ролевую игру, в которой ученики воплощают разных персонажей. Цифровой инструмент позволяет стимулировать командную работу, улучшать поведение учащихся в классе и повышать мотивацию. В рамках проекта [7], вооружившись данными, собранными в классе, можно использовать ИИ, чтобы помочь учителям управлять учебным процессом.

ИИ особенно широко ежедневно используется учащимися и преподавателями в приложениях на мобильных телефонах [8] или при проведении исследований в сети Интернет. Например, приложение Duolingo [10] с его системой распознавания голоса – это цифровой инструмент с ИИ, который широко используется в образовании. Данная интеллектуальная платформа, предназначенная для изучения языков, популярна во всем мире и применяется учителями для повышения качества проводимых уроков. В данном случае ИИ позволяет, в частности, адаптировать учебную деятельность в соответствии с текущим знанием языка. Существуют и другие подобные платформы, такие как My Coach Bescherelle [19] – приложение для обучения правописанию, которое адаптируется к уровню учащегося. В настоящее время все больше образовательных учреждений используют программное обеспечение, использующее ИИ для обнаружения плагиата в творческих работах. Например, Turnitin [22] использует ИИ для определения степени плагиата в эссе, рефератах, курсовых и пр. работах.

Современные исследователи [20] прогнозируют увеличение числа интеллектуальных помощников, призванных оказывать разнообразную помощь учителям в их профессиональной деятельности. Действительно, собирая школьные данные и объединяя их с учебными привычками учащихся, некоторые алгоритмы смогут адаптировать программу обучения, которая будет способствовать образовательной дифференциации. Например, программа будет способна за короткое время классифицировать учащихся по наиболее эффективным для них методам работы. Такой подход, который раньше занимал много времени при наблюдении, сборе данных и статистических расчетах, может быть оптимизирован с помощью ИИ, повышая влияние преподавания на обучение учащихся. В этом контексте ИИ не заменяет, а скорее усиливает значимость учителя

для учащихся [6].

Перечислим некоторые преимущества использования ИИ в образовании.

1. ИИ позволяет персонализировать обучение, используя, например, платформу Usage des Technologies de l'Information pour la Formation des Enseignants – UTIFEN [23] (<https://www.utifen.org>) и другие инструменты, способствуя академическим успехам учащихся, что и стремится показать данная платформа.

2. ИИ позволяет автоматически исправлять определенные виды работ (эссе, реферат и пр.), тем самым освобождая учителям время на решение других учебных задач.

3. ИИ способствует непрерывной оценке учащихся. Учебный опыт, полученный при использовании ИИ, позволит проследить за учащимся на протяжении всего его учебного пути и с относительной точностью узнать уровень его компетентности в конкретный момент.

4. ИИ может позволить учителям корректировать учебные материалы, что реализовано, в частности, на платформах Coursera [9] и MOOC [3], которые информируют учителя в случае появления большого количества неправильных ответов на вопрос или задание.

5. ИИ позволяет внедрять интеллектуальные системы на платформах дистанционного обучения. Появляется все больше и больше платформ дистанционного обучения, на которых используются услуги интеллектуальных помощников.

6. ИИ меняет то, как мы взаимодействуем с информацией. Например, Google адаптирует результаты поиска в соответствии с нашей геолокацией или предыдущим поиском. Система распознавания голоса Siri от Apple адаптируется к потребностям и запросам и т.д.

7. ИИ увеличивает возможности обратной связи для учащихся,

как в случае с платформой UTIFEN [23], где учащиеся получают от нее персонализированные текстовые сообщения, связанные с их траекторией обучения. С помощью ИИ обратная связь может быть не только персонализирована, но и осуществляться быстрее, чаще и т.д.

8. ИИ упрощает адаптацию учебного контента, как в случае с цифровыми книгами издательств Pearson [12] и McGraw-Hill [18].

9. ИИ расширяет возможности для общения и сотрудничества между учащимися.

10. ИИ позволяет увеличить взаимодействие между учащимся и учебным контентом, в частности, с чат-ботами, этими коммуникационными интерфейсами между человеком и программным обеспечением.

11. ИИ может преобразовать работу учителя, предоставив ему, например, играть роль помощника, а не передатчика знаний (учебного материала). Однако следует при этом помнить, что роль учителей остается центральной, а использование ИИ только поддерживает их в решении сложных задач.

12. ИИ может облегчить персонализированную помощь в выполнении домашних заданий, связанных с академическими проблемами, с которыми сталкиваются учащиеся. Этими возможностями обладает Allprof [4] – платформа, предназначенная для помощи в выполнении домашних заданий.

13. ИИ может способствовать использованию в образовании так называемых иммерсивных технологий (immersive – «создающий эффект присутствия, погружения»), которые обычно определяют как погружение в определенные, искусственно сформированные условия; она включает в себя дополненную реальность AR, виртуальную реальность VR, смешанную реальность MR и искусственный интеллект AI), таких как виртуальные учебные

среды или виртуальные миры. Например, образовательное использование игры Assassin's Creed позволяет молодым людям изучать историю, будучи героем (виртуально) исторических событий [15]. Таким образом, иммерсивные технологии позволяют учащимся получать более насыщенный и интерактивный опыт, что направлено на непосредственное продвижение их обучения.

14. ИИ может позволить школам предотвращать отсев из школы, в частности, на основе данных, уже собранных от учащихся. Кроме того, ИИ позволяет школам быстрее собирать информацию об учениках, находящихся в группе риска, и, таким образом оперативно оказывать им соответствующую помощь.

15. ИИ может еще больше повысить популярность дистанционного обучения, позволяя учащимся получать знания из любого места и в любое время, а также в рамках индивидуального обучения. Это немного из того, что, например, Duolingo [10] предлагает для изучения языков.

16. ИИ также может предоставить учащимся возможность самим управлять учебным процессом, способствуя учебе. Эту возможность им обеспечивает платформа Classcraft [7].

17. ИИ может расширить возможности игровых методов преподавания (геймификации образования), что напрямую способствует мотивации (вовлечению) учащихся.

18. ИИ может упростить выполнение административных школьных задач, таких как таблицы успеваемости, отсутствие учащихся и т.д.

19. ИИ позволяет определять, хотя бы частично, настроение учащихся и, таким образом, предоставлять важную информацию учителю, чтобы он мог адаптировать свое педагогическое мастерство.

20. При использовании ИИ сбор и архивирование данных приобретают первостепенное значение в обучении не только по эти-

ческим, но и по образовательным вопросам.

21. ИИ может оказать ценную помощь всем учащимся, особенно тем из них, кто старается получить больше знаний, чем предусматривает школьная программа.

22. Благодаря ИИ многие задачи, считающиеся важными в образовании, будут автоматизированы интеллектуальными системами.

23. Благодаря ИИ роботы-помощники будут все больше и больше присутствовать в классах не для того, чтобы заменить учителей, что демонстрируется в некоторых художественных фильмах, а скорее для того, чтобы прийти на помощь учителю в его задаче [14], какой бы сложной и трудоемкой она ни была.

Необходимость подготовки будущих учителей к приходу ИИ в образование обусловлена несколькими причинами. Поскольку ИИ влияет на нашу индивидуальную и коллективную жизнь, необходимо развивать критическое отношение к его использованию. Поэтому обучение учителей владению ИИ означает работу по предотвращению потенциальных злоупотреблений, которые могут произойти в ближайшем будущем. Кроме того, это поможет реализовывать информационную безопасность личности всех участников образовательного процесса. Вследствие того, что появление интеллектуальных роботов изменит будущие рабочие места, необходимо готовить учащихся к новым реалиям уже с порога начальной школы. Важно не оставлять эту область на откуп технологическим компаниям. ИИ повсеместно используется в образовании: умные книги, поисковые системы, образовательные приложения, обучающие платформы и т.д. Его приход следует четко обозначить и осознать всеми субъектами образования, начиная с учителей и учащихся. Некоторые эксперты [5] считают, что ИИ может представлять опасность, если общество не установит ограничения на использование интеллектуальных машин. Также важно, чтобы

люди, не входящие в технологические сообщества, были вовлечены в решение этого вопроса [13].

По мнению автора, не следует рассматривать ИИ как парадигму современного образования, это всего лишь инструмент, обладающий большим потенциалом, который необходимо реально оценивать и понимать, как использовать на образовательном уровне [21] с обязательным соблюдением информационной безопасности личности. Одна из задач, стоящих перед образовательной системой, столкнувшейся с появлением ИИ, состоит в том, чтобы найти правильный баланс между сохранением традиционных аспектов, которые веками делали образование всеобъемлющим, и использованием новых возможностей, предлагаемых ИИ [11]. Если не ограничиваться утилитарным видением ИИ, четко определяя области, которые он может усовершенствовать, полезные свойства ИИ позволят повысить академические успехи учащихся и не будут противодействовать межличностному общению.

Литература

1. Модуль «Системы искусственного интеллекта». Письмо Министерства науки и высшего образования РФ от 2 июля 2021 г. N МН-5/2657 «О направлении информации» [Электронный ресурс] // URL: <https://www.garant.ru/products/ipo/prime/doc/401364914/> (дата обращения: 18.03.2020).
2. Национальная стратегия развития искусственного интеллекта в России [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/Статья:Национальная_стратегия_развития_искусственного_интеллекта (дата обращения: 18.03.2020).
3. Что такое MOOC (Массовые открытые онлайн курсы) [Электронный ресурс] // URL: <https://etu.ru/ru/on-line-obuchenie/mooc> (дата обращения: 18.03.2020).
4. Alloprof [Электронный ресурс] // URL: <http://alloprof.qc.ca> (дата обращения: 18.03.2020).

5. *Bilodeau, M., Yoshua Bengio* (2018). Monsieur intelligence artificielle. Québec science, (janvier-février), 61.

6. *Bovo, Angela & Sanchez, Stéphane & Heguy, Olivier & Duthen, Yves.* (2013). L'apprentissage automatique comme base du suivi d'élèves et de l'amélioration de formations.

7. Classcraft [Электронный ресурс] // URL: <https://www.classcraft.com/> (дата обращения: 18.03.2020).

8. Communiqué du Fonds de recherche du Québec, le 30 mars 2018. Le Québec jette les bases d'un observatoire mondial sur les impacts sociétaux de l'intelligence artificielle et du numérique.

9. Coursera [Электронный ресурс] // URL: <http://coursera.org> (дата обращения: 18.03.2020).

10. Duolingo [Электронный ресурс] // URL: <https://www.duolingo.co/> (дата обращения: 18.03.2020).

11. École branchée (2019). Façonner l'avenir de l'école avec l'intelligence artificielle. Rendez-vous pédagogique avec François Guité. En ligne [Электронный ресурс] // URL: <https://www.youtube.com/watch?v=5FGWjl-buiI0> (дата обращения: 18.03.2020).

12. Introducing Pearson+ [Электронный ресурс] // URL: <https://www.pearson.com/> (дата обращения: 18.03.2020).

13. *Karsenti, T.* (2018). Intelligence artificielle en éducation: L'urgence de préparer les futurs enseignants aujourd'hui pour l'école de demain? *Formation et profession*, 26(3), 112-119. DOI: <http://dx.doi.org/10.18162/fp.2018.a159>.

14. *Karsenti, T., Bugmann, J. et Gros, P-P.* (2017). Using Humanoïd Robots to Support Students with Autism Spectrum Disorder [Chronique]. *Formation et profession*, 25(3), 123-126. DOI: <http://dx.doi.org/10.18162/fp.2017.a135>.

15. *Karsenti, T., Bugmann, J. et Parent, S.* (2018). Apprendre l'histoire avec le jeu Assassin's Creed? Une étude exploratoire menée auprès de 329 élèves du secondaire. Montréal, QC: CRIFPE.

16. *L.-Desjardins, A., Tran, A.* L'intelligence artificielle en éducation [Электронный ресурс] // URL: <https://ecolebranchee.com/dossier-intelligence-artificielle-education/> (дата обращения: 18.03.2020).

17. *Lamb, C.* (2016). *The Talented Mr. Robot: The impact of automation on Canada's workforce.* Toronto, Ontario: The Brookfield-Institute-for-Innovation-Entrepreneurship.

18. *McGraw Hill* / eBook & ReadAnywhere App [Электронный ресурс] // URL: <https://www.mheducation.com/highered/learning-solutions/digital-solutions/mhebook.html> (дата обращения: 18.03.2020).

19. Mon coach Bescherelle [Электронный ресурс] // URL: <https://itunes.apple.com/fr/app/mon-coach-bescherelle/id1300598870?mt=8> (дата обращения: 18.03.2020).

20. *Stone P & al.* (2016). Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel. Stanford University. [Электронный ресурс] // URL: <http://ai100.stanford.edu/2016-report> (дата обращения: 18.03.2020).

21. TeachThought (2018). 10 Roles For Artificial Intelligence In Education. En ligne [Электронный ресурс] // URL: <https://www.teachthought.com/the-future-of-learning/10-roles-for-artificial-intelligence-in-education/> (дата обращения: 18.03.2020).

22. Turnitin [Электронный ресурс] // URL: <https://www.turnitin.com/> (дата обращения: 18.03.2020).

23. Usage des technologies de l'information pour la formation des enseignants au Niger [Электронный ресурс] // URL: <https://www.utifen.org/wp/le-projet> (дата обращения: 18.03.2020).

24. *Wang H., Chang C., Li T.* (2008). Assessing creative problem-solving with automated text grading. *Computer and Education*, 51(4), 1450-1466. DOI: <https://doi.org/10.1016/j.compedu.2008.01.006>.

*А. Д. Шматко,
доктор экономических наук, профессор,
профессор Российской академии образования,
директор ИПРЭ РАН*

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ НЕКОНТАКТНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ОБРАЗОВАНИИ

Развитие сквозных цифровых технологий становится ключевым фактором роста национальных экономик, позволяющим обеспечить глобальную конкурентоспособность компаний и стран. Цифровые преобразования затрагивают все сферы развития общества, в том числе образование. Высшие учебные заведения вырабатывают мощные стимулы для консолидации усилий в области цифровизации и внедрения технологий неkontaktного информационного взаимодействия. ВУЗы являются площадками для внедрения цифровых экосистем.

Опираясь на труды И. В. Роберт [1–4], можно говорить о смене парадигм в образовании и переходе от традиционного образования к парадигме современного периода информатизации образования как совокупности научно-педагогических положений и технологических решений, ориентированных на реализацию в образовании достижений современного «цифрового» общества массовой сетевой коммуникации и глобализации в условиях предотвращения возможных негативных последствий. Объектом дидактики в условиях информатизации образования стал процесс обучения, реализованный в информационно-образовательном пространстве путем применения технологий неkontaktного информационного взаимо-

действия субъективных возможностей обучающегося и результатов педагогического воздействия, направленного на раскрытие, развитие и реализацию интеллектуального потенциала обучающегося, трансформирующееся в его компетентность и общую культуру члена современного общества массовой сетевой коммуникации и глобализации.

Одним из компонентов неkontaktного информационного взаимодействия в образовании является система управления обучением (LMS), элементом которой выступает управление дистанционным обучением. Следует отметить, что системы управления дистанционным обучением применимы как для обучения в дистанционном формате, так и для поддержки очного обучения, а также для обеспечения программ дополнительного профессионального образования. Функционирование системы дистанционного обучения в вузе повышает его конкурентоспособность на рынке, поэтому был проанализирован системы управления обучением и системы дистанционного обучения (СДО) с целью выявления тех из них, которые обладают необходимым функционалом для образовательных организаций высшего образования.

Анализ LMS и СДО, проведенный в [5], показал, что на рынке представлено немалое количество цифровых продуктов разного качества и разного функционала для управления обучением как для корпораций, так и для предприятий и организаций малого и среднего бизнеса, а также для некоммерческих организаций, к которым относятся ВУЗы. На сегодняшний день при работе в такой системе доступен целый спектр функций, к которым прежде всего следует отнести:

- взаимодействие всех цифровых платформ и информационных систем вуза с внешними информационными системами, обеспечивающее связанности на интеграционном уровне

бизнес-процессов, сервисов и структур данных;

- централизованный ввод и распространение всем заинтересованным пользователям единых справочников, классификаторов и реестров;
- идентификация, авторизация и аутентификация пользователей системы с применением единой службы хранения учетных данных;
- доступ к финансовым, инфраструктурным и интеллектуальным ресурсам вуза;
- доступ к фонду опубликованной научно-технической литературы;
- доступ к электронным фондам, каталогам и репозиторию фундаментальной библиотеки вуза;
- доступ к хранилищу научной, технической информации, а также к результатам исследовательской деятельности вуза.

Изменение парадигмы информационного взаимодействия между субъектами образовательного процесса расширяет методические возможности учебного процесса за счет появления принципиально новых средств обучения, функционирующих на базе информационно-коммуникационных технологий.

Опираясь на исследования, опубликованные в [5], представим краткий обзор достоинств и недостатков использования технологий неконтактного информационного взаимодействия в образовании.

Спецификой психофизического развития молодого человека в студенчестве является достижение наилучших результатов в процессах биологического, психологического и социального развития в этот период. Наблюдаются наивысшее развитие физических и интеллектуальных сил, активизация социальной активности, наивысшая скорость оперативной памяти и переключения внимания, высокая способность к решению вербально-логических задач. Таким

образом, студенческий возраст является периодом динамического развития основных социальных компетенций человека. В этом возрасте происходит овладение полным комплексом социальных ролей взрослого человека: гражданских, профессионально-трудовых и межличностных.

При благоприятных условиях за время обучения в вузе у студентов происходит развитие всех познавательных способностей, в частности восприятия, памяти, мышления, внимания, уровня владения определенным кругом логических операций, формируется профессионально направленный склад мышления. Не только включенность в деятельность, но и содержание, и характер этой деятельности определяют качественные особенности познавательных способностей студентов. Исходя из этого, цифровизация образования и повсеместное применение цифровых образовательных технологий оказывает существенное влияние на специфику способностей современной учащейся молодежи. В некоторых работах отмечается, что применение информационных технологий в процессе обучения способствует развитию интеллекта и креативности. Использование цифровых информационных технологий позволяет значительно увеличить объем учебного материала, его тематику и подачу, облегчает поиск, интерпретацию, выбор нужного содержательного аспекта. За счет использования информационных технологий у обучающихся сохраняется на более длительный срок высокая познавательная активность, интерес к получению и закреплению знаний [6].

Вместе с тем, нельзя не отметить и негативные свойства цифровых информационных технологий, таких как реальный риск деформации мышления, речи и всех познавательных способностей у обучающихся. Вследствие чрезмерного потребления информации у обучающихся нарушаются все когнитивные процессы, а именно такие свойства внимания как концентрация, объем, рас-

пределение. Человек проявляет рассеянность, низкий уровень самоконтроля, трудности в управлении своим вниманием и др. Наблюдается существенное ухудшение памяти, уменьшается ее объем, способность к сохранению и воспроизведению материала. Также технологии неконтактного информационного взаимодействия способствуют развитию технократического мышления, которое характеризуется доминированием средства над целью и техники над человеком [7].

И. В. Роберт в [1] указывает на отрицательные последствия технологий неконтактного информационного взаимодействия: деструктивное поведение индивида в социуме; доминирование поведения сообщества над поведением индивида; искажение представлений индивида о традиционных ценностях; превалирование визуализации над содержательной основой изучаемого (рассматриваемого) объекта, процесса, сюжета («визуализационный примитивизм»), что может привести к превалированию «клипового» восприятия и искажению представлений индивида о реальной действительности с последующим «вылущиванием» индивида из реального социума; размывание «Я-личности» индивида при различных вариантах его самопредставления в информационных сетях (в виде графического знака, картинки, курсора), приводящего к деструкции личности, к потере ее цельности; приоритет для индивида мнений, полученных из «виртуальных источников». Длительное присутствие в профессиональном виртуальном мире может привести к: делегированию своих профессиональных функций техническим системам, что неизбежно приведет к ослаблению профессиональных навыков и к деградации профессионализма; смещению доверия в области решения профессиональных задач технико-технологическим реализациям, а не собственному профессионализму.

Таким образом, не смотря на очевидные преимущества, использование технологий неконтактного информационного взаимодействия в образовании может иметь целый ряд негативных последствий – от развития «визуализационного примитивизма» до «вылущивания» индивида из социума, что особенно опасно в студенческие годы, когда наибольшее влияние на молодого человека, на развитие личностной и интеллектуальной, социальной и профессиональной сферы оказывает именно система образования.

Литература

1. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надежность и качество». – 2018. – Т. 1. – С. 68–71.
2. Роберт И.В., Мухаметзянов И.Ш., Касторнова В.А. Информационно-образовательное пространство: Монография. – М.: ФГБНУ «ИУО РАО», 2017. – 92 с.
3. Роберт И.В. Научно-педагогические практики как результат конвергенции педагогической науки и информационных и коммуникационных технологий // Педагогическая информатика – 2015 – № 3, с. 27–41.
4. Роберт И.В. Направления развития информатизации отечественного образования периода цифровых информационных технологий//Электронные библиотеки. – 2020. – Т. 23. – № 1–2. – С. 145–164.
5. Исследование проблем и тенденций развития высшего образования в современной России: сборник научных трудов / авт.-сост. Г. А. Бордовский, А. Д. Шматко. – СПб.: ИПЦ СЗИУ РАНХиГС, 2021. – 308 с.
6. Маслова Ю.В. Позитивные и негативные аспекты использования компьютерных технологий у детей и подростков // Образовательные технологии и общество – Т.4 – №16. – 2013. Режим доступа: <https://readera.org/pozitivnye-i-negativnye-aspekty-ispolzovaniya-kompjuternyh-tehnologij-u-detej-i-14062522> (дата обращения: 01.12.2021).
7. Воложанина С.С., Лоханева К.В. Влияние информационных технологий на развитие познавательной активности детей [Электронный ресурс]. Сайт педагога-исследователя – Режим доступа: http://sisv.com/publ/vlijanie_informacionnykh_tekhnologij/6-1-0-641 (дата обращения: 11.12.2021).

*Л. И. Миронова,
доктор педагогических наук, доцент,
кандидат технических наук, профессор,
кафедра промышленного, гражданского строительства
и экспертизы недвижимости
ФГАОУ ВО «Уральский федеральный университет имени
первого Президента России Б. Н. Ельцина»*

РЕАЛИЗАЦИЯ МЕЖДИСЦИПЛИНАРНОГО ПОДХОДА В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ

Согласно результатам исследований, проводимых в Институте стратегии развития образования РАО в рамках научной школы И. В. Роберт, под *цифровой трансформацией образования* понимается *результат существенных системных изменений, произошедших и происходящих в сфере образования (как позитивных, так и негативных), в связи с активным и систематическим использованием цифровых технологий и реализацией в образовательной практике результатов достижений научно-технического прогресса современного информационного общества массовой глобальной коммуникации* [7].

В контексте развития и функционирования цифровой образовательной среды современного вуза наиболее активно подвергаются цифровой трансформации процесс создания цифровых образовательных ресурсов, информационно-методическое обеспечение учебного процесса, информационное взаимодействие, как между субъектами образовательного процесса, так и с интерактивными цифровыми ресурсами.

В то же время научно-методические основания в области разработки и использования цифровых образовательных ресурсов, ориентированных на информационно-методическое обеспечение учебного процесса в вузах в условиях цифровой трансформации высшего образования, недостаточно исследованы, в том числе на базе междисциплинарного проектирования. Такие исследования требуют в первую очередь анализа понятия «междисциплинарность», обоснования и формулировки цели междисциплинарного проектирования, а также решения организационно-технологических вопросов в области разработки цифровых образовательных ресурсов. Рассмотрим особенности междисциплинарного подхода при разработке информационно-методического обеспечения образовательного процесса (ИМО ОП) вуза в условиях цифровой трансформации высшего образования.

Библиографический обзор

Так как ИМО ОП разрабатывается, как правило, для двух или нескольких предметных областей, то целесообразно использовать проектный подход, который рассматривался в исследованиях Ю. В. Громыко [1], У. Х. Килпатрика [3], Дж. Дьюи [2], Е. С. Полат [6] и др. в контексте междисциплинарности (Franks D. et al. [18], Margalef Garcia L. и др. [24], Rabb R. и др. [32]), что инициирует «развитие тесного взаимодействия между представителями разных дисциплин (в том числе естественнонаучных: физики, химии, биологии и др.) и ИТ-специалистами» [26].

Исследователи, студенты и преподаватели, включенные в проблему установления связи и интеграции двух или более академических дисциплин, профессий или технологий с их методами и курсами преследуют общую цель. Проблемы, которые кажутся для исследователей, принадлежащих одной дисциплине, сложными

или широкомасштабными, как правило, решаются при использовании междисциплинарных подходов. В образовательной сфере прилагательное «междисциплинарный» используется, когда исследователи двух и более дисциплин объединяют свои подходы и трансформируют их так, чтобы они стали приемлемыми для решения определенных проблем.

Согласно исследованиям (Б. И. Бортника, Н. Ю. Стожко [13, 37], А. Гендьева, В. Йорданова [19], И. Гребенюка [22], С. К. Конга [23], Л. И. Мироновой [26, 27], М. Науменко [28], Д. Г. Сампсона [29], Х. С Чу [15] и др.) междисциплинарный проект включает специалистов разных дисциплин и профессий, которые вовлечены в процесс совместной работы как стороны, заинтересованные в решении общей задачи. Согласно Дж. Бергеру, междисциплинарная группа может состоять из лиц, имеющих подготовку в разных областях знания, с характерными для каждой понятиями и концепциями, методами, материалом и терминологией. Эти лица объединены для совместной работы над проблемой в условиях постоянной коммуникации между участниками, представляющими различные дисциплины [12].

Основываясь на исследованиях ряда ученых (Гарсиа Л. Маргарет и Роблин Н. Парейя [24], С. Никитина [29], Дж. Хейвуд [21] и др.), а также исходя из понимания того, что процесс образования в высшей школе опирается на базовые принципы системности и интегративности в условиях цифровой трансформации образования, был сделан вывод о том, что реализация междисциплинарного подхода предоставляет новые возможности в области организации и повышения эффективности, в частности, инженерного образования [4].

В ряде работ (О. К. Альшара и М. Ибрагима [10], Р. Рабб [32] и др.) описан опыт совместного обучения студентов разной про-

фессиональной направленности. Целесообразным для решения комплексных социальных, инженерных и других задач является формирование междисциплинарных команд студентов (Да Фигуэредо [16], С. Л. Карпентер [14], П. А. Е. Пиуно [30], С. П. Пулей [31], Р. Стеттер [36], К. Шеа [35] и др.). Результат такой активности студентов в междисциплинарной практической и исследовательской деятельности описан в работах А. Хайтера [20], Н.Б. Мак Голдрика [25], И. Рахала [33], Д. М. Рихтера [34], Дж. К. Тана [38], Д. Франкса [18] и др.).

Вопросы разработки междисциплинарных проектов в профессиональном образовании рассматриваются и во многих отечественных исследованиях (Б. И. Бортник и Н. Ю. Стожко [13], А. Гендьева [19], И. Гребенюк [22], С. К. Конг [23], Л. И. Миронова [27], М. Науменко [28], Н. Ю. Стожко [37] и др.).

При любом подходе к решению проблемы междисциплинарности актуальным является проектный подход, который по своей сути носит надпредметный характер и рассматривается методологами в рамках деятельностного и личностно ориентированного направлений обучения [5].

При этом используемые в различных предметных областях вычислительные методы требуют применения современных программных средств, что способствует развитию тесного сотрудничества между специалистами в различных дисциплинах (в т.ч. естественнонаучных: физики, химии, биологии) и специалистами в информационной сфере.

Одной из форм реализации междисциплинарного сотрудничества является междисциплинарное проектирование (Project Based Learning (PBL)). М. Барак и Я. Дж. Дори описали опыт интеграции PBL в ИТ-среде при реализации этой технологии на трех курсах бакалавриата химии [11]. Студенты экспериментальной

группы разрабатывали индивидуальные проекты на ИТ-основе, тогда как их сокурсники из контрольной группы – традиционные химические проекты. Сопоставление результатов обучения убедительно продемонстрировало высокую результативность примененной технологии.

С. Декхан и М. Я. Тсои [17] представили своеобразную модель междисциплинарного взаимодействия студентов на основе «бизнес-отношений»: студенты информационного направления обучения были «наняты» студентами-химиками для разработки программного обеспечения для проектирования мобильных приложений к курсу органической химии с целью более эффективного изучения курса.

Приведенный краткий обзор свидетельствует о востребованности, актуальности и значимости различных стратегий и технологий междисциплинарного проектирования.

Метод

В ходе исследования проведен теоретический анализ и обобщение положений педагогической науки по проблемам профессиональной подготовки студентов; изучен и проанализирован опыт преподавания различных вузовских дисциплин на базе средств ИКТ; проведен анализ ГОС и ФГОС ВО по ИТ-направлению подготовки будущих программистов, учебные программы и учебно-методические материалы для подготовки бакалавров и магистров в области программирования.

Результаты и обсуждение

Анализ научных публикаций по данной теме позволяет утверждать, что одним из путей решения проблемы цифровой трансформации высшего образования является разработка междисци-

плинарных проектов будущими ИТ-специалистами.

Предметно-профессиональная подготовка студентов – будущих ИТ-специалистов реализуется на базе блоков базовых и профилирующих дисциплин, содержательное наполнение которых изменяется чрезвычайно динамично благодаря быстрому развитию научных и технологических основ информатики как научной области. Информатика, являясь междисциплинарным научным направлением и выполняя интегративную функцию в системе наук, находит отражение в системе высшего образования. Резко возросшая роль цифровых технологий должна найти отклик в педагогических исследованиях по совершенствованию предметной подготовки специалистов для различных областей экономики, в том числе в сочетании с проектным обучением. При этом учебные проекты могут быть не только исследовательскими, но и отражать закономерности технологических процессов предметной области, т.е. иметь черты профессиональных проектов, что характерно для инженерных, строительных, архитектурных, экономических и других специальностей.

В современных вузах осуществляется подготовка студентов для различных отраслей экономики, что в условиях цифровой трансформации высшего образования требует разработки распределенного образовательного ресурса (учебно-методических материалов в электронных форматах представления, информационно-коммуникационных предметных сред, информационно-справочных систем, систем контроля знаний, реализации имитационных моделей в предметных областях, программно-аппаратных средств для организации учебного процесса, баз данных предметных областей и пр.). При этом квалификация преподавателей, которые осуществляют подготовку по этим специальностям, имеет другую направленность. Кроме того, программное обеспечение, которое

имеется в свободном доступе, не всегда удовлетворяет требованиям учебного процесса.

Согласно ФГОС ВО будущих ИТ-специалистов, объектами их профессиональной деятельности являются математические и алгоритмические модели, программы, программные системы и комплексы, а также методы их проектирования и реализации в междисциплинарных областях [4, 5].

Базовая профессиональная подготовка ИТ-специалистов традиционно представляет собой сочетание программистского (Computer Science) и инженерного (Computer Engineering) подходов в обучении. Такой симбиоз двух направлений подготовки позволяет формировать у студентов одновременно с навыками оценки, отбора, упорядочения и обработки информации творческий подход к созданию новых методов обработки информации и средств информатизации. При этом их базовая профессиональная подготовка формирует в них потенциал, который позволяет решать задачи, связанные с разработкой сервисов, обеспечивающих учебный и любые другие процессы вуза под руководством преподавателей и методистов кафедр, на которых обучаются будущие программисты.

Таким образом, базовая подготовка будущих ИТ-специалистов позволяет им интегрировать профессиональные компетенции в области разработки программного обеспечения, регламентируемые ФГОС ВО, в междисциплинарное проектирование цифровых образовательных ресурсов в процессе цифровой трансформации образования. Такой подход позволит будущим ИТ-специалистам решать задачи, связанные с разработкой цифровых образовательных ресурсов (ЦОР) для обеспечения образовательного процесса вуза, в состав которых входит:

- контент и учебно-методического обеспечение, представленные в электронном формате;

- автоматизированные средства контроля результатов обучения;
- средства формирования знаний и умений в конкретных предметных областях.

Тогда под междисциплинарным проектированием (МДП) цифровых образовательных ресурсов (ЦОР) будем понимать «деятельность будущих ИТ-специалистов, включающую следующую последовательность действий:

- разработку алгоритма, реализующего содержательную составляющую контента ЦОР;
- разработку алгоритма, реализующего технологическую составляющую интерфейса ЦОР;
- разработку кода прикладной программы ЦОР;
- отладку кода ЦОР;
- опытное использование ЦОР в учебном процессе;
- корректировку ЦОР по результатам опытного использования;
- использование ЦОР в учебном процессе вуза;
- разработку методической документации для пользователей ЦОР;
- разработку методической документации для проведения обучающего семинара для потенциальных пользователей разработанного ЦОР;
- оформление результатов междисциплинарного проектирования (презентация на научной студенческой конференции, публикация научной статьи, получение свидетельства о государственной регистрации программы для ЭВМ, подготовка доклада для выступления на научной конференции, участие в конкурсе, творческий отчет и т.п.)» [5].

Целью междисциплинарного проектирования в рамках учебно-методического процесса подготовки будущих ИТ-специалистов

одновременно с пропедевтикой подготовки выпускных квалификационных работ является формирование их профессиональных компетенций в области разработки современных цифровых образовательных ресурсов и сервисов в ходе цифровой трансформации образования для создания цифровой образовательной среды вуза, в ходе которого у будущих программистов развиваются проектно-рольничные умения и формируется опыт по оценке качества программных продуктов педагогического назначения.

Реализация данного подхода позволит более интенсивно создавать и расширять цифровую образовательную среду, обеспечивая ее участников актуальными образовательными ресурсами и сервисами.

Организационное и методическое руководство процессом разработки ЦОР в рамках МДП должно осуществляться преподавателями выпускающей кафедры, где проходят подготовку будущие ИТ-специалисты, и преподавателями и методистами кафедр вуза, для которых разрабатываются ЦОР в рамках межкафедрального научного коллектива (МКНК), куда входят студенты, пожелавшие принять участие в разработке ЦОР.

В ходе совместной работы в рамках МКНК у студентов-разработчиков ЦОР формируется компетентность в области разработки и использования ЦОР, под которой будем понимать следующую совокупность:

- *знаний в области:* теоретических основ разработки ЦОР на базе междисциплинарного проектирования; использования алгоритмических структур при обработке данных; основных теоретических положений в области проектирования для применения методик обучения; требований к педагогико-эргономическому качеству ЦОР (курирует преподаватель кафедры-исполнителя и ведущий преподаватель-предметник кафедры-заказчика);

- *умений в области:* применения современных технологий программирования; реализации этапов междисциплинарного проектирования при разработке ЦОР; разработки сценария ЦОР; разработки технологической составляющей контента и интерфейса ЦОР (курирует преподаватель кафедры-исполнителя); определения соответствия разработанных ЦОР педагогическим, технологическим и педагогико-эргономическим требованиям для организации учебного процесса (курирует ведущий преподаватель-предметник кафедры-заказчика или представитель подразделения-заказчика);
- *опыта в области:* определения педагогической цели использования ЦОР в процессе обучения; разработки сценария обучения (курирует ведущий преподаватель-предметник кафедры-заказчика или представитель подразделения-заказчика); проектирования контента (курирует преподаватель кафедры-исполнителя, ведущий преподаватель-предметник кафедры заказчика или представитель подразделения-заказчика); разработки прикладных программ для реализации содержательной и технологической составляющей контента и интерфейса ЦОР в соответствии с техническим заданием от подразделения-заказчика (курирует преподаватель кафедры-исполнителя или представитель подразделения-заказчика).

Выводы

Реализация междисциплинарного подхода является фактором успешной организации самостоятельной работы студентов в вузе, которая позволяет формировать познавательную активность будущих ИТ-специалистов и направлена на их профессиональное самосовершенствование. При этом результатом междисциплинарного проектирования, осуществляемого в рамках работы межкафедраль-

ных научных коллективов, будут актуальные цифровые образовательные ресурсы для обеспечения учебного процесса вуза, развитие его цифровой образовательной среды, которая должна обеспечивать взаимодействие с образовательными ресурсами все направления подготовки студентов, осуществляемой на кафедрах вуза. Эта взаимовыгодная деятельность ориентирована на повышение качества результатов обучения за счет интенсификации образовательного процесса, активизацию познавательной деятельности студентов, повышение их работоспособности и мотивации к обучению.

Задача освоения цифровых технологий для цифровой экономики России носит междисциплинарный характер, что требует четкого понимания образовательных задач в области цифровизации, связанных с необходимостью формировать компетентность специалистов в области разработки и реализации проектов цифровой трансформации в любой прикладной области, что напрямую зависит от уровня подготовки выпускников современных вузов. Междисциплинарное сотрудничество кафедр современных вузов может стать одним из направлений активизации процесса цифровой трансформации вузовского образования.

Литература

1. Громыко, Ю.В. Понятие и проект в теории развивающего образования / Ю.В. Громыко, В.В. Давыдова // Известия РАО / Ред. В.А. Сластёнин, В.Н. Харькин. – №2, 2000. – С. 36–43.
2. Дьюи Дж. Педагогический энциклопедический словарь / Под ред. Б.М. Бим-Бада. – М.: 2003. – 356 с.
3. Килпатрик У.Х. Метод проектов. Применение целевой установки в педагогическом процессе // Л. Брокгауз– Эфрон. – 1925. – 43 с.
4. Миронова Л.И. Информационное обеспечение вузовской подготовки в условиях междисциплинарного проектирования и менеджмента качества. Монография. – Екатеринбург: ООО «Издательство УМЦ УПИ», 2021. – 296 с.

5. Миронова Л.И. Методика оценки уровня сформированности компетентности студентов в области разработки электронных образовательных ресурсов // Образовательные технологии и общество, – 2016. – Т. 19. – № 3. – С. 544–560.

6. Новые педагогические и информационные технологии в системе образования // под ред. Е.С. Полат. – М.: Academia, 2000. – 268 с.

7. Роберт И.В. Аксиологический подход к прогнозу развития образования в условиях цифровой парадигмы // Инновационные процессы в профессиональном и высшем образовании: коллективная монография / Авторы составители: М.Н. Стриханов, Е.Н. Геворкян, Н.Д. Подуфалов. – М.: Изд-во «Экон-Информ», 2020. – С. 47–73.

8. Сайт <http://www.merriam-webster.com/info/copyright.htm>, вход свободный.

9. Сайт WordNet® 3.0, 2006 by Princeton University, вход свободный.

10. Alshara O.K., Ibrahim M. Business integration using the Interdisciplinary Project Based Learning model (IPBL). Symposium on Human Interface 2007 // Beijing, China, 2007. pp. 821–833.

11. Barak M., Dori Y.J. Enhancing undergraduate students' chemistry understanding through project-based learning in an IT environment // Science Education, 2005, vol. 89, no.1. pp. 117–139.

12. Berger G. Opinions and Facts. In.: Interdisciplinary // Problems of Teaching and Research in Universities // Paris: OECD, 1972. P. 23–26.

13. Bortnik B.I., Stozhko N.Y. Designing Innovative Process for Teaching Natural Sciences in Economic Universities. Review of the Ural State University of Economics, 2013, vol. 49, no. 5, pp. 113–118. // URL:<http://izvestia.usue.ru/download/49/16.pdf> (дата обращения: 22.08.2021).

14. Carpenter S.L., Delugach H.S., Etzkorn L.H., Farrington P.A., Fortune J.L., Utley D.R., Virani S.S. A knowledge modeling approach to evaluating student essays in engineering courses. // Journal of Engineering Education, 2007. vol. 90, no.3. pp. 227–239.

15. Chu H.-C., Hwang G.-J., Tsai C.-C. A knowledge engineering approach to developing mind tools for context-aware ubiquitous learning // Computers and Education, 2010. vol. 54, no. 1, pp. 289–297.

16. Da C. Figueiredo, R.M., De Sales A.B., Ribeiro Jr., L.C.M., Laranjeira L.A.F., Rocha A. Teaching software quality in an interdisciplinary course of engineering // Porto, Portugal, 2010. pp. 144–149.

17. Dekhane S., Tsoi M.Y. Work in progress – Inter-disciplinary collabora-

tion for a meaningful experience in a software development course. 40th Annual Frontiers in Education Conference: Celebrating Forty Years of Innovation, FIE 2010. // Arlington, VA, United States, 2010. pp. S1D1–S1D2.

18. *Franks D., Dale P., Hindmarsh R., Fellows C., Buckridge M., Cybinski P.* Interdisciplinary foundations: Reflecting on interdisciplinarity and three decades of teaching and research // *Studies in Higher Education*, 2007. vol. 32. no.2. pp. 167–185.

19. *Gendjova A., Yordanova B.* Project-Based Learning in Science at the American College of Sofia // *Chemistry*, 2009, vol.18, no. 4. pp. 255–267.

20. *Hayter A.* Probability and Statistics for Engineers and Scientists, 2012, URL: <http://omungameshack.files.wordpress.com/2012/08/probability-and-statistics-for-engineers-and-scientists-4th-edgnv64.pdf> (дата обращения: 25.10.2021).

21. *Heywood J.* Engineering Education: Research and Development in Curriculum and Instruction, 2005. URL: <http://onlinelibrary.wiley.com/advanced/search/results?articleDoi=10.1002/0471744697.ch8&scope=allContent&start=1&resultsPerPage=20> (дата обращения: 22.05.2022).

22. *Hrebenyk I., Primova O., Berest B.* Using of computer simulations of laboratory work for practical classes on biological chemistry URL:http://journal.iitta.gov.ua/index.php/itlt/issue/view/66/showТoc#.U5YVitJ_s9c (дата обращения: 15.09.2021).

23. *Kong S.C., Chan T.-W., Griffin P., Hoppe U., Huang R., Kinshuk, Looi C.K., Milrad M., Norris C., Nussbaum M., Sharples M., So W. M.W., Soloway E., & Yu S.* E-learning in School Education in the Coming 10 Years for developing 21st Century Skills: Critical Research Issues and Policy Implications // *Educational Technology & Society*. 2014, 17 (1). pp. 70–78.

24. *Margalef García L., Pareja Roblin N.* Innovation, research and professional development in higher education: Learning from our own experience // *Teaching and Teacher Education*. 2008, vol. 24, no.1. pp. 104–116.

25. *Mc Goldrick, N.B., Marzec, B., Scully, P.N., Draper, S.M.* Implementing a multidisciplinary program for developing learning, communication, and team-working skills in second-year undergraduate chemistry students // *Journal of Chemical Education*. 2013, vol. 90, no.3. pp. 338–344.

26. *Миронова Л.И., Стожко Н.Ю., Бортник Б.И., Чернышева А.В., Подшивалова Е.А.* Interdisciplinary project based learning: technology for improving student cognition // *Research in Learning Technology*, Австралия, ноябрь, 2015. P.1-13. URL:<http://dx.doi.org/10.3402/rlt.v23.27577> (дата обращения: 18.11.21).

27. *Миронова Л.И., Стожко Н.Ю., Чернышева А.В.* Computer Assisted Learning System for Studying Analytical Chemistry // *Chemistry: Bulgarian Jour-*

nal of Science Education. 2014. P. 606–613.

28. *Naumenko M.* Internet resources and improving the quality of school chemical education // *Information Technologies and Learning Tools*. 2013. Vol. 34. № 2. pp. 56–63.

29. URL:http://journal.iitta.gov.ua/index.php/itlt/issue/view/59/showТoc#.U5YZLdJ_s9c (дата обращения: 17.09.2021).

30. *Nikitina S.* Three strategies for interdisciplinary teaching: Contextualizing, conceptualizing, and problem-centring // *Journal of Curriculum Studies*. 2006, vol. 38, no.3. pp. 251–271.

31. *Piunno P.A.E., Boyd C., Barzda V., Gradinaru C.C., Krull U.J., Stefanovic S., Stewart B.* The advanced interdisciplinary research laboratory: A student team approach to the fourth-year research thesis project experience. // *Journal of Chemical Education*. 2014, vol. 91, no.5. pp. 55–661.

32. *Pooley S.P., Mendelsohn J.A., Milner-Gulland E.J.* Hunting down the chimera of multiple disciplinarity in conservation science. *Conservation Biology*, 2014. vol. no.28. pp. 22–32.

33. *Rabb R., Rogers J., Chang D.* Course development in interdisciplinary controls and mechatronics // *Saratoga Springs, NY, United States*. 2008. pp. T3F11-T3F15.

34. *Rahal I.* Undergraduate research experiences in data mining. 39th ACM Technical Symposium on Computer Science Education, SIGCSE 2008. Portland, OR, United States. 2008. pp. 461–465.

35. *Richter D.M., Paretti M.C.* Identifying barriers to and outcomes of interdisciplinarity in the engineering classroom // *European Journal of Engineering Education*. 2009, vol. 34, no.1, pp. 29–45.

36. *Shea K., Engelhard M., Helms B., Merz M.* Teaching an integrated new product development seminar on cognitive products. 10th International Design Conference, DESIGN 2008 // *Dubrovnik, Croatia*. 2008. pp. 1401–1408.

37. *Stetter R., Paczynski A., Voos H., Bäuerle P.* Teaching "coupling competence" by means of interdisciplinary projects. 9th International Design Conference, DESIGN // *Dubrovnik, Croatia*, 2006. pp. 1267–1274.

38. *Stozhko N.Y., Tchernysheva A.V., Mironova L.I.* Computer assisted learning system for studying analytical chemistry // *Chemistry: Bulgarian Journal of Science Education*, 2014, vol. 23, no. 4, pp. 607–613.

39. *Tan J.K., Fleming W.J., Connor C.G., Wilson C.* Development of an interdisciplinary design curriculum: Preparing the students for final year major design projects // *Salzburg, Austria*, 2006. pp. 33–38.

А. В. Рупецкий,
кандидат технических наук,
доцент кафедры «Инженерная графика»

Р. Р. Анамова,
кандидат технических наук, доцент,
доцент кафедры «Инженерная графика»

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ИНСТРУМЕНТОВ ПРОЕКТИРОВАНИЯ И ПРОИЗВОДСТВА В ОБРАЗОВАТЕЛЬНОЙ И НАУЧНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТА ТЕХНИЧЕСКОГО ВУЗА: ПЕДАГОГИЧЕСКИЙ КОНТЕКСТ

Бурное развитие в сфере электроники, вычислительной техники и робототехники ведет к цифровизации экономики, промышленности и образования. Говоря о цифровизации образования, необходимо отметить два аспекта: внедрение цифровых технологий в уже существующие образовательные программы и разработка новых образовательных программ цифровой направленности, а именно программ, ориентированных на аддитивные технологии, робототехнику, специализированное программное обеспечение и автоматизацию процессов.

Лаборатория аддитивного производства [1], успешно функционирующая на базе кафедры «Инженерная графика» МАИ с 2005 года, позволяет реализовывать научные, образовательные проекты,

научно-исследовательские работы студентов. Коллектив лаборатории состоит из преподавателей кафедры, студентов и выпускников МАИ, с интересом вовлеченных в работы по трехмерному моделированию и 3D-печати. Среди оборудования лаборатории представлены настольные 3D-принтеры, установки для промышленного изготовления деталей и сборочных единиц методами селективного лазерного спекания и выборочного лазерного плавления, 3D-сканеры и координатно-измерительная машина. Перечень имеющегося оборудования и программного обеспечения позволяет реализовать полный цикл создания изделия аддитивного производства: от моделирования до изготовления, финишной обработки, контроля и испытаний.

В МАИ с 2019 года осуществляется подготовка магистров по профилю «Аддитивные технологии в металлургии» (выпускающая кафедра 904). Среди профессиональных компетенций, которые осваивают обучающиеся магистерской программы:

- способность самостоятельно создавать при помощи современных САПР полный электронный макет изделия, адаптированный для производства средствами аддитивных технологий;
- готовность создавать при помощи современных систем автоматизации производства управляющие программы для современного оборудования, используемого в аддитивном производстве;
- готовность разрабатывать решения по автоматизации подготовки этапов аддитивного производства с учетом особенностей использования цифровых технологий.

Для студентов вуза непрофильных направлений подготовки реализуются программы повышения квалификации на базе «Школы 3D-печати» МАИ (кафедра 904) [2], в числе которых:

- программы, посвященные изучению систем автоматизированного проектирования для подготовки 3D-модели для трехмерной печати;
- программы, посвященные изучению технологий 3D-печати, доступных каждому;
- программы, предназначенные для лиц, знакомых с 3D-печатью и планирующих работу на промышленных установках аддитивного производства.

Методические и организационные проблемы реализации образовательных программ цифровой направленности

Модернизация существующих и разработка новых образовательных программ цифровой направленности неизбежно влечет за собой решение ряда задач:

- определение дидактической составляющей, обладающей новизной и отвечающей современному уровню развития научно-технического прогресса;
- подбор профессорско-преподавательского состава, отвечающего требованиям, предъявляемым федеральными нормативными документами (образовательными стандартами) к кадровому обеспечению образовательных программ, и одновременно обладающего необходимыми профессиональными компетенциями в области цифрового производства;
- подбор учебно-методического обеспечения, отвечающего современному уровню развития цифровых технологий и доступного для вузов;
- материально-техническое обеспечение учебного процесса при реализации образовательных программ цифровой направленности.

Рассмотрим каждую из задач.

1. *Определение дидактической составляющей.* Структура и содержание образовательной программы цифровой направленности должны соответствовать требованиям актуальных нормативных документов (ФГОС, профессиональных стандартов). Однако сложность состоит в том, что стандарты для относительно новых отраслей промышленности, например, аддитивной, утверждены не в полном объеме. 22 декабря 2015 г. утвержден Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 15.02.09 «Аддитивные технологии», содержащий требования к подготовке специалиста среднего звена с последующим присвоением квалификации «Техник-технолог». 5 октября 2020 года в Российской Федерации утвержден профессиональный стандарт «Специалист по аддитивным технологиям» [3] для вида профессиональной деятельности «Производство изделий методами аддитивных технологий». Указанный профессиональный стандарт должен быть использован при разработке дополнительных профессиональных программ повышения квалификации и профессиональной переподготовки [4]. Образовательные стандарты высшего образования применительно к сфере аддитивных технологий в России отсутствуют, в связи с чем подготовка специалистов в данной области, как правило, привязана к конкретной сфере промышленности (например, «Аддитивные технологии в металлургии» – профиль направления подготовки 22.04.02 «Металлургия»), что затрудняет разработку образовательных программ.

Другая сложность состоит в том, что научно-технический прогресс во всех отраслях промышленности, а особенно в цифровых, идет быстрее, чем вузы успевают реагировать на эти изменения – к моменту окончания студентом образовательной организации

компетенции, которые были им получены, не всегда в полной мере соответствуют потребностям промышленности, запросам работодателей, и требуется дополнительное обучение, например, по программам повышения квалификации или профессиональной переподготовки. Избежать отставания позволят опережающий характер образовательных программ вузов и стажировки на предприятиях с уже внедренными и успешно функционирующими цифровыми технологиями. В первом случае необходимо пересмотреть порядок утверждения ФГОС и профессиональных стандартов, сократив время их утверждения, второй требует дополнительного финансирования и регулирования.

2. Подбор профессорско-преподавательского состава. Преподаватели, обеспечивающие учебный процесс, сталкиваются с необходимостью подготовки и ведения новых учебных дисциплин цифровой направленности, не всегда имея для этого достаточный профессиональный опыт. Одним из вариантов решения данной проблемы является профессиональная переподготовка действующих преподавателей предпочтительно непосредственно на производстве с изучением нового оборудования и цифровых технологий и последовательности работы с ними. Другим вариантом является привлечение в качестве преподавателей специалистов с производства, уже освоивших новые технологии. Но здесь возникает вопрос соответствия данной кандидатуры требованиям, предъявляемым к педагогическим работникам, наличие опыта педагогической деятельности или документа о квалификации по профилю педагогической деятельности, что затрудняет реализацию этого варианта.

3. Подбор учебно-методического обеспечения. Большинство новых технологий, в том числе и аддитивные, разработаны за

рубежом. В связи с этим большая часть литературы, посвященной цифровым технологиям, издана на английском языке, отсутствует в библиотеке вуза, что осложняет ее изучение российскими студентами. Учебники по аддитивным технологиям малочисленны и, как следствие, дороги, не всегда отражают современный уровень развития технологий, зачастую основаны на более ранних зарубежных публикациях и их переводах.

4. Материально-техническое обеспечение учебного процесса. Одной из основных проблем при реализации образовательных программ цифровой направленности является недостаточное финансирование. Передовое оборудование и программное обеспечение, используемое для образовательной и научной деятельности цифровой направленности, в основном импортного производства и требует серьезных финансовых вложений для приобретения расходных материалов, ремонта, технического обслуживания. Как правило, изыскивать средства на решение этих проблем вынуждены кафедры, факультеты.

Опыт реализации образовательных программ в сфере аддитивных технологий позволил выявить такие проблемы российского образования, как недостаточное финансирование образовательных программ по новым направлениям и отсутствие продуманного механизма организации опережающей подготовки студентов вузов.

Очевидно, что применение цифровых инструментов проектирования и производства в образовательном процессе является необходимым условием подготовки компетентного специалиста, но их внедрение, а также разработка специализированных образовательных программ цифровой направленности требуют последовательных итерационных подходов по устранению ряда сложностей, часть из которых рассмотрена выше.

Литература

1. 3D-лаборатория. URL: <https://3d-laboratory.ru/> (дата обращения: 10.05.2023).

2. Петров В.П., Власова С.В. Первая в России школа 3D-печати «МАИ» // Аддитивные технологии в цифровом производстве. Металлы, сплавы, композиты. – 2019. – №1. URL: <https://cyberleninka.ru/article/n/pervaya-v-rossii-shkola-3d-pechati-mai> (дата обращения: 10.05.2023).

3. Профессиональный стандарт 40.159 «Специалист по аддитивным технологиям». URL: <https://classinform.ru/profstandarty/40.159-spetcialist-po-additivnym-tekhnologiiam.html> (дата обращения: 10.05.2023).

4. Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам. Приказ Минобрнауки Российской Федерации от 1 июля 2013 года N 499. URL: <https://docs.cntd.ru/document/499032387> (дата обращения: 10.05.2023).

М. В. Карелина,

доцент, кандидат технических наук,

Российский университет транспорта (МИИТ)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ НА ВЫСОКОТЕХНОЛОГИЧНОМ ТРЕНАЖЕРНОМ ОБОРУДОВАНИИ В ТРАНСПОРТНОМ ВУЗЕ

Изучение безопасности используемых информационных технологий, от которой в конечном итоге зависит безопасность обучающихся, особенно актуально в связи с применением в вузах тренажерного оборудования с элементами искусственного интеллекта и робототехнических систем. По мере дальнейшего увеличения масштабов внедрения современных информационных и коммуникационных технологий в образовательные процессы проблема информационной безопасности будет только возрастать [1]. В этих условиях чрезвычайно важно создание методических, научно-педагогических и организационных подходов для обеспечения информационной безопасности пользователя при работе на высокотехнологичном тренажерном оборудовании и недопущения возможных нежелательных последствий от «негативного» информационного контента.

Вопросам информационной безопасности личности посвящены работы исследователей (А. В. Брушлинского, Г. В. Грачева, А. А. Головинского, А. Н. Дегтярева, Т. С. Кабаченко, Т. И. Колесниковой, Т. М. Краснянской, И. Ш. Мухамедзянова, С. Ю. Решетиной, И. В. Роберт, А. М. Столяренко, Р. В. Сухова, Е. Е. Тимонина и др.), которые рассматривали проблему с различных позиций

педагогических принципов и технологий, однако анализ состояния проблемы информационной безопасности личности при использовании современным высокотехнологичным оборудованием позволяет сделать вывод о ее недостаточной разработанности.

Под *информационной безопасностью пользователей при работе на высокотехнологичном тренажерном оборудовании* понимается обеспечиваемое образовательным учреждением состояние защищенности пользователя и его психики от разрушительного воздействия информации при ее получении в процессе обучения.

Опасности и риски информационной безопасности пользователей, связанные с применением в образовательном процессе высокотехнологичного тренажерного оборудования, условно можно разделить на *психолого-педагогические, технико-технологические и медицинские*.

К *психолого-педагогическим опасностям и рискам информационной безопасности* можно отнести:

- несоответствие базового контента педагогико-эргономическим требованиям;
- психологический дискомфорт пользователя при использовании контента («проблема психологического дискомфорта»);
- ошибочное доверие подлинности информации, что может быть опасно в связи со снижением осознанного контроля.

К *технико-техническим опасностям и рискам информационной безопасности* относятся:

- технические неполадки, сбои в энергопотреблении;
- выход из строя и повреждение тренажерного оборудования;
- несанкционированное внедрение нежелательной информации или программного обеспечения;

- применение нелицензионного программного обеспечения.

Медицинские опасности и риски информационной безопасности:

- замедление реакции понимания пользователем при длительном влиянии «сомнительного» контента ;
- состояние стресса, тревожности, подавленности, нервно-психического напряжения при продолжительном воздействии информации [7].

Под процессом нивелирования возможных негативных последствий информационной безопасности пользователей, связанных с применением в образовательном процессе высокотехнологичного тренажерного оборудования, понимается формирование модели поведения пользователя и обучение его правилам действия в ситуациях, способствующих минимизации последствий от возможных информационных опасностей и рисков.

Нивелировать возможные негативные последствия *психолого-педагогического характера информационной безопасности пользователя* при применении высокотехнологичного тренажерного оборудования возможно путем выявления условий психолого-педагогической защиты от опасных воздействий, отказа от использования некачественной педагогической продукции, не отвечающей педагогико-эргономическим требованиям, и корректировки базового контента [2].

В качестве возможных методов предотвращения и уменьшения возможных негативных последствий, связанных с *технико-техническим характером информационной безопасности пользователя* при применении высокотехнологичного тренажерного оборудования является обеспечение технической надежности и безопасности работы тренажера и соблюдение правил охраны

труда: перед началом работы убедиться в отсутствии технических неполадок и сбоев в энергопотреблении; обеспечить отслеживание инструктором действий обучающегося для предотвращения травмоопасных действий; убедиться, что необходимый тип тренажера подобран с учетом использования возможностей технологической и технической реализации тренажеров.

Нивелирование возможных негативных последствий *медицинского характера информационной безопасности пользователя* при применении высокотехнологичного тренажерного оборудования возможно: при информировании обучающихся о рисках возникновения стресса, тревожности, подавленности и состояния нервно-психического напряжения, вызванного «сомнительным» контентом [8]; при выработке умения определить факторы, сигнализирующие о проявлении информационной опасности; создании благоприятной обстановки и эмоционального фона для плодотворного взаимодействия пользователя, тренажерного оборудования и преподавателя (инструктора). Несмотря на агрессивный и негативный характер последствий информационной безопасности пользователя «искусственно созданные психологические и информационные опасности и перегрузки на высокотехнологичном тренажерном оборудовании приводят к тому, что обучающийся обладает возможностью за достаточно короткий промежуток времени не только сформировать профессиональные знания, навыки и умения, но и выработать в себе психофизиологическую стрессоустойчивость» [5].

Наступление события с возможными негативными последствиями информационной безопасности пользователя при работе на высокотехнологичном тренажерном оборудовании в образовательной организации высшего образования маловероятно, однако, это не умаляет значения педагогического, методического и

дидактического изучения обозначенной проблемы. Очевидно, что информационная подготовка обучающихся должна осуществляться комплексно и обеспечивать все аспекты информационной безопасности пользователя. Также необходимо разработать систему мероприятий по нивелированию возможных негативных последствий, включающих контроль, позволяющий выявить воздействия психолого-педагогического, технико-технологического и медицинского характера.

Литература

1. Бочаров М.И., Симонова И.В., Можаров М.С. Влияние систематического обучения информационной безопасности на уровень тревожности обучаемых // Перспективы науки и образования. – 2019. – №4(40). – С. 169–182.
2. Вачков И.В. Основы технологии группового тренинга / И.В. Вачков. – М.: Ось-8, 1999. – 138 с.
3. Карелина М.В. Психологические аспекты применения современных тренажеров как средства профессиональной подготовки студентов транспортного вуза / Человеческий капитал. – Рязанский государственный университет им. С.А. Есенина, ООО «Объединенная редакция». – Том 2. – № 5 (161). – 2022. – С. 158–163.
4. Ломота А.В. Основы проектирования техники: учеб. пособие / А.В. Лопота, Е.И. Юревич. – СПб.: Изд-во Политехн. ун-та, 2017. – 154 с.
5. Лытаев, С.А. Психофизиология: учеб. пособие / С.А. Лытаев, М.В. Александров, М.С. Березанцева. – 3-е изд., перераб. и доп. – СПб.: СпецЛит, 2018. – 255 с.
6. Мухамедзянов И.Ш. Медицинские аспекты информатизации образования. 2-е изд. испр. и доп. – М.: ФГБНУ «ИУО РАО», 2017. – 168 с.
7. Роберт И.В. Дидактика эпохи цифровых информационных технологий // Профессиональное образование. Столица. – 2019. – №3. – С. 16–26.
8. i-Disorders – новые виды психических расстройств, связанные с использованием современных информационных технологий / И.А. Федотов [и др.] // Омск. психiatr. журн. – 2015. – № 4. – С. 16–19.
9. Dennison, M.S. Use of physiological signals to predict cybersickness / M.S. Dennison, A. Z. Wisti, M. D’Zmura // Displays. – 2016. – Vol. 44. – P. 42–52.

А. Е. Поличка,
доктор педагогических наук,
кандидат физико-математических наук, доцент,
профессор кафедры «Математика и информационные технологии»
ФГБОУ ВО «Тихоокеанский государственный университет»

Е. А. Гец,
старший преподаватель кафедры
«Физика, математика и информатика»
ФГБОУ ВО «Дальневосточный государственный
медицинский университет»

ОРГАНИЗАЦИЯ ПОДГОТОВКИ СТУДЕНТОВ МЕДИЦИНСКОГО ВУЗА К ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ

Эффективность медицинского образования предопределяется использованием современных средств информационных и коммуникационных технологий и потенциалом цифровой трансформации образования. Ряд проблем информатизации здравоохранения выделены еще в нормативных документах конца XX века («Концепция информатизации здравоохранения», утвержденная Минздравом РФ 29 июня 1992 г., «Программа информатизации здравоохранения России на 1993–1995 годы» (приказ Минздрава РФ от 30.12.93 № 308), на 1996–1998 годы (приказ Минздрава РФ от 23.04.96 № 158), «Программа «Основные направления развития информатизации охраны здоровья населения России на 1999–2002 гг.» (приказ Минздрава РФ от 14 июля 1999 г.). Одной из

самых существенных, как в области управления здравоохранением, так и внедрения медико-технологических процессов, является необходимость создания высокого интеллектуального уровня в среде медиков, начиная с руководителей и заканчивая средними медицинскими работниками.

Выделим противоречие между, с одной стороны, процессом цифровой трансформации и профессиональной деятельности, и медицинского образования с социальным заказом на подготовку профессиональных медицинских работников, обладающих современными знаниями, умениями и навыками в области использования современных средств цифровых технологий, с другой – необходимым интеллектуальным уровнем специалистов и системой образовательных программ в медицинских вузах.

Ввиду инновационности цифровой трансформации здравоохранения согласно законов инноватики для *организации подготовки студентов медицинского вуза к профессиональной деятельности с соблюдением требований информационной безопасности* в качестве особенности этой подготовки следует выделить *проектирование*, когда в условиях цифровой трансформации общества обучаемым необходимы адаптивность, способность переключать внимание, использовать навыки работы с обновляющимися цифровыми средствами не только при освоении образовательной программы, но и для взаимодействия с преподавателем, а в последующем – и для профессиональной деятельности [1].

В ФГБОУ ВО «Дальневосточный государственный медицинский университет» во ФГОС 2020 года специальности «31.05.01 Лечебное дело» по категории общепрофессиональной компетенции «Информационная грамотность» общепрофессиональной компетенции выпускника установлено «ОПК-10: Способен пони-

мать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности» выделена составляющая «основы информационной безопасности в профессиональной деятельности».

- ОПК-10.1: Знает: возможности справочно-информационных систем и профессиональных баз данных; методику поиска информации, информационно-коммуникационных технологий; современную медико-биологическую терминологию; основы информационной безопасности в профессиональной деятельности.
- ОПК-10.2: Умеет: применять современные информационно-коммуникационные технологии для решения задач профессиональной деятельности; осуществлять эффективный поиск информации, необходимой для решения задач профессиональной деятельности с использованием справочных систем и профессиональных баз данных; пользоваться современной медико-биологической терминологией; осваивать и применять современные информационно-коммуникационные технологии в профессиональной деятельности с учетом основных требований информационной безопасности.
- ОПК-10.3: Имеет практический опыт: использования современных информационных и библиографических ресурсов, применения специального программного обеспечения и автоматизированных информационных систем для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.

Наш подход, учитывающий инновационность формирования профессиональных компетенций, основан на выделении понятия информационно-адаптивной компетентности студентов и

необходимости описания системы ее формирования [2, 3], направленной на развитие менталитета обучаемых как в области информационной компетентности с особой ее составляющей – информационной безопасностью, так и в части адаптивных способностей к электронному обучению и средствам цифровизации. Отметим, что в условиях цифровой трансформации здравоохранения профессиональная компетенция, включающая составляющую по основам проектирования подготовки кадров в медицинских университетах, позволяет эффективно овладевать информационно-адаптивной компетентностью. Рассмотрим проектирование подготовки кадров в медицинских университетах для эффективного овладения информационно-адаптивной компетентностью на основе компетентностного и системно-деятельностного подходов.

Понятие «информационно-адаптивной компетентности студентов-медиков» [2] рассматривается как динамическое личностное качество, характеризующееся освоенностью совокупности адаптивных и информационных компетенций, включающих способность и готовность: применять средства современных информационных технологий для решения задач, возникающих в медицинской практике, а также устойчивое признание значимости этой компетентности для решения профессиональных задач.

Анализ источников показал, что, как правило, исследуются вопросы преподавания в медицинских вузах медицинской информатики и формирования профессиональных компетенций, связываемых с понятием информационной компетентности. Специальные исследования информационно-адаптивной компетентности студентов медиков не выделены, тем более с учетом требований информационной безопасности.

Авторами было проведено исследование организации подготов-

ки студентов медицинского вуза к профессиональной деятельности в условиях цифровой трансформации образования с учетом требований информационной безопасности, в частности внедрения телемедицинских технологий. В работе представлена логика рассмотрения проектной составляющей для выявления специального технологического инструментария педагогического работника медицинского вуза, представлено описание некоторых определяющих элементов специального технологического инструментария в научно-методическом обеспечении формирования необходимых компетенций, а именно, принципа оценки информационных фрагментов и пошагового метода решения ситуационных задач.

Исследование основано на нормативно-правовом подходе исторического развития процесса информатизации высшего медицинского образования как на федеральном, так и региональном уровнях, опирается на исследования ученых в области подготовки медицинских кадров в условиях информатизации здравоохранения и на подход научной школы «Информатизация образования» И. В. Роберт.

Следуя указанному подходу, в научном направлении информатизации образования в разделе «Подготовка кадров информатизации образования» как одно из направлений выделена подготовка медицинских работников интеллектуального уровня в области использования современных средств цифровых технологий.

Общероссийский классификатор специальностей по образованию нормативно устанавливает разделение по специальностям и направлениям подготовки на укрупнённые группы, в частности «Здравоохранение и медицинские науки». С учетом существующей нормативной базы высшее медицинское образование (см. напр., Закон РФ от 21.11.2011 № 323-ФЗ «Об основах охраны

здоровья граждан в РФ») может рассматриваться как группа программ профессионального обучения, направленных на подготовку врачей, фармацевтов, специалистов по охране здоровья.

В соответствии с положениями, изложенными в концепции комплексной, многоуровневой и многопрофильной подготовки кадров информатизации образования (И. В. Роберт, О. А. Козлов) [4], под *подготовкой студентов медицинского вуза к профессиональной деятельности в условиях цифровой трансформации образования* будем понимать научное направление и практико-ориентированную деятельность, которые ориентированы на разработку содержания и методики подготовки этих кадров в области реализации основных направлений информатизации образования здравоохранения и прикладных аспектов применения средств ИКТ в своей профессиональной деятельности в условиях информатизации здравоохранения.

В *организации подготовки студентов медицинского вуза к профессиональной деятельности в условиях цифровой трансформации образования выделим такую составляющую* как проектирование подготовки кадров в медицинских университетах для эффективного овладения информационно-адаптационной компетентностью в условиях цифровой трансформации здравоохранения и основания требований к этапам проектирования.

Одним их видов требований к этапам данного проектирования (концептуальному, моделированию, конструирования, технологическому) является принцип качественного научно-методического обеспечения формирования информационно-адаптационной компетентности, которое должны осуществлять соответствующие учреждения. Реализация этого принципа опирается на деятельность преподавателя по проектированию методических систем обучения информатическим дисциплинам с выделением темати-

ческого вида заданий, связанных с будущей профессиональной деятельностью.

В тематических полях выделены такие контентные поля, как:

- деятельность на основе инструментальных средств использования нормативных документов;
- схемы теории вероятностей и математической статистики;
- анализ и использование больших данных;
- использование открытых данных; работа в сетях;
- анализ и выбор оптимальных цифровых средств;
- основы информационной безопасности в профессиональной деятельности.

Основополагающим элементом для описания остальных элементов методических систем обучения учебных дисциплин выбран задачный материал, который основывается на пошаговых методах и ситуационных задачах.

В преподавании информатических дисциплин, следуя работам по использованию возможностей задачного материала и задачного подхода, разработаны методические материалы использующие указанные типы задачного материала, в том числе по основам информационной безопасности в профессиональной деятельности: настройки безопасности на уровне операционной системы; настройки безопасности приложений; настройки безопасности интернет-обозревателей; антивирусное программное обеспечение; профессиональные программные и аппаратные средства защиты информации; ситуационные задачи.

В заключение следует отметить следующие результаты исследования:

- определены составляющие информационно-адаптационной компетентности;

- выявлена взаимосвязь между ними и видами задач, применяемыми в обучении информатическим дисциплинам;
- задачный подход применен в Дальневосточном государственном медицинском университете на кафедре физики, математики и информатики при обучении информатическим дисциплинам;
- подготовлена серия учебно-методических пособий для студентов первого курса специальностей: 39.03.02 социальная работа; 31.02.05 стоматология ортопедическая; 31.02.06 стоматология профилактическая; 33.02.01 фармация.

Планируется продолжить исследования формирования информационно-адаптационной компетентности будущих специалистов медицинского направления подготовки для рассмотрения границ применимости и педагогической практики реализации методических подходов таких составляющих проектирования организации подготовки студентов медицинского вуза к профессиональной деятельности в условиях цифровой трансформации образования, как координации деятельности элементов информационно-образовательной среды медицинского университета и достижению взаимного соответствия функционирования ее частей. Кроме того, определяются понятия информационной подготовленности и ее необходимых параметров.

Литература

1. *Полечка А.Е.* Формирование адаптационных способностей обучаемых к электронному обучению в условиях цифровизации методических систем обучения // Информатизация образования и методика электронного обучения: цифровые технологии в образовании: материалы IV Междунар. науч. конф. Красноярск, 6–9 октября 2020 г.: в 2 ч. Ч. 1 / под общ.ред. М.В. Носкова. – Красноярск: Сиб. федер. ун-т, 2020. – С. 313–317.

2. Гец Е.А., Поличка А.Е. Понятие информационно-адаптационной компетентности для студентов медицинского вуза // Far East Math – 2021: материалы национальной научной конференции / Министерство науки и высшего образования Российской Федерации, Тихоокеанский государственный университет; [редакционная коллегия: Е. Г. Агапова (ответственный редактор) и др.]. – Хабаровск: Издательство ТОГУ, 2021. – С. 215–220.

3. Поличка А.Е., Гец Е.А. Формирование информационно-адаптационной компетентности студентов в информационной образовательной среде медицинского вуза // Международная научно-практическая конференция «Образовательное пространство в информационную эпоху» (2021 International conference «Education Environment for the Information Age» (EEIA–2021)): сборник научных трудов / под ред. С. В. Ивановой. – М.: ФГБНУ «Институт стратегии развития образования РАО». – 2021. – С. 355–361.

4. Роберт И.В., Козлов О.А. Концепция комплексной, многоуровневой и многопрофильной подготовки кадров информатизации образования. – М.: ИИО РАО, 2005. – 36 с.

С. С. Галстян,
кандидат филологических наук,
доцент кафедры геополитики и устойчивого развития

Е. Р. Кроввиди,
старший преподаватель кафедры геополитики и устойчивого
развития

*Российский государственный университет нефти и газа
(национальный исследовательский университет)
имени И. М. Губкина*

ФОРМИРОВАНИЕ ЯЗЫКОВОЙ И РЕЧЕВОЙ КОМПЕТЕНЦИИ В ВУЗЕ ПРИ ОБУЧЕНИИ ИНОСТРАННЫМ ЯЗЫКАМ

Открытое информационное пространство, расширение информационно-коммуникационных форм общения актуализирует проблему обеспечения свободного самовыражения обучаемых на иностранном языке, развития межкультурной коммуникативной компетенции. Развитию межкультурной коммуникативной компетенции во многом способствуют цифровые инструменты коммуникации, но с другой стороны – бесконтрольное погружение в «цифровой мир» может дать обучаемым неправильные ориентиры. Как следствие, как и в «доцифровую эпоху» межкультурная коммуникативная компетенция объединяет в себе два аспекта: воспитательный аспект социального общения, при этом одной из главных задач остается установление понимания своего как ценного и чужого как интересного, и коммуникативный аспект взаимопонимания через иностранный язык. Научно обоснованные

интенсивные методы обучения иностранному языку в высшей школе направлены не столько на преподавание грамматики, формирование словарного запаса, умения переводить и т.д., сколько сконцентрированы, главным образом, на овладении навыками профессионального общения – сложного многопланового процесса, в основе которого находится личностное взаимодействие, обмен информацией, опытом, знаниями, умениями, навыками. Профессиональное взаимодействие не исключает эмоциональности, чаще всего в скрытой форме, следовательно, требует большего, чем просто знание языка, а именно, обучения вербальному и невербальному общению, что требует от преподавателя следования классическим методикам обучения и воспитания. Сразу отметим, что несмотря на то, что достаточно большая часть профессионального общения происходит в опосредованном виде, формирование межкультурной коммуникативной компетенции происходит в диалоге – преподаватель – обучаемый, строящемся на когнитивном, эмоциональном и мотивационном общении.

Общение, в том числе в образовательном процессе, характеризуется содержанием, целями и средствами, рассмотрим эти составляющие. Немаловажное место в учебном процессе отводится подбору тем, которые способствуют развитию речемыслительных способностей у студентов, вводу, активации и интериоризации новых наборов лексических элементов, что способствует их выходу на новый, продвинутый уровень владения языком. Удачно подобранные тексты одновременно знакомят студентов с историей и культурой других стран, информируют об их политических и экономических устройствах и помогают воспитывать характер, целеустремленность, способствуют формированию личности с сильной волей, организационными способностями, умением работать в команде.

В начале вузовского курса изучения иностранного языка, как показывает практика, необходимо сформулировать его актуальные и реальные цели и задачи. Обучаемые с самого начала узнают, какой разновидностью иностранного языка и в какой степени они собираются овладеть, т.к. приобретение всех разнообразных навыков – чтение специальной литературы, газет, художественной литературы, написание научных работ, понимание текстов стихов, прозы – невозможно за ограниченный программой подготовки период времени. В этой связи следует акцентировать внимание на разных видах речевой деятельности различной степени сложности, с одной стороны (говорение, аудирование, письмо и чтение), с другой стороны – по уровням языка – лексика, грамматика, правильное произношение, понимание текстов. В процессе обучения активно применяется коммуникативно-прагматический подход, целью которого является повышение уровня профессиональной лингвориторической подготовки студентов, где особое внимание обращается на личности студента, его языковые способности и умения грамотно произнести речь.

Главенствующее место в образовательном процессе занимает системно-структурный подход, т.е. в процессе преподавания широко применяется структурно-семантическое описание грамматического строя, толкование семантических структур слов и анализ грамматических правил и категорий, однако с появлением в конце 20-го века нового коммуниктивно-прагматического подхода в изучении языка акцент от семантики, т.е. с содержания общения, смещается на условия и цели общения, где центральное место занимает личность как носитель и хранитель языка, сочинитель текстов.

Современная лингвистическая наука отмечает смену парадигмы, сдвиг от «чистой лингвистики», стремящейся к изучению

языка в самом себе и для себя, на уровень лингвориторики, где язык рассматривается как средство речевой деятельности. Как отмечает Ю. Караулов «коммуникативно-прагматическая волна расширяет возможности этого подхода за счет вторжения в сферу социального и социально-психологического. Недаром все чаще можно услышать призывы изучать «человеческий фактор» в языке, язык в связи с человеческой деятельностью, человека в языке и язык в человеке» [2, с. 19].

Разработанная Ю. Карауловым структура языковой личности как субстрата системы языка, состоящая из трех уровней – вербально-семантического, когнитивного, прагматического – активно используется в образовательном процессе как инструмент определения уровня языковой компетенции студентов. Под термином компетенция в данном контексте изучения языков подразумевается умения и способности учащихся воспроизвести качественный текст или качественную речь адекватно сложившейся ситуации. Иными словами, языковую компетенцию можно определить, как степень овладения разнообразием лингвистических элементов и оттенков родного или другого языка, которая обеспечивает достойный уровень общения человека в разных ситуациях коммуникации. «Возможности и формы взаимодействия индивида с лексической системой языка в значительной мере обусловлены образованием и профессией индивида. Профессиональный и образовательный уровень и их лексическая проекция – это своего рода социальный «костюм», который каждый человек выбирает по своему усмотрению и носит всю жизнь» [3, с. 221]. Этим «костюмом» является произнесенная речь человека.

Одним из традиционных способов развивать речевые способности является организация беседы, когда группа студентов собирается с преподавателем или носителем языка, если предостав-

ляется такая возможность. Такая форма общения часто вырождается в более или менее биографическую сессию вопросов и ответов, монополизированную меньшинством бегло говорящих. Причина этого, в первую очередь, в отсутствии определенной и интересной темы, а также недостаточной языковой подготовленности учащихся поддерживать продолжительные беседы.

Интересные темы для разговора, тематические дискуссии или дебаты развивают беглость речи, однако, по мнению авторов, большее значение является не столько тема беседы, сколько ее направленность (цель общения) – зачем об этом говорим, и характер – как говорим.

Дискуссия, у которой есть цели, часто бывает успешной, если обучаемые относятся к типу, который любит спорить и способен мыслить абстракциями. Но часто, по нашему опыту, участие постепенно стихает в связи с недостаточностью лексики. Во избежание такого развития событий необходимо предварительно ознакомить обучаемых с достаточным количеством лексических и грамматических материалов, попрактиковать их в предложениях собственного сочинения, научив применять их в процессе дискуссий. Например, сочетание *богатства и счастья* как одна из важных тем социально-экономического характера часто становится объектом дискуссий в обществе, представляя не меньший интерес для активного обсуждения в аудитории, развивая дискурс по определенной преподавателем траектории. Например, тщательный разбор всего лексического материала и осмысление статьи «Healthy, Wealthy and Unhappy»⁶ (Gerd Behrens, Time) перевели на обсуждение таких утверждений в тексте как «*When the carpenter of Galilee declared that man does not live by bread alone, he remembered all those who see man as Homo economicus of their*

⁶ Здоровый, богатый и несчастный.

material blinkers»⁷ or «A happy intellectual is an oxymoron»⁸.

Обучаемым необходима причина, чтобы говорить больше, чем им нужно что-то, о чем можно говорить; однако, если у них есть такая причина, тот факт, что тема является стимулирующей, делает всю дискуссию более интересной. И если целью дискуссии является возможность попрактиковаться в разнообразных языковых функциях, обучение профессиональному общению, следует значительно расширить наше представление о том, что делает предмет шире и интереснее.

Еще одним естественным и эффективным для обучаемых способом попрактиковаться в свободном общении является совместное обдумывание какой-либо проблемы или ситуации посредством словесного обмена идеями. На курсе иностранного языка еще одной целью такого обмена может быть развитие беглости речи. Сегодня принято говорить, что язык, являясь средством общения, никогда не используется сам по себе, а всегда ради достижения цели или выполнения функции: убеждать, информировать, спрашивать, советовать и т.д. Цель дискуссии – обозначить проблему, исследование последствий идеи, построение предложений или что-то еще, что должно восприниматься серьезно.

Еще одной целью может быть обучение на основе контента. В дискуссиях можно многое усвоить из сказанного и научиться конструктивно участвовать в коллективном обсуждении. Это включает в себя ясное, логическое мышление, с одной стороны, и навыки ведения дискуссий, с другой. Под ясным, логическим мышлением подразумеваются такие вещи, как способность производить речь,

⁷ Когда галилейский плотник заявил, что не хлебом единым жив человек, он имел в виду всех тех, кто видел в человеке Homo economicus со своей материальной зашоренностью.

⁸ Счастливый интеллигент – это оксюморон.

аргументировать, обобщая примеры, или наоборот, проводить аналогии, судить о приоритетах, делать выводы о причинах и т. д. Приемы дебатов включают в себя выслушивание того, что говорит другой человек, не перебивая его, говоря уместно и четко, стремясь понять точку зрения другой стороны, если ситуация конфликтная.

Таким образом можно заключить, что формы взаимодействия с лексической системой языка в значительной мере обусловлены уровнем образованности и профессиональной подготовленности личности. Полученные знания в вузе, навыки и умения правильно и грамотно построить речи являются хорошим фундаментом для ведения дискуссий на любом уровне с подкрепленными аргументами, служат залогом успеха в ведении сложных деловых переговоров и способствуют построению успешной профессиональной карьеры. Навыки речевой деятельности позволяют качественно взаимодействовать с другими людьми, делиться важными идеями и информацией, убеждать и оказывать влияние на других людей при принятии решений, корректно вести опосредованное общение в глобальной информационно-коммуникационной среде. Воспитание профессионала как гармонично развитой личности – это диалог человек-человек, преподаватель-обучаемый, вне зависимости от степени развития технологий.

Литература

1. Галстян С.С. Роль языковой личности в телевизионной речевой культуре: дис. ... канд. филол. наук. – М., 2008. – 151 с.
2. Караулов Ю.Н. Русский язык и языковая личность. – М.: УРСС, 2002. – 264 с.
3. Наумов В.В. Лингвистическая идентификация личности. – М.: URSS, 2022. – 240 с.
4. Пассов Е.И. Коммуникативный метод обучения иноязычному говорению. – М.: Просвещение, 1991. – 223 с.

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ШКОЛЕ

А. А. Николаева,

ЧУОО ВО «Омская гуманитарная академия»,

БОУ г. Омска «Лицей №54»

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ И СОХРАНЕНИЯ ЗДОРОВЬЯ УЧЕНИКОВ ПРИ ИСПОЛЬЗОВАНИИ ГОЛОСОВОГО SMART-ПОМОЩНИКА В ОСНОВНОЙ ШКОЛЕ

Разработка педагогических практик использования голосовых смарт-технологий в основной школе в условиях цифровой трансформации образования имеет большую практическую значимость. Голосовые интеллектуальные помощники (ГИП) предустановлены в телефоны и SMART-доски, интегрированы в поисковые программы, электронные сервисы, внедрены в социальные сети, электронную почту, их используют ученики и учителя в обыденной жизни, активно формируется практика применения голосовых интеллектуальных помощников в образовательном процессе. При этом ГИП, участвующие в процессах цифровизации информационного взаимодействия и информационной деятельности, обеспечения информационной безопасности личности, дополняют эти процессы своими возможностями.

Принципиально новые IT-технологии на базе искусственного

интеллекта (ИИ) имеют различный функционал и ресурсный потенциал в образовании и по-разному влияют на здоровье человека. Изучение этих влияний и разработка специальных педагогических практик для использования новых IT-технологий в основной школе является важной научно-практической задачей.

Рассмотрим пример использования в основной школе голосовых интеллектуальных помощников (ГИП) на уроках социально – гуманитарного цикла и внеурочной деятельности на примере русифицированного ГИП «Маруся», разработанного российской компанией Mail.ru Group на базе единой экосистемы, опираясь на подходы к использованию цифровых технологий в образовании цифровой трансформации образования А. Ю. Уварова [1], фундаментальные научные исследования научной школы И. В. Роберт [2, 3, 4, 5, 6, 7].

Информационно-коммуникационная экосистема «Маруся» основана на технологии искусственного интеллекта⁹, что позволяет настраивать систему в соответствии с решаемыми задачами. Важной новацией является навык распознавания и идентификации голоса, перевод в текстовый вид, понимание голосовых команд и синтез речи. Голосовые помощники на базе ИИ позволяют применять средства дополненной и виртуальной реальности; помогают организовать коммуникацию между субъектами образовательного процесса, могут управлять другими «smart»-устройствами, программируются на автоматизацию задач повседневной деятельности (создают напоминания, строят маршруты, выполняют переводы и т.д.). Есть функционал поиска и систематизации информации, что существенно при работе с большим объёмом данных.

⁹ Для целей данного исследования «искусственный интеллект» рассматривается в узком смысле прикладного использования в специализированных программных системах, реализующих естественный пользовательский интерфейс и ряд интеллектуальных функций [8].

Для определения проблем и возможностей использования ГИП «Маруся» в основной школе было проведено исследование, проанализирован и опробован функционал, заявленный авторами. Результаты проведенного анализа возможностей и ограничений использования голосового интеллектуального помощника (ГИП) «МАРУСЯ» на базе единой информационно-коммуникационной экосистемы Mail.ru Group в цифровой образовательной среде основной школы приведены в таблице 1.

Таблица 1

	Возможности	Ограничения
Цифровизация информационного взаимодействия	Единая русифицированная экосистема VK: интегрирована в почту Mail.ru, социальные сети ВКонтакте, в браузер Atom и ICQ. Кроссплатформенность: «смарт-колонка» от VK, SmartVoice, MiSmartSpeaker от Xiaomi, приложения iOS и Android на ПК и мобильных телефонах, интерактивных досках, умных часах. «Голосовое» управление цифровыми техническими средствами, функцией «умный класс», автоматизация процессов виртуальной передачи-приема информации в различном виде и объеме, приложения в распределенных и доступных сетях; коммуникации с обратной связью между пользователями, между пользователями и интерактивным информационным ресурсом [9].	Регистрация только для граждан РФ. Необходим аккаунт в VK, доступ к контактам для обеспечения безопасности информации настраивается вручную (и плюс, и минус). Не интегрируется с iPad, ресурсами компании Meta (концепция разработчика). Необходима почта на mail.ru. Требуется точка подключения к сети Интернет, к источнику питания (нет аккумулятора). Зарядка, подключение через повербанк 9В.

Продолжение табл. 1

	Возможности	Ограничения
	Передает голосовые сообщения, читает сообщения, голосовой ввод текста. Кастомизация системы, создание пользовательских «скилов». ¹⁰	
Цифровизация информационной деятельности	Совместим со всеми русифицированными ресурсами, утвержденными для основной школы Минпросвещения России. Автоматизация процессов информационной деятельности (поиск, отбор, обработка, использование, передача) голосовыми командами. Использование прикладных и инструментальных приложений в голосовом режиме учениками и учителями в урочной и внеурочной деятельности. Кастомизации системы, создание необходимых пользователю «скилов» с использованием программ, доступных учителю и ученику. Визуализация информации на экранных носителях.	Наличие платного и бесплатного образовательного контента. При поиске требуется навык четкой формулировки запроса, выделения ключевых слов. Нет доступа к контенту, защищенному авторским правом. В голосовом интерфейсе пользователь не может оценить полностью информации.
Цифровизация образовательных услуг	Наличие бесплатного образовательного контента.	Наличие платного контента.
	Введение «скилов» – команд «МАРУСЯ» через приложение на всех платформах.	
	Оцифровка голоса в текст. Озвучивание и визуализация информации.	Ошибки в ударении при синтезе речи.

¹⁰ «скил» – в данной работе понимается в узком смысле, как термин программирования – «голосовое мини приложение», «код команда», «код-вызов» разработанный на основании протокола взаимодействия с платформой [10].

Окончание табл. 1

	Возможности	Ограничения
Цифровизация образовательных услуг	Образовательный контент на базе инструментальных средств web-платформ от разработчиков; быстрый доступ к безопасному образовательному контенту в речевой и электронной форме, в т. ч. на уроке.	Ограничен набор готовых виджетов с образовательным контентом (идет разработка). Подключение к школьной сети, поиск информации на уроке через предустановленные фильтры.
	Участие учеников и учителей в сообществах на базе сети Интернет.	
	Создание цифрового образовательного ресурса командой в условиях удаленного доступа.	
	Идентификация личности, в т. ч. в условиях удаленного доступа.	
Цифровизация обеспечения процессов информационной безопасности личности обучающегося	Идентификация личности по голосу. Концепция разработчика: автоматизированный «Детский» режим при идентификации детского голоса; автоматизирована защита от неэтичной, противозаконной, агрессивной недостоверной информации. Защита личной информации настраивается пользователем. Режим защиты от «информационного насилия», фильтры-ограничители большого потока информации (опция: «хотите узнать больше?», «меню голосового выбора»), фильтры на рекламу.	Декларирует право на свободу информации, защита персональных данных, частной информации, определяющей статус и жизнедеятельность пользователя по настройкам при недостаточной форсированности соответствующих компетенций у учеников и учителей.

В качестве вывода можно отметить, что внедрение ГИП позволяет создавать условия персонализации образовательного процесса, защищать интеллектуальную собственность. Разработчиками учтены основные психолого-педагогические аспекты информационной безопасности личности (ИБЛ), блокируется контент электронно-образовательных ресурсов, не соответствующий педа-

гогико-эргономическим требованиям [5, 7].

Использование ГИП в школе требует формирования навыков цифровой грамотности как одной из базовых цифровых компетенций функционально грамотной личности, т.к. степень защиты экосистемы определяет пользователь, смарт-колонки имеют доступ к личной информации. Включение правил безопасности при разработке педагогических практик в основу учебного алгоритма, применяемого в рамках деятельностных технологий, позволяет системно формировать навыки цифровой безопасности личности [11]. Новая и уникальная технология еще не классифицирована в справочниках и в нормативно-правовых актах. «Методические рекомендации по использованию компьютерных технологий и электронного обучения в работе с обучающимися» определяют: «При работе с любыми цифровыми средствами на уроке предполагается соблюдение гигиенических регламентов их использования согласно Санитарному законодательству» [12]. Идентифицировать ГИП только как колонку представляется не вполне корректным. Применение нормативов по аналогии затруднено многофункциональностью и кроссплатформенностью ГИП – они могут устанавливаться на экранных и не экранных носителях и являются средством как и коллективного, так и индивидуального пользования. Звуковые характеристики зависят от носителя, на котором установлено приложение, следовательно, приходится исходить из того, что смарт-доска и ПК соответствуют требованиям санитарных норм.

Затрудняет применение ГИП в школе запрет использовать на учебных занятиях телефон [9], обосновывая требование негативным влиянием на зрение ребенка из-за размера экрана. Следует отметить, что больший вред здоровью обучаемых наносит разрешение пользоваться телефоном на переменах, когда доступ к информации не контролируется, а подвижные игры замещаются играми

компьютерными. По нашему мнению, законодателем не учтен потенциал применения телефона на уроке: использование голосовых ресурсов, арт-технологий, приемов оценивания с помощью скан-кодов и т.д. К числу положительных характеристик ГИП отнесем легкость и бесплатность установки на любом гаджете, голосовые команды и синтез речи, «чтение» текста найденной информации.

К одним из очевидных направлений использования ГИП относятся аудио методики, которые эффективно применяются при изучении иностранных языков, в инклюзивном образовании, обучении грамоте в дошкольном образовании. В практике начальной школы они используются значительно реже, иногда на уроках литературы и в единичных случаях на уроках общественно-гуманитарного цикла. Ранее ограниченность их использования объясняли недостаточной технической оснащённостью, сейчас гаджеты совместимы со смарт-колонкой, расширился образовательный аудиоконтент и его доступность, появились аудиоучебники по школьной программе.

С одной стороны, функции синтеза речи позволяют озвучить любой текст, аудиальное восприятие информации уменьшает риски снижения зрения у школьников, развивает аудиальную память, расширяет когнитивные возможности. Формулировка голосовых команд для поиска информации по ключевым словам развивает когнитивные навыки. С другой стороны, есть риск нарушения метакогнитивных навыков из-за разницы восприятия письменного и устного текста, изменения тактики использования информации школьниками, сокращения практики написания текстов, заменой этого процесса на наговаривание. Данные аспекты следует учитывать и изучать в ходе дальнейших исследований, результаты которых могут стать основанием для внесения некоторых поправок в нормативы, смягчающих общий запрет.

Некорректное использование смарт-технологий в образовании, направленность на поиск и трансляцию информации вместо формирования нового знания и умения его применять препятствуют становлению и закреплению компетенций функционально грамотной личности. Смарт-формат позволяет найти, использовать и не удерживать в голове информацию. Если отсутствует контроль и непосредственное педагогическое воздействие, стимулирующее и координирующее мыслительные процессы, то при дефиците у учеников мотивации не актуализируется потребление контента, оно пассивно «транслируется» и «стирается» из памяти. Это провоцирует развитие транзактивной памяти. Новые педагогические практики должны учитывать методологические противоречия между когнитивными возможностями смарт-образования и реальными когнитивными и метакогнитивными компетенциями обучающихся, условиями их формирования.

Трансформационные изменения при внедрении ГИП на данном этапе обеспечиваются использованием принципа переноса возможностей цифрового ресурса в образовательные технологии деятельности обучения, такие как Технология проблемно диалогического урока Е. Л. Мельниковой [14], Технология решения изобретательских задач Г. С. Альтшуллера [15], Технология формирования типа правильной читательской деятельности Е. В. Бунеевой, О. В. Чиндиловой [16] и др. Эти технологии позволяют формировать познавательную активность, самостоятельность, самоорганизацию, навыки коллективной работы. Формируется критическое мышление, способность к творчеству. Функциональные параметры «Маруси» расширяют возможности ученика и педагога. Разработчики смарт-колонки предлагают «скилы» команды для реализации на уроке арт-технологии, эффекты и инструменты для иммерсивных технологий и т.д.

Перенос возможностей смарт-колонки в организацию технологии продуктивного, понимающего чтения (слушания) на разных этапах, использование практики активного слушания и конспектирования при общении с учителем «лицом-к-лицу», перенос аудирования в изучение различных дисциплин позволяют развивать «активную» память учеников. Это дает возможность корректировать процесс образования и предотвращать возможные негативные последствия смарт-технологий. Разработка педагогических практик использования ГИП для основной школы требует серьезных научно-практических исследований, учитывающих риски негативного влияния и возможности их предотвращения.

Литература

1. Цифровая трансформация и сценарии развития общего образования / А.Ю. Уваров; Национальный исследовательский университет «Высшая школа экономики», Институт образования. – М.: НИУ ВШЭ, 2020. – 108 с. (Современная аналитика образования. – № 16(46)). – С. 17–18.
2. Официальный сайт научной школы Роберт И.В. «Информатизация образования» // режим доступа <http://robert-school.ru/iio/pages/struct/publications> [дата обращения 29.11.2022]
3. Роберт И.В. Дидактика периода информатизации образования / И. В. Роберт // Педагогическое образование в России. – 2014. – № 8. – С. 110–118.
4. Развитие информатизации образования в школе и педагогическом вузе в условиях обеспечения информационной безопасности личности / С.А. Бешенков, Я.А. Ваграменко, В.А. Касторнова, О.А. Козлов, Э.В. Миндзаева, И.Ш. Мухаметзянов, В.П. Поляков, И.В. Роберт, В.И. Сердюков, Т.Ш. Шихнабиева, Г.Ю. Яламов. – М.: ФГБНУ «ИУО РАО», 2018. – 105 с.
5. Мухаметзянов И.Ш. Методические рекомендации по предотвращению негативных медицинских последствий использования ИКТ в образовании. – М.: ИИО РАО, 2012. Мухаметзянов И.Ш. Социальные последствия информатизации образования // Казанский педагогический журнал. – 2011. – № 3. – С. 109–116.
6. Роберт, И.В. Развитие образования в условиях цифровой парадигмы

в контексте аксиологического подхода / И.В. Роберт // Мир психологии. – 2021. – № 1–2(105). – С. 89–103.

7. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надёжность и качество». – 2018. – Т. 1. – С. 68–71.

8. Касторнова В.А. К вопросу о внедрении технологий искусственного интеллекта в школьное образование // Педагогическая информатика. – 2022. – № 1. – С. 18–29.

9. Роберт, И.В. Цифровая трансформация образования: ценностные ориентиры, перспективы развития / И. В. Роберт // Россия: тенденции и перспективы развития: ежегодник: материалы XX Национальной научной конференции с международным участием, Москва, 14–15 декабря 2020 года. Том Выпуск 16. Часть 1. – Москва: Институт научной информации по общественным наукам РАН, 2021. – С. 868–876.

10. Документация. Термины и определения / Официальный ресурс ВК платформы. // <https://dev.vk.com/rules/> [дата обращения 06.02.2023]

11. Приказ Минпросвещения РФ от 02.08.2022 № 653 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования» (Зарегистрирован 29.08.2022 № 69822) // <http://publication.pravo.gov.ru/Document/View/0001202208290012?index=0&rangeSize=1> [дата обращения 21.11.22]

12. Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 «Об утверждении санитарных правил» СП 2.4. 3648-20 (Зарегистрирован 18.12.2020 № 61573) // <http://publication.pravo.gov.ru/>

13. Гигиенические нормативы и специальные требования к устройству, содержанию и режимам работы в условиях цифровой образовательной среды в сфере общего образования. Руководство. М.: НМИЦ здоровья детей Минздрава России, 2020. – 20 с.

14. Мельникова Е.Л. Проблемно-диалогическое обучение: понятие, технология, методика: Монография / Е.Л. Мельникова. – М.: Баласс, 2015. – 272 с.

15. Альтиуллер Г.С., Шапиро Р.Б. О психологии изобретательского творчества // Вопросы психологии. – 1956. – № 6. – С. 37–49.

16. Чиндилова, О.В. Технология продуктивного чтения на разных этапах непрерывного литературного образования в ОС «Школа 2100»: Монография. – М.: Баласс, 2010. – 208 с.

В. И. Сердюков,
*доктор технических наук, профессор,
главный научный сотрудник ФГБНУ «Институт управления
образованием Российской академии образования»,
профессор Московского государственного технического
университета имени Н.Э. Баумана*

Н. А. Сердюкова,
*доктор экономических наук,
профессор Российского государственного университета
имени Г.В. Плеханова и Российской таможенной академии*

СТАТИСТИЧЕСКИ-ДОКАЗАТЕЛЬНЫЙ ПОДХОД К СРАВНИТЕЛЬНОЙ ОЦЕНКЕ РЕЗУЛЬТАТОВ ПРОФЕССИОНАЛЬНОГО РОСТА УЧИТЕЛЕЙ

Примеры идеального учителя – человека ищущего, требовательного к себе, считающего, что его «коэффициент полезного действия мог бы быть гораздо выше» [1], хорошо показаны в отечественной классике, это Карл Иванович из автобиографической повести Л. Н. Толстого «Детство», Лидия Михайловна из рассказа В. Г. Распутина «Уроки французского», Илья Семенович Мельников из кинофильма: «Доживём до понедельника». Но как найти таких учителей...

Далеко не каждый может стать учителем, т.к. необходимо соответствовать критериям пригодности, изложенным в ст. ст. 46, 48 и 51 Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» [2], ст. ст. 69, 213 и 331 Трудового Кодекса Российской Федерации от 30.12.2001 №197-ФЗ [3], Приказе Минтруда России от 19.04.2021 №250н [4]. Кроме того, кандида-

тура учителя должна быть одобрена аттестационной комиссией общеобразовательной школы (далее – школы), однако такая «аттестация проходит формально» [5], в том числе из-за дефицита учителей¹¹, многие директора школ недовольны «качеством подготовки будущих учителей в педагогических вузах» [6], а каждый 5–6 учитель русского языка и математики плохо знает свой предмет [5].

За рубежом также, как и у нас, оценка учителей основывается на критериях пригодности, о чем, в частности, свидетельствуют данные табл. 1.

Таблица 1

Критерии оценки учителей, используемые в Австралии и США [7]

Критерии оценки	Разработчик критериев	
	Австралийский совет по обучению и преподаванию, 2008 г.	Американский совет по образованию, 2017 г.
Ожиданий	–	Знание учителем целей обучения, критериев оценки учащихся и их прогресса в обучении.
Соответствия (экспертизы)	Соответствие проводимых занятий и используемых образовательных ресурсов учебной программе и учебным планам.	Соответствие применяемых методических подходов к обучению, включая подходы к персонализированному и активному обучению, целям обучения.
Обратной связи	Использование обратной связи с обучаемым, способствующей его самостоятельному обучению.	Формирование текущих и итоговых оценок учащегося с учетом выполнения им заданий с обратной связью.

¹¹ Так, например, в 2019 году доля ставок учителей, фактически занятых списочным составом, в среднем по стране составила 93,2% от их общего числа, текучка учителей – 8,5% [8].

Критерии оценки	Разработчик критериев	
	Австралийский совет по обучению и преподаванию, 2008 г.	Американский совет по образованию, 2017 г.
Выравнивания	–	Формирования текущих и итоговых оценок учащегося в соответствии с заданными результатами обучения.
Взаимодействия	Поддержка развития учащегося как личности.	–
Поддержки	Использование приемов и методов обучения, мотивирующих и вдохновляющих учащихся учиться.	Использование приемов и методов активного обучения и саморегулирования.

Однако, каждый из учителей, удовлетворяющих критериям пригодности, неповторим, и способен добиться большего за счет профессионального роста, способствующего повышению эффективности его работы в школе.

В условиях, порождаемых третьей профессиональной революцией¹² и цифровой трансформацией, «каждому из нас – государству, обществу, бизнесу, конкретному человеку – необходимо соответствовать впечатляющей динамике перемен, осваивать новые знания и технологии, быстрее, решительнее идти в новую эру» [11]. Следовательно, необходим новый подход к оценке учителя. Происходящие изменения предъявляют новые требования к общему образованию, в том числе к федеральным государственным образовательным стандартам и к учителям, способным их реали-

¹² Первая была связана с появлением свободных профессий, вторая – с формированием массовых профессий [9, 10].

зовать. Ценность человеческого капитала, «значение образования как важнейшего фактора формирования нового качества» общества [12] существенно возрастают.

При этом необходимо учитывать следующее.

Во-первых, постижение сути происходящих изменений происходит не сразу, поэтому процесс уточнения, а то и изменение требований, предъявляемых к общему образованию, будет не одномоментным, а постепенным, растянутым по времени на многие годы, но он уже начался. Так, например, выступая на конференции по искусственному интеллекту 12 апреля 2020 года, Президент Российской Федерации В. В. Путин дал поручение Правительству Российской Федерации по совершенствованию преподавания математики и информатики в школах, указав на то, что необходимо:

- «начать наращивать «цифровой потенциал наших школ», т.к. технологии искусственного интеллекта, анализа больших данных «меняют повседневные привычки, весь уклад жизни людей», становятся «новыми возможностями, новыми инструментами достижения успеха»;
- быть лидерами в сфере искусственного интеллекта, а для этого надо быть лидерами в сфере школьного образования;
- повысить уровень «математического образования в школах», т.к. «достигнутый базовый уровень математики сегодня уже недостаточен» [11].

Нет сомнений в том, что по мере развития процесса цифровой трансформации требования к общему образованию будут продолжаться уточняться.

Во-вторых, нынешние школьники отличаются от тех, что были вчера, и цифровая трансформация будет способствовать ускорению этого процесса.

В-третьих, эффективность учителя существенно зависит от цели

обучения и условий его работы. Уточнение или изменение цели и требований к общему образованию может привести к тому, что те учителя, которые ранее работали эффективно, вдруг стали работать менее неэффективно или совсем неэффективно. Так, например, с переходом на ЕГЭ выяснилось, что не все учителя, успешно работавшие ранее, могут подготовить своих учеников к сдаче ЕГЭ [13, 14].

В-четвертых, проведение сравнительной оценки эффективности профессионального роста учителей методом опроса невозможно из-за несовпадения контингентов участников, оценивающих каждого из учителей. Конечно, можно проводить сравнительную оценку эффективности профессионального роста учителей по результатам сдачи ими соответствующего экзамена, но следует учитывать, что такая оценка будет получена каждым учителем в условиях, существенно отличающихся от тех, в которых он работает. В тоже время в системе образования циркулирует большой объем информации более высокого уровня достоверности, который можно бы было использовать для сравнительной оценки профессионального роста учителей.

Безусловно, точно измерить результат профессионального роста учителя нельзя, ибо проведение безупречного эксперимента здесь невозможно [15]. Однако возможна сравнительная оценка этих результатов, которая не может быть точнее данных внешних наблюдений за этим ростом, представленных в виде интервальных временных рядов, удовлетворяющих требованиям к полноте и сопоставимости их уровней. Это позволило разработать подход к проведению сравнительной оценки результатов профессионального роста учителей, изложение возможностей которого раскроем на примере учителей математики старших классов.

Сравнительную оценку эффективности профессионального роста учителей предлагается проводить на основе данных:

- о результатах сдачи каждым выпускником школы профильного ЕГЭ по математике (базового или профильного уровней);
- о выпускниках, поступивших после окончания школы в высшие и средние профессиональные учебные заведения, и их будущей специальности;
- о результатах «входного контроля» знаний математики, проводимого в различных вузах страны в начале первого семестра обучения;
- о результатах первичной сдачи студентами экзаменов по математическим дисциплинам за первый семестр обучения¹³;
- других сведений.

В этот перечень не включены сведения о сдаче каждым школьником ОГЭ, результатах написания ими всероссийских проверочных работ, т.к. их достоверность, хоть, возможно, и выше результатов опросов, но значительно ниже данных ЕГЭ (из-за возможности использования школьниками подсказок, шпаргалок и мобильных телефонов [13]).

Для сбора, передачи, накопления и хранения этих данных можно использовать любую современную территориально распределенную информационную систему. При этом важно, чтобы база данных информационной системы, содержащая совокупность указанных сведений, позволяла исследовать динамику их изменения по времени в связке учитель – ученики – их результаты.

Для расчета значений критериев сравнительной оценки результатов профессионального роста учителей можно использовать методы математической статистики. Поясним это на следующем примере.

¹³ При этом желательно, чтобы номера и темы контрольных заданий были такими же, что и в заданиях ЕГЭ.

Пример. Одним из проблемных вопросов в обучении школьников математике является их подготовка к сдаче профильного ЕГЭ. В этом случае сравнительную оценку результатов профессионального роста учителей можно произвести, используя метод парной регрессии. Рассмотрим таблично заданную функцию $y = f(x)$, где в качестве регрессора x_i , рассматривается каждый из учебных годов, в который его ученики сдавали ЕГЭ, а в качестве объясняемой, зависимой переменной y_i – среднее количество баллов, полученных этими школьниками на ЕГЭ. Сведем эти данные в табл. 2.

Таблица 2

Результаты ЕГЭ по математике профильного уровня за последние n лет

Значения y_i	y_1	y_2	y_3	...	y_n
Значения x_i	x_1	x_2	x_3	...	x_n

Будем искать зависимость между данными табл. 2 в виде уравнения парной линейной регрессии: $y = a + b \cdot x_i + \varepsilon_i$, где a и b – свободный член и угловой коэффициент прямой, соответственно, а ε_i – случайная ошибка, из-за которой среднее количество набранных школьниками в разные годы баллов y_i отклонялось от значения $y = a + b \cdot x_i$ то в большую, то в меньшую стороны. Подбор значений коэффициентов a и b произведем методом наименьших квадратов. Определив их, можно спрогнозировать результат, с которым школьники, обучающиеся у этого учителя, сдадут ЕГЭ в будущем году¹⁴, приняв его за рейтинговый показатель, который обозначим через R_1 . Проведя аналогичные расчеты для других учителей, можно составить их список, ранжирован-

ный по значениям данного рейтингового показателя (далее – первый список) и выбрать из них тех, кто добился лучших результатов в решении проблемного вопроса.

Однако вернемся к данному учителю, точнее к коэффициентам уравнения парной линейной регрессии, описывающему результаты его деятельности. Значение свободного члена a в нем характеризует уровень готовности к подготовке школьников к сдаче ЕГЭ на начальный момент рассматриваемого n – летнего периода, а угловой коэффициент b – скорость его профессионального роста в решении данного проблемного вопроса (значение которой может быть как положительной, так, к сожалению, и отрицательной), приняв их за рейтинговые показатели R_2 и R_3 , соответственно. Проведя аналогичные расчеты для других учителей, можно составить два новых списка учителей, ранжированных по значениям R_2 и R_3 , соответственно (далее – второй и третий список), и определить тех, кто в начале n – летнего периода наблюдений был лучшим по показателю R_2 , а также тех, кто за n – лет добился большего прогресса по показателю R_3 .

При подготовке школьников к сдаче профильного ЕГЭ по математике важно сформировать у них необходимые знания и умения для решения самых сложных заданий, оцениваемых четырьмя баллами (в первичной шкале измерения). Понимая под значением показателя y_i среднее количество баллов, полученных школьниками за выполнение таких заданий ЕГЭ, можно по аналогии с рассмотренным примером провести сравнительную оценку результатов профессионального роста учителей по данному показателю, и приняв его за рейтинговый показатель R_4 , составить новый рейтинговый список и определить тех, кто добился большего прогресса по этому показателю.

По аналогии с рассмотренным примером можно составить и дру-

¹⁴ При условии, что уровень сложности заданий будет таким же, как в предыдущие n лет.

гие рейтинговые списки:

- приняв за рейтинговый показатель R_5 долю выпускников, продолживших свое обучение в вузах, готовящих высококвалифицированных специалистов в интересах углубления цифровой трансформации страны (фундаментальная и прикладная математика, IT-технологии и робототехника, учитель математики и др.);
- приняв за рейтинговый показатель R_6 среднюю оценку, полученную первокурсниками при первичной сдаче экзаменов за первый семестр обучения по математическим дисциплинам¹⁵.

Подобных примеров сравнительных оценок профессионального роста учителей по различным критериям можно привести много. Заменяв модель парной линейной регрессии на модель множественной линейной регрессии, можно провести обобщенную оценку профессионального роста учителей. Можно также получить обобщенную оценку профессионального роста учителей, используя для этого метод среднего арифметического взвешивания различных частных показателей профессионального роста учителей.

Заключение

Сравнительная оценка профессионального роста учителей может меняться при изменении цели обучения, требований ФГОС общего образования и условий их работы. Предлагаемый подход позволяет уловить эту зависимость и, исходя из этого, помочь целенаправленному профессиональному росту учителей и повышению эффективности их работы в школе. Его можно использовать

¹⁵ Можно также использовать результаты «входного контроля» знаний студентом по курсу школьной математики.

при определении лауреатов ежегодного Всероссийского конкурса «Учитель года России», проводимого Министерством просвещения Российской Федерации, Общероссийским профсоюзом образования и «Учительской газетой».

Литература

1. Текст фильма «Доживем до понедельника», сценарий фильма «Доживем до понедельника». Электронный ресурс: <https://vvord.ru/tekst-filma/Dozhivom-do-ponedeljnika>. Дата обращения: 29 октября 2022 года.
2. Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации». Электронный ресурс: https://www.consultant.ru/document/cons_doc_LAW_140174. Дата обращения: 03 ноября 2022 года.
3. Трудовой Кодекс Российской Федерации от 30.12.2001 №197-ФЗ. Электронный ресурс: https://www.consultant.ru/document/cons_doc_LAW_34683. Дата обращения: 03 ноября 2022 года.
4. Приказ Минтруда России от 19.04.2021 №250н «Об утверждении профессионального стандарта «Руководитель общеобразовательной организации (управление дошкольной образовательной организацией и общеобразовательной организацией)». Электронный ресурс: <https://mintrud.gov.ru/docs/mintrud/orders/2093>. Дата обращения: 03 ноября 2022 года.
5. Кравцов: 15-20 процентов учителей не знают русский язык и математику. Электронный ресурс: <https://4ege.ru/obrazovanie/55671-kravcov-15-20-procentov-uchiteley-ne-znayut-russkiy-yazyk-i-matematiku.html>. Дата обращения: 04 ноября 2022 года.
6. Мониторинг эффективности школы. Учителя российских школ: проблемы и перспективы. Электронный ресурс: <file:///C:/Users/MSI%20ПК/Downloads/08-07-2019-monitoring-ef-shkol%20РАНХиГС.pdf>. Дата обращения: 04 ноября 2022 года.
7. Richards D., Lambert L. Evaluating Teaching Effectiveness at Utah Valley University: Past, Present, and Future. Электронный ресурс: https://www.uvu.edu/otl/docs/white_paper_evaluation_of_teaching_effectiveness_august_2018.pdf. Дата обращения: 08 октября 2022 года.
8. Заур-Бек С.И., Мерцалова Т.А., Анчиков К.М. Кадры школьного образования: возможности и дефициты / Мониторинг экономики образования:

2020: в 2 т. / Т. 1. Общее и среднее профессиональное образование. – М.: НИУ ВШЭ, 2021. – С. 67–83.

9. *Perkin G.* The third revolution: Professional society in international perspective. – Routledge: London and New York, 1996. – 253.

10. Управление персоналом: Учебник / Т. Ю. Базарова [и др.]; под ред. Т. Ю. Базарова, Б.Л. Еремина. – М: ЮНИТИ, 2002. – 560 с.

11. Стенограмма конференции по искусственному интеллекту Artificial Intelligence Journey (AI Journey 2020) от 12 апреля 2020 года «Искусственный интеллект – главная технология XXI века». Информационный ресурс: <http://www.kremlin.ru/events/president/transcripts/copy/64545>. Дата обращения: 17 июня 2022 года.

12. Конституция Российской Федерации. Электронный ресурс: https://www.consultant.ru/document/cons_doc_LAW_28399. Дата обращения: 03 ноября 2022 года.

13. Глава Рособнадзора: наша задача – привить школьнику культуру честности. Электронный ресурс: <https://tass.ru/interviews/4726457>. Дата обращения: 07 ноября 2022 года.

14. Готовьте ваши денежки: министр образования признал, что школа к ЕГЭ не готовит! Электронный ресурс: <https://dzen.ru/media/kp40.ru/gotovte-vashi-denezhki-ministr-obrazovaniia-priznal-chto-shkola-k-ege-ne-gotovit-5d70e67e3639e600adebc36a>. Дата обращения: 07 ноября 2022 года.

15. *Готтсданкер Р.* Основы психологического эксперимента. – М.: МГУ, 1982. – 464 с.

Содержание

<i>Введение</i>	3
ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ И СОЦИАЛЬНЫЙ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ	7
<i>И. В. Роберт</i> ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ	7
<i>В. Г. Мартынов, А. А. Туманов</i> ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АСПЕКТЕ ЦИВИЛИЗАЦИОННЫХ КУЛЬТУР	30
<i>В. М. Жураковский</i> ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТУДЕНТОВ В ИННОВАЦИОННО-ПРЕДПРИНИМАТЕЛЬСКОЙ СРЕДЕ СОВРЕМЕННОГО ВУЗА.....	49
<i>П. В. Кузьмин, В. А. Разумовский</i> ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В КОНТЕКСТЕ ГОСУДАРСТВЕННОЙ ОБРАЗОВАТЕЛЬНОЙ ПОЛИТИКИ.....	58
<i>Д. А. Гаврилов</i> ОБ УГРОЗАХ ОТЕЧЕСТВЕННОМУ ОБРАЗОВАНИЮ В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ.....	70
<i>Ю. Д. Алашкевич, Л. В. Юртаева</i> ОСНОВЫ ОТЕЧЕСТВЕННОГО ОБРАЗОВАНИЯ И ГУМАНИТАРНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНИЧЕСКОМ ВУЗЕ	80
<i>А. Л. Димова</i> ПОДГОТОВКА ЛИЧНОСТИ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОХРАНЕНИЮ ЗДОРОВЬЯ В УСЛОВИЯХ СОЦИАЛЬНО-ИНФОРМАЦИОННОГО ДАВЛЕНИЯ НЕДРУЖЕСТВЕННЫХ СТРАН	88
<i>М. В. Мананникова</i> АКСИОЛОГИЧЕСКИЕ ОСНОВЫ ОБРАЗОВАНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ	98

В. Вл. Чекмарев, Вл. В. Чекмарев НООСФЕРНАЯ БЕЗОПАСНОСТЬ: МАКРОСХЕМА КРИСТАЛЛА РОСТА	105
Н. Д. Подуфалов О ЗАДАЧАХ ОБЕСПЕЧЕНИЯ НЕОБХОДИМОГО УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ НАУЧНЫХ ИССЛЕДОВАНИЙ В УНИВЕРСИТЕТАХ.....	109
Р. З. Сафиева КУЛЬТУРНЫЙ КОД КАК ВЫСОКОЭФФЕКТИВНОЕ СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ	128
Е. А. Носков ОПРЕДЕЛЕНИЕ КОМПЕТЕНЦИЙ ПЕДАГОГОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК КОМПОНЕНТА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ.....	136
Е. В. Никульчев, П. Ю. Пушкин, Е. О. Карамышева АНАЛИЗ ИНЦИДЕНТОВ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ: 2020–2022	147
РЕАЛИЗАЦИЯ ВОЗМОЖНОСТЕЙ ЦИФРОВОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ДЛЯ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБРАЗОВАНИЯ	154
Е. В. Лопанова, Н. В. Савина ГОТОВНОСТЬ ПРЕПОДАВАТЕЛЕЙ ВУЗА К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ	154
В. А. Касторнова КОНЦЕПТУАЛЬНЫЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ С СОБЛЮДЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ	170
А. Д. Шматко ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ НЕКОНТАКТНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ОБРАЗОВАНИИ	183
Л. И. Миронова РЕАЛИЗАЦИЯ МЕЖДИСЦИПЛИНАРНОГО ПОДХОДА В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ.....	189

А. В. Рупецкий, Р. Р. Анамова ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ИНСТРУМЕНТОВ ПРОЕКТИРОВАНИЯ И ПРОИЗВОДСТВА В ОБРАЗОВАТЕЛЬНОЙ И НАУЧНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТА ТЕХНИЧЕСКОГО ВУЗА: ПЕДАГОГИЧЕСКИЙ КОНТЕКСТ	203
М. В. Карелина ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ НА ВЫСОКОТЕХНОЛОГИЧНОМ ТРЕНАЖЕРНОМ ОБОРУДОВАНИИ В ТРАНСПОРТНОМ ВУЗЕ.....	210
А. Е. Поличка, Е. А. Гец ОРГАНИЗАЦИЯ ПОДГОТОВКИ СТУДЕНТОВ МЕДИЦИНСКОГО ВУЗА К ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ	215
С. С. Галстян, Е. Р. Кроввиди ФОРМИРОВАНИЕ ЯЗЫКОВОЙ И РЕЧЕВОЙ КОМПЕТЕНЦИИ В ВУЗЕ ПРИ ОБУЧЕНИИ ИНОСТРАННЫМИ ЯЗЫКАМ	224
ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ШКОЛЕ	231
А. А. Николаева ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ И СОХРАНЕНИЯ ЗДОРОВЬЯ УЧЕНИКОВ ПРИ ИСПОЛЬЗОВАНИИ ГОЛОСОВОГО SMART-ПОМОЩНИКА В ОСНОВНОЙ ШКОЛЕ.....	231
В. И. Сердюков, Н. А. Сердюкова СТАТИСТИЧЕСКИ-ДОКАЗАТЕЛЬНЫЙ ПОДХОД К СРАВНИТЕЛЬНОЙ ОЦЕНКЕ РЕЗУЛЬТАТОВ ПРОФЕССИОНАЛЬНОГО РОСТА УЧИТЕЛЕЙ.....	241

МОНОГРАФИЯ

Авторы-составители
МАРТЫНОВ Виктор Георгиевич
РОБЕРТ Ирэна Веньяминовна
АЛЕХИНА Ирина Геннадьевна

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ЛИЧНОСТИ СУБЪЕКТОВ
ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА
В СОВРЕМЕННОМ ОБЩЕСТВЕ**

В АВТОРСКОЙ РЕДАКЦИИ

Компьютерная верстка: *Л. О. Иванова*

Подписано в печать 31.08.2023. Формат 60×90¹/₁₆.
Бумага офсетная. Гарнитура «Таймс». Усл. п. л. 15,875.
Тираж 500 экз. (1-й завод 001–100 экз.) Заказ № 244

ISBN 978-5-91961-489-0



Издательский центр
РГУ нефти и газа (НИУ) имени И. М. Губкина
119991, Москва, Ленинский проспект, дом 65
тел./факс: (499) 507 82 12