

*Ляхова Елена Георгиевна*

*Глаголев Александр Борисович*

*Душина Ирина Владимировна*

## **ЦИФРОВАЯ БЕЗОПАСНОСТЬ**

### **КАК НЕОТЪЕМЛЕМАЯ СОСТАВЛЯЮЩАЯ ОБУЧЕНИЯ ИНОСТРАННОМУ ЯЗЫКУ В НЕЯЗЫКОВОМ ВУЗЕ**

*Аннотация:* цель исследования заключается в разработке и научном обосновании необходимости включения в рабочую программу по иностранному языку в неязыковом вузе таких дисциплин как цифровая грамотность и безопасность, стандартизация цифрового пространства, средства шифрования, особенности Рунета и др. Результаты проведенного исследования позволяют сделать вывод о том, что формирование компетентного специалиста в эпоху цифровизации требует изменения содержания обучения иностранному языку. Особенно это важно при обучении иностранному языку будущих журналистов. Глава фокусируется на методике эффективного формирования новой компетенции в сфере цифровой безопасности у будущих журналистов.

*Ключевые слова:* обучение иностранному языку, цифровая грамотность, цифровая безопасность, цифровизация.

*Abstract:* the objective of the research consists in developing and substantiating scientifically a necessity of such disciplines as digital literacy, digital safety, digital standardization, encryption means and Runet peculiarities embedded into the process of foreign language teaching in non-linguistic universities. The results of the conducted research allow to conclude that mastering a competent specialist during digitalization era requires the changes in the foreign language teaching content. It is especially crucial to take this factor into account to teach future journalists a foreign language. The chapter focuses on the method to develop the new competency in the area of digital safety while teaching journalists a foreign language.

*Keywords:* foreign language teaching, digital literacy, digital safety, digitalization.

Основной стратегической задачей обучения иностранному языку специальности в неязыковом вузе является формирование, развитие и активизация знаний, умений и навыков, позволяющих будущему профессиональному полностью реализовать себя в своей деятельности. В процессе обучения иностранному языку у студентов постепенно формируется иноязычная профессиональная межкультурная компетенция, т. е. сочетание социально-значимых и профессионально важных качеств, готовность к постоянному совершенствованию этих качеств и актуализации их на практике в контексте межкультурных контактов в профессиональных целях [1; 5–7].

Специалисты рассматривают результат развития профессиональной личности, которая владеет иностранным языком специальности, как билингвальную профессиональную личность. Формирование такой личности происходит на трех уровнях – когнитивном, личностном и деятельностном [5].

На когнитивном уровне формируются понятия, свойственные иноязычной деловой коммуникации, и их описания средствами как родного, так и иностранного языков [5; 7].

На личностном уровне профессиональной билингвальной личности происходят изменения, связанные с выявлением системы профессиональных ценностей, формирование мотивации и целей своей профессии [5; 7]. Деятельностный уровень билингвальной профессиональной личности составляет умение найти оптимальные приемы качественного и творческого выполнения всех этапов профессиональной деятельности [5; 7].

При обучении иностранному языку в вузе необходимо так же ориентироваться на эти три уровня. В процессе обучения студенты должны иметь возможность осознать свои ценностные установки, научиться решать конфликты и выбирать альтернативы, опробовать различные варианты профессионального поведения, изучить различные ролевые модели на примере узкопрофессиональных ситуаций. Другими словами, для гармоничного формирования билингвальной профессиональной личности во время обучения иностранному языку необ-

---

ходимо создать развивающую среду, в которой обучающийся может стремится к своим целям и в процессе этого развивать свою компетенцию [1; 2; 7].

Содержание курса обучению иностранному языку должно соответствовать трем уровням формирования билингвальной личности, т. е. сферы и ситуации общения, темы и проблемы общения, а, также, учебные стратегии такого курса должны быть представлены студентам на когнитивном, личностном и деятельностном уровнях [5].

Рассмотрим, каким образом можно сформировать билингвальную профессиональную личность, учитывая изменения, происходящие на когнитивном, личностном и деятельностном уровнях, при обучении иностранному языку будущих журналистов.

На когнитивном уровне профессионального сознания журналиста сейчас на первый план выходит тема цифровой безопасности.

Журналисты способны выполнять роль интеграторов медийной и информационной грамотности и безопасности с потребностями общества и эта тема является одной из самых актуальных и востребованных при формировании профессиональных компетенций при обучении иностранному языку в неязыковом вузе [3].

Среди не менее важных тем на занятиях по иностранному языку в вузе можно назвать гендерные аспекты медийной и информационной грамотности, вопросы мониторинга и модерации деятельности СМИ с точки зрения смягчения потенциального негативного влияния на граждан, вопросы укрепления доверия к средствам массовой информации с помощью медийной грамотности и безопасности [3; 9].

Каждый преподаватель журналистики, студент факультета журналистики, журналист или профессионал в области регулирования СМИ или саморегулирования СМИ должны улучшить своё понимание и оценку медийной и информационной безопасности как стандарта в своей работе и учебе. Медийная и информационная грамотность и безопасность могут повысить качество этической

журналистики, укрепить доверие граждан к СМИ и правительству и таким образом стимулировать гражданскую активность населения [3].

Медийная грамотность и безопасность призваны стать важным и практическим инструментом для журналистов, педагогов вузов, регуляторов СМИ и организаций гражданского общества в реализации своей профессиональной деятельности.

В международной практике можно познакомиться с множеством публикаций по таким темам, как распознавание дезинформации, работа с дезинформацией, выявление лжи. Например, Международный центр журналистов (ICFJ) недавно опубликовал краткое руководство по истории дезинформации, где авторы рассказывают об эволюции нынешнего кризиса дезинформации. В публикации освещаются исторические моменты от эпохи Клеопатры до Cambridge Analytica<sup>2</sup> [1; 3; 5; 8].

Учебное пособие под названием Fred Fact Doesn't Fall for Desinformation, опубликованный Aos Fatos, бразильской платформой проверки фактов в апреле 2017 года, ясно показывает, как ложная информация может легко распространяться через цифровые СМИ [1; 3; 5; 8].

Примером последних публикаций о дезинформации является публикация ЮНЕСКО, выпущенная в 2018 г., «Журналистика, «фейковые новости» и дезинформация: справочник по журналистскому образованию и обучению». Публикация предлагает ряд способов, которыми журналисты могут бороться с дезинфекцией, распознавать недостоверную информацию, в том числе посредством медийной и информационной грамотности [1; 3; 5; 8].

Большинство инструментов и руководств, разработанных для СМИ, журналистов и журналистики, сосредоточены на том, как профессионалы СМИ могут улучшить качество своего контента.

Стандартная программа по журналистики в вузе включает следующие темы: способность СМИ влиять на политику, выборы и управление в целом; вклад СМИ в культуру различных стран и роль СМИ в сохранении культурных ценностей; потенциальное негативное влияние СМИ на жизнь и благополучие

4 <https://phsreda.com>

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

---

граждан; нередкое злоупотребление в распространении информации и вторжение в личную жизнь граждан; медийные и технологические посредники в коммерческих целях; усилия правительства по управлению и контролю над социальными изменениями; правительенная политика по управлению социальными изменениями и контролю СМИ; централизация владения СМИ; влияние на СМИ бизнеса и др.

Однако, в рабочих программах по иностранному языку для студентов, обучающихся по направлению «Журналистика», не уделяется серьезного внимания такой теме как формирование медийной грамотности среди гражданского населения. Движение гражданской активности имеет много граней, в том числе оно обладает огромным потенциалом для стимулирования межрелигиозного диалога, межкультурного диалога, развития социальной инклюзии, терпимости, мирного устойчивого развития в целом. Развитие медийной грамотности среди населения позволяет гражданам понять необходимость свободы СМИ, сформировать адекватное отношение к средствам массовой информации и к способам защиты конфиденциальности и т. д. Медийная грамотность может выступать в качестве альтернативы государственному регулированию и цензуре, но для этого необходимо формировать её и среди журналистов, и среди населения [1, 3, 5, 8].

Для этого в рабочие программы по журналистике необходимо включить следующие темы.

1. Продвижение информационной грамотности и безопасности среди населения, с помощью чего СМИ и ассоциации журналистов получат возможность саморегуляции вместо государственного регулирования, основанного на определенных стандартах, таких как пригодность определенного контента для детей, реклама и т. д. Активный диалог СМИ с гражданами может эффективно решить эти вопросы.

2. Разработка редакционной политики, соответствующей информационной грамотности и безопасности.

3. Как можно добиться прозрачности в отношении редакционной политики информационных ограничений.

4. Методы и программы, разрабатываемые журналистами для граждан с целью объяснить им, как создаются новости и другой медиаконтент.

5. Развитие медиа-партнерства с гражданским обществом.

6. Как лучше освещать в СМИ вопросы и проблемы, представляющие интерес для общественности.

7. Формирование прозрачности СМИ в отношении их собственников и характера их взаимоотношений со спонсорами и рекламодателями.

8. Интеграция информационной грамотности и безопасности в журналистскую практику.

9. Мониторинг и модерация сообщений СМИ для снижения потенциально-го негативного воздействия на граждан [6, 7, 9].

Случаи, когда некачественная журналистика и необоснованный контент в Интернете приводят к манипулированию сообщениями СМИ и, таким образом, к манипулированию людьми, встречаются довольно часто. ЮНЕСКО заявляет по этому поводу, что профессиональная и этичная журналистика является более эффективным и устойчивым способом защиты граждан, чем цензура. Граждане, владеющие информационной грамотностью, смогут прибегнуть к самозащите, распознав вредоносные сообщения [9].

Журналистское образование призвано повышать гражданское сознание среди журналистов, которые должны разбираться в том, что поможет им предугадать реакцию граждан на определенные сообщения, принять необходимые меры, чтобы управлять этими реакциями и документировать процесс.

Установление редакционной политики в организациях средств массовой информации является проверенным механизмом контроля того, что транслируется или публикуется. Однако, скорость, с которой должны выходить публикации, иногда приводит к снижению контроля качества.

Некоторые исследователи предлагают решить эту проблему введением трехуровневой защиты, обеспечивающей баланс актуальности информации, этической защиты и правдивости сообщения. С этой целью, помимо обучения журналистов стандартным принципам журналистики таким как правдивость,

6 <https://phsreda.com>

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

точность, актуальность, своевременность, сбалансированность, справедливость и беспристрастность, независимость и т. д., журналистское образование также должно выдвигать на передний план формирование компетенций, помогающих журналисту лучше модерировать и мониторить сообщения СМИ в интересах граждан. Среди них можно выделить следующие:

- психологическая грамотность в области когнитивного познания действительности, т. е. журналист должен знать, как человек усваивает информацию и уметь правильно представить аудитории свое сообщение;
- эмоциональная грамотность в области продвижения информации среди населения, т. е. журналист должен знать, как граждане реагируют на определенную информацию и уметь стимулировать критическое мышление у аудитории, продвигая свои сообщения;
- умение использовать онлайн инструменты и платформы для поддержания обратной связи с населением, обработки и оценивания отзывов и откликов, и обнародования выводов для этически-корректного воздействия на аудиторию.

Успешное формирование таких компетенций будущего журналиста должно помочь ему ориентироваться в современном информационном поле со всеми его преимуществами и недостатками и стать компетентным гидом в сфере информационной грамотности и, как следствие, информационной безопасности для граждан [1; 3; 5].

Первые попытки зафиксировать некоторые правила, ведущие к урегулированию наиболее важных составляющих информационного поля с точки зрения правового общества уже сделаны многими странами. Например, страны-члены ЮНЕСКО предлагают следовать следующим законам [1; 3; 5]:

- общество должно критически использовать и осмысливать различные источники информации, такие как библиотеки, СМИ, Интернет. При этом все источники информации считаются равными по статусу, что позволяет избежать доминирование той или иной информации и поощряет поиск альтернативных источников информации;

– каждый гражданин является одновременно потребителем и создателем информации. В условиях современных интернет-технологий каждый человек становится автором, соавтором и распространителем информации, что ведет к необходимости считать обязанностью каждого человека быть информационно-грамотным для того, чтобы избежать нарушения им информационной безопасности других граждан, с одной стороны, и не стать самому жертвой, с другой стороны. Правительства должны обеспечить равный доступ к информационным инструментам для всех граждан, внеся соответствующие изменения в своё законодательство;

– гражданам необходимо объяснять, что любая информация, несущая какое-то знание, не всегда бывает нейтральна, независима или беспристрастна. Это явление не обязательно связано с манипуляцией, так как даже просто подбирая и сортируя факты, выбирая, что первично, а что вторично, мы уже влияем на информационный продукт. Это процесс, с помощью которого люди описывают мир со своей точки зрения;

– каждый гражданин имеет право и должен иметь возможность получать новую информацию и знания, даже если он не выражает это желание. Это принцип уже закреплен законом во многих странах, но, в связи с бурным развитием интернет-технологий это право стало более размытым. Важно, чтобы это право на информацию и на общение с другими людьми, которое изменилось в связи с развитием новых технологий, не нарушалось при переходе на электронный формат обмена информацией;

– информационная безопасность зависит от медийной и информационной грамотности, которая формируется в результате приобретения знаний, формирования навыков и длительного опыта использования, создания и передачи информации, начиная с дошкольного возраста и в течении всей жизни [1; 3; 5]. Информация сегодня окружает и сопровождает каждого гражданина везде и всегда. Если принять во внимание все медиаресурсы, находящиеся в каждом доме и в каждой семье, то станет очевидным, что формирование медиа-информационной грамотности сегодня обусловлено такой же первичной потребностью как необходимость пищи, личной гигиены и т. д.

## *Стандартизация информационной безопасности*

С точки зрения когнитивного наполнения содержания курса обучения иностранному языку будущих журналистов в последнее время на передний план выходит тема стандартизации информационной безопасности.

Стандарты определяют систему управления экономикой страны, способствуя повышению эффективности производства, своевременному внедрению инновационных технологий и поддержанию общественного блага. Развитие цифровых технологий приводит к созданию новых бизнес-моделей, которые должны вписаться в традиционные нормы и законы общества [1; 3; 5]. Правила, регулирующие цифровые подходы, должны быть более гибкими и использовать экспериментальные варианты, упреждающие подходы и ориентацию на активное международное сотрудничество.

Среди множества появившихся в последнее время цифровых инноваций выделяются следующие семь основных направлений: искусственный интеллект, «большие данные», блокчейн/технология распределенных ресурсов, Интернет вещей, робототехника, 3D-печать, автономные транспортные средства. Эти направления обладают различным влиянием на общество и различной скоростью развития, поэтому стандартизация призвана гармонизировать их преимущества с потребностями потребителей, обеспечив формирование понимания, каким образом использовать эти технологии; какие риски необходимо предотвратить при их распространении; каким образом получить кумулятивный эффект от их использования и как эффективно приспособить этот инновационный продукт к уже существующим технологиям [1; 3; 5].

Обучение будущих журналистов, направленное на формирование новых профессиональных компетенций, составляющих информационную грамотность как самих специалистов, так и их способность обучать граждан информационной безопасности, происходит в период бурного развития инновационных технологий с одной стороны и противоречивой политической обстановки с другой стороны.

Разработка и внедрение новых подходов к обучению в этих условиях невозможны без стандартизации в сфере информационной безопасности. Сейчас в

мире существуют следующие организации, занимающиеся этими вопросами на национальном и международном уровнях: Госстандарт России, Американский национальный институт стандартов (специализируется на языках программирования и интерфейсах, сетевых протоколах, передачи и шифровании данных), Европейская ассоциация производителей компьютеров (стандартизация в области информационных и вычислительных систем), Международная организация по стандартизации с огромным набором созданных и создаваемых стандартов, Международная электротехническая комиссия (занимающаяся стандартами в области электротехники и электроники), Институт инженеров по электротехнике и радиоэлектроники (стандарты по программным и инженерным системам и сетевые стандарты), Национальный институт стандартов и технологий США и др [1; 3; 5].

Проанализировав такое многообразие организаций, которые активно разрабатывают стандарты для общего информационного пространства современности и будущего, можно сделать следующие выводы: 1. рабочий язык почти во всех перечисленных организациях – английский; 2. будущие специалисты нашей страны должны уметь сотрудничать с представителями данных организаций и быть в курсе тех инноваций, которые они предлагают. Следовательно, в рабочую программу по профессиональному английскому языку в неязыковом вузе необходимо ввести тему стандартизации информационного пространства в контексте возможного влияния на решения международных организаций в этой сфере.

Классификация цифровых стандартов довольно сложная. Согласно исследованиям, их можно разделить на две большие категории:

- стандарты уровня и статуса, связанные с цифровизацией экономики (т. е. цифровая трансформация);
- стандарты по отдельным цифровым технологиям.

Наиболее востребованные стандарты в современной цифровой экономике – это стандарты на:

- цифровые шины и интерфейсы (PCI, USB и др.);
- способы кодирования и сжатия, форматы цифровых аудио-материалов и видеоматериалов (MPEG ISO, MP3 и др.);

- на шифрование данных, т. е. криптографические стандарты (AES и др.);
- на языки программирования (ANSI C, ANSI Fortran и др.);
- на построение компьютерных и коммуникационных сетей и сетевые протоколы (HTTP и др.);
- на технологии цифровой мобильной сотовой связи (GPRS, EDGE и др.);
- цифровой транкинговой радиосвязи (TETRA, APCO 25 и др.);
- военное оборудование MIL STD;
- цифровое телевидение и телевидение высокой четкости (ЦТВ, ТВЧ) [1; 3; 5].

Каждое из вышеперечисленных направлений так или иначе связано с повседневной работой современного журналиста. В рабочих программах по профессиональному иностранному языку по направлению журналистики современные технологии освещаются с точки зрения возможности их использования при поиске или передачи информации, теперь же для будущего журналиста возникает необходимость изучать способы и методы безопасного использования цифровых технологий.

При составлении стандартов по инновационным технологиям специалисты используют следующие принципы:

- достоверность, прозрачность, необходимость информировать потребителей как о достоинствах, так и о возможных недостатках и угрозах, возникающих наряду с преимуществами;
- всеохватность. Инновационные ресурсы распределены неравномерно, что приводит к нарушению прав тех людей, которым они не доступны;
- устойчивость. Этот принцип, предусматривающий такое внедрение и распространение новшеств, которое будет способствовать развитию людей, планеты, процветанию и миру.;
- совместимость. Внедрение инноваций стремительно меняет характер производства, какие-то профессии становятся ненужными, в то же время появляются новые рабочие места и стандарты должны стать регулятором, который обеспечит плавный переход на новые технологии, заранее перераспределяя кадры;

- надежность и безопасность. Этот принцип вытекает из предыдущих и связан с физической, психологической и цифровой безопасностью общества в целом и отдельных потребителей;
- конфиденциальность данных. Этот принцип отстаивает право людей на личную жизнь, которое необходимо соблюдать и в условиях цифрового изменения общества;
- принцип международного сотрудничества утверждает, что все вышеперечисленные принципы возможно соблюсти только в условиях максимальной открытости и прозрачности сотрудничества между странами всего мира, так как решение проблемы цифрового изменения общества лежит на глобальном уровне.

Активное развитие цифровой экономики продолжается, с чем связана потребность в новых стандартах и технологиях, которые будут регламентировать использование искусственного интеллекта, интернета вещей, умных домов и городов, аддитивного производства и т. д. Большинство современных стандартов относящихся к цифровым технологиям написаны на английском языке, что ставит перед будущими специалистами задачу грамотного и своевременного перевода необходимых документов на русский язык. Работа с современными технологиями в России требует внедрения действующих международных стандартов так же, как и активного участия российских специалистов в международных организациях по стандартизации и создания новых стандартов с учетом специфики нашей страны. Без этого невозможно регулировать качество услуг в сфере информационных технологий и расширения цифрового бизнеса [1; 3; 5].

### *Средства шифрования*

Обсуждая необходимость повышения цифровой безопасности, нельзя не сказать о том, что первостепенной задачей этой сферы деятельности является защита конфиденциальности каждого гражданина, использующего цифровые технологии.

Защита данных от прочтения их лицами, для которых эта информация не предполагалась, называется криптографией (от греческого κρυπτός – скрытый и γράφω – писать). Для современного журналиста, выступающего в качестве но-

---

сителя знаний о цифровой безопасности, и просвещдающего население по вопросам безопасного получения и распространения информации, оказывается не лишним знать криптологию, т. е. науку о шифровании и дешифровании.

Согласно анализу состояния дел на сегодняшний день, шифрование данных можно разделить на две большие группы методов обработки – полное шифрование диска и шифрование отдельных папок и файлов. Эти группы составляют наиболее надежный способ защиты данных и пользуются максимальным спросом. Обычно, организации, заказывающие такие услуги, сочетают оба способа, так как они предназначены для решения различных частных задач сохранения конфиденциальности. В ближайшее десятилетие планируется увеличение спроса на защиту данных в корпоративном секторе экономики. По оценкам экспертов, объем рынка шифрования возрастет более чем на 50%.

Представители Комитета по правам человека при ООН заявили, что основой цифровой безопасности является сохранение анонимности и связанные с этим возможности шифрования в цифровых коммуникациях. Грамотная и надежная защита данных в интернете позволяет поддержать право пользователей на свободу мнений и их выражение.

Обнаружено, что если государство ограничивает доступ к шифрованию данных, то от этого страдают его граждане, права которых нарушаются. В эпоху цифровизации конфиденциальность и безопасность неразрывно связаны с шифрованием и анонимностью информации, с возможностью граждан осуществлять права на свободу мнений и свободно выражать свои идеи. В свою очередь, из обеспечения этого права вытекает осуществление других прав, таких как имущественные права, право на свободу ассоциаций и собраний, неприкосновенность частной жизни и физическая неприкосновенность граждан, право на жизнь [1; 3; 5].

Журналисты всегда стояли на страже этих священных прав каждого человека в гражданском обществе, отстаивали их, описывая случаи их нарушения, проводя журналистские расследования, чтобы общество могло воздействовать на их нарушителей. В цифровую эпоху для продолжения миссии журналиста

как защитника основных общественных устоев, специалисты в этой сфере обязаны знать особенности различных методов шифрования данных и уметь объяснить гражданину, для чего они необходимы и как их использовать.

Так, например, Рунет использует меньше зашифрованных данных по сравнению с глобальной сетью, но в последнее время количество доменов с SSL-сертификатами резко выросло, а в будущем, по отзывам аналитиков, зашифрованный трафик может достигнуть 95%.

В то же время во всем мире наблюдается противоположная тенденция отслеживания трафика в реальном времени, что противоречит самой идеи конфиденциальности данных, но необходимо в определенных ситуациях для поиска нарушителей, представляющих угрозу безопасности. С целью повышения информационной безопасности в России создан реестр трансграничных линий связи для того, чтобы фиксировать трансграничные переходы трафика [1; 3; 5].

Компетентный журналист призван проанализировать каждый противоречивый, касающийся информационной безопасности случай и представить его общественности в максимально прозрачном и понятном виде.

### *Рунет*

Еще одна животрепещущая тема, которая должна быть освещена в рабочей программе по профессиональному иностранному языку для журналистов, это развитие и организация работы суверенного Рунета, являющегося российским сегментом интернета. На поддержку его эксплуатации и гарантитное обслуживание установленного оборудования предусмотрено выделить 15% от суммы в 31 млрд. рублей, создание и развитие программно-аппаратного комплекса и расширение каналов связи требует до 35% от этой суммы. Основная же сумма, около 20 млрд. рублей, должна быть потрачена на информационную безопасность проекта, т. е. на технические средства противодействия угрозам. Кроме того, был принят закон о штрафах за нарушение правил установки и использования оборудования, необходимого для противодействия угрозам устойчивости российского интернета. Предусмотрена и ответственность за нарушение владельцем информационного

ресурса основополагающих прав и свобод человека, прав и свобод граждан РФ, в том числе на свободу массовой информации [1; 3; 5].

Для формирования журналистской компетентности в сфере информационной безопасности необходимо дать студентам возможность почувствовать себя ответственными за общественную информационную безопасность. С этой целью целесообразно включение в рабочую программу учебной деловой игры для магистров-журналистов «Мой Рунет», в которой они обсуждают уже принятые законы по обеспечению информационной безопасности российского интернета и предлагают свои законы и правила Рунета.

#### *Контроль или анонимность в интернете*

Специалисты и эксперты по информационной безопасности обсуждают масштабы распространения сети и ее влияния на человечество, которые достигли такого масштаба, что дальнейшее ее развитие без регулирования представляет собой реальную угрозу. В то же время, очевидно, что мониторинг деятельности пользователей ограничивает их конституционные права и свободы [1; 3; 5].

В США создана программа «Свобода интернета», которая направлена на комплексную поддержку общества и продвижение свободного потока информации и состоит из четырех направлений.

1. Направление, посвященное технологиям, предлагает различные способы использования современных технологий Интернета и разрабатывает методы противодействия цензуре.

2. Направление, изучающее цифровую безопасность, способствует развитию цифровой безопасности в обществах с репрессивным подходом к Интернету.

3. Следующее направление «Политика и защита прав» разрабатывает правозащитные меры, противодействующие ограничительным законам в сфере интернет-регулирования.

4. Направление «Прикладные исследования» сфокусировано на повышение пользы программы «Свобода интернета» во всем мире, привлекая организации, желающих участвовать в этой программе на глобальном или на региональном уровнях. Участникам программы предлагаются гранты до 3 млн. долларов [1; 3; 5].

В рамках подобной программы возможно совместить разумный контроль с осуществлением прав и свобод граждан.

В целях формирования журналистской компетенции в сфере информационной безопасности у будущих журналистов мы предлагаем включить в рабочую программу по английскому языку учебную деловую игру «Контроль или анонимность. Совместить несовместимое». В рамках этой игры студенты разрабатывают программу, аналогичную американской «Свобода интернета», которая помогает осуществлять мягкий контроль цифровой информации и, в тоже время, позволяет пользователям изучать и распространять информацию без нарушения их прав и свобод.

#### *Дети и вредоносное влияние онлайн-контента*

Говоря о контроле в интернете, нельзя не согласится с необходимостью усилить меры по защите детей от опасной информации. Правозащитники пытаются оградить детей не только от прямо запрещенного контента, но и от информации, которая формально не запрещена, но в определенных случаях может быть вредна для несовершеннолетних. Например, в России существуют законы, защищающие детей от такой запрещенной информации как детская порнография, материалы об изготовлении наркотиков и др. Кроме того, этот запрет действует и в отношении вредного контента, к которому относятся насилие, нецензурная брань, жестокость и др.

Российский закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» требует от социальных сетей блокировать социально опасный контент сразу после его выявления и ежегодно отчитываться о результатах самоконтроля своей сети [9].

Если пользователь находит вредоносную информацию, он может сообщить об этом с помощью специального приложения через официальный сайт Роскомнадзора, после чего происходит проверка, и по результатам суда противоправные материалы блокируются [9].

Законопроекты Ирландии и Великобритании контролируют помимо незаконного контента, информацию, которая оказывает значительное психологиче-

---

ское и физическое воздействие на детей, к которой относятся сообщения о суициде, легальная порнография, демонстрация самоповреждений. Онлайн-платформы обязаны контролировать количество пользователей, которые прочтут этот материал и скорость его распространения.

ЕС полагает, что поставщики цифровых услуг должны фильтровать незаконную и нежелательную информацию. В создающемся Законе о цифровых услугах указано, что порталы должны предоставить пользователям возможность подать и оспорить жалобу на вредоносный контент, с последующей отчетностью о результатах [8; 9].

В Италии с 2017 года сайты удаляют незаконные материалы по требованию родителей или несовершеннолетних старше 14 лет в течение 2 суток.

В Индии публикация материалов с пометкой «только для взрослых» приводит к необходимости провести проверку возраста потребителя.

В Китае для защиты информационной безопасности детей ввели закон, который требует подтверждение личности пользователя в онлайн-видеоиграх. Если ребенок младше возрастной категории, указанной в игре, он не сможет играть в неё. Подтверждение возраста происходит на государственном уровне [9].

*Учебные деловые игры, имитирующие деятельность журналиста в сфере цифровой безопасности, как инструмент формирования билингвальной профессиональной личности будущего журналиста*

Процесс профессионального становления неразрывно связан с разрешением противоречия, возникающего между характерными свойствами личности и теми качествами, которые требует от человека его профессия. Движущей силой для возникновения необходимых изменений в личности обучающегося становится ориентация учебного процесса на его профессиональное развитие, которое формирует обобщенные способы решения профессиональных задач.

В практике обучения инструментом, позволяющим этого добиться, являются учебные деловые игры. Учебная деловая игра по иностранному языку представляет собой комплексное учебное мероприятие, включающее разнообразные задания и все виды речевой деятельности, имитирующее профессиональную

ситуацию общения, в которой студенты в процессе совместной деятельности решают поставленные перед ними задачи. Каждый участник такого обучения получает возможность проявить свои творческие, лидерские, командные способности. Элемент соревнования усиливает учебную мотивацию студентов. При обучении иностранному языку в процессе деловой игры обучающиеся погружаются в языковую среду, так как общаются только на изучаемом иностранном языке. Учебные деловые игры требуют значительных временных затрат от преподавателя на их подготовку, но, в то же время, этот вид учебной работы является незаменимым, когда понимание темы требует от обучающихся практического участия [2; 4; 7].

Для будущих журналистов мы разработали целую серию учебных деловых игр, которые позволяют проработать тему цифровой безопасности на должностном уровне, способствуя эффективному формированию иноязычной коммуникативной профессиональной компетенции студентов. Приведем здесь пример такой игры.

#### *Деловая учебная игра «Счастливое цифровое детство»*

Вопрос о том, какие угрозы существуют в современном цифровом мире для детей и каким образом журналист может повлиять на создание безопасной цифровой среды для детей был поднят во время учебной деловой игры «Счастливое цифровое детство», проходившей в МГЛУ с магистрами 1 курса, обучающимися по направлению Журналистика.

#### **Сценарий игры**

Участники игры делятся на две команды: команда родителей и команда журналистов. Команда родителей ищет в интернете англоязычную информацию о всех возможных цифровых угрозах, с которыми сталкиваются дети. Команда журналистов собирает англоязычную информацию о том, как можно обезопасить детей и ответить на цифровые угрозы. После сбора информации участники игры проводят пресс-конференцию, на которой выступают родители, а журналисты комментируют их выступления и предлагают свои решения проблемы цифровой безопасности детей.

---

*Список цифровых угроз, составленный командой родителей (перевод на русский язык)*

1. Подключение к сети и работу в диалоговом режиме трудно контролировать. Дети могут познакомиться с вредоносной информацией, последствия такого знакомства могут быть самые негативные. Среди которых – киберзапугивание, нелегальная информация на порно- и игровых сайтах, жестокое обращение, эксплуатация и торговля детьми и др.

2. Пока дети используют подключенные устройства для игры или общения в Интернете, эти устройства собирают о них информацию, которая в дальнейшем может попасть к нечистым на руку людям.

3. Сложно соблюсти правильный баланс между предоставлением ребенку возможности для самостоятельного освоения мира и развития и тщательным контролем.

4. Интернет усиливает психологические проблемы неблагополучных детей. В то же время, испытывающий трудности в общении ребенок может получить в интернете поддержку и найти друзей.

5. Родители вынуждены приобретать дорогостоящие устройства, чтобы их дети могли идти в ногу со временем.

6. Вопрос о том, какое количество времени ребенок может проводить у экрана, до сих пор не решен, что приводит к тому, что многие дети все время постоянно применяют цифровые технологии.

7. Дальнейшее развитие цифровых технологий только усилит пропасть между благополучными и маргинализированными детьми, которые, с одной стороны лишены возможности иметь современные дорогостоящие цифровые устройства, а, с другой стороны, больше подвержены вероятности причинения вреда в сети [5; 8; 9].

*List of digital threats compiled by the team of parents*

1. Network connection and online operation are difficult to control. Children can get acquainted with harmful information, the consequences of such acquaintance can

be the most negative. Among them are cyberbullying, illegal information on porn and gaming sites, abuse, exploitation and trafficking of children, etc.

2. While children use connected devices to play games or communicate on the Internet, these devices collect information about them, which can later fall into the hands of dishonest people.

3. It is difficult to strike the right balance between giving the child the opportunity to independently explore the world to develop their personalities and careful control.

4. The Internet amplifies the psychological problems of disadvantaged children. At the same time, a child with difficulties in communication can get support on the Internet and find friends.

5. Parents are forced to purchase expensive devices so that their children can keep up with the times.

6. The question of how much time a child can spend in front of the screen is still unresolved, which leads to the fact that many children constantly use digital technologies all the time.

7. Further development of digital technologies will only widen the gap between well-to-do and marginalized children, who, on the one hand, are deprived of the opportunity to have modern expensive digital devices, and, on the other hand, are more likely to be harmed online.

*Меры, предложенные журналистами по созданию безопасной цифровой среды для детей (перевод на русский язык)*

1. Обеспечить всем детям доступ по умеренной стоимости к онлайновым ресурсам. Так как это обеспечит им равенство возможностей в обучении, поиске работы, общении.

Для этого необходимо: – снижать стоимость подключения к сети во всех регионах мира; – обеспечивать общественные точки доступа к сети в неблагополучных регионах; – заниматься создание полезного развивающего контента на языке ребенка; – воздействовать на обеспечение равного доступа для всех

---

граждан, на муниципальных и общинных уровнях; – предоставлять доступ детям беженцам и мигрантам.

2. Обеспечить защиту детей от цифровых угроз. Для этого: – предоставлять информацию о вредоносных сайтах правозащитным органам; – борьба с сексуальной эксплуатацией детей в интернете (например, присоединившись к деятельности Глобального Альянса «WePROTECT»); – обеспечить защиту детей в соответствии с их возрастом; – помогать людям, способным поддержать детей, например, формировать у родителей навыки позитивного посредничества вместо политики запретов.

3. Каждый производитель цифрового контента должен обеспечивать конфиденциальность личных данных детей, не позволяя их использование в целях рекламы и в других целях. Для этого: – школы и другие детские организации, которые обладают банком информации о детях должны предпринимать меры по обеспечению неприкосновенности этих данных; – все компании, производящие цифровой контент для детей должны обеспечить неприкосновенность данных и, в случае нарушения этого принципа, прямо и понятно сообщать об этом ребенку или его родителям; – запретить требовать ввод личных данных от ребенка с целью рекламы, установив жесткие этические протоколы; – повысить степень конфиденциальности при шифровании данных детей и расшифровывать их только в целях защиты ребенка специальными органами правопорядка.

4. Объяснять и обучать детей мерам предосторожности при работе в сети, формируя у них цифровую грамотность. Для этого: – включить в учебные планы школы дисциплину по цифровой грамотности; – использовать при обучении детей только зарекомендовавшие себя как безопасные методы обучения онлайн; – организовать специальные центры профессиональной подготовки, в которых дети из неблагополучных семей смогут получить цифровое образование и научиться цифровой грамотности; – развивать соответствующие навыки и умения у преподавателей, регулярно проводя повышение квалификации; – создать доступные для всех детей онлайн библиотеки; – дети должны понимать, что при совместном использовании контента в соц. сетях информация перестает

быть конфиденциальной и учиться не подвергать риску себя и своих собеседников; – дети должны уметь настраивать параметры конфиденциальности при работе онлайн; – необходимо прививать детям привычки психологически грамотного общения в сети, они должны понимать, что общаться лучше, проявляя эмпатию, сочувствие и не вступая в конфликты; – взрослые люди, особенно родители, должны представлять собой модель корректного и безопасного поведения в сети.

5. Частный сектор цифровой экономики должен повысить свою ответственность за информацию, которая поступает к ним от детей. Для этого: – необходимо предотвращать появление вредоносного материала, особенно, связанного с насилием над детьми; – предоставлять детям доступ к образовательному, образовательно-развлекательному контенту без дискриминации; – разработчики цифрового контента должны следовать принципу проектной безопасности, ориентируясь на этические стандарты; – специально для родителей необходимо предлагать набор простых и эффективных инструментов безопасности, с помощью которых они могут создать для своих детей комфортную виртуальную среду.

6. Стандарты и правила, которые сейчас разрабатываются для цифровой индустрии направлены на взрослого потребителя, хотя дети составляют треть пользователей Интернета. При разработке стандартов необходимо учитывать прежде всего интересы безопасности детей, от благополучия которых зависит будущее нашего общества. Для этого: – необходимо изучить потребности и интересы детей в цифровом контенте и стимулировать их высказываться по этим вопросам; – выявлять случаи нарушения потребностей детей в доступе к Интернету и устранять их; – включить в национальную политику вопросы, связанные с созданием комфортной и безопасной цифровой среды для детей как важнейшие вопросы, влияющие на будущее всего общества.

*Measures proposed by the journalists to create a safe digital environment for children*

1. Provide all children with affordable access to online resources since this will provide them with equal opportunities in training, job search, communication.

To do this, it is necessary – to reduce the cost of connecting to the network in all regions of the world; – provide public access points to the network in disadvantaged regions; – engage in the creation of useful educational content in the language of the child; – influence the provision of equal access for all citizens, at the municipal and community levels; – provide access to refugee and migrant children; -

2. Protect children from digital threats. For this: provide information about malicious sites to human rights bodies; – combating the sexual exploitation of children on the Internet (for example, by joining the activities of the Global Alliance «WePROTECT»); – ensure the protection of children in accordance with their age; – help people who are able to support children, for example, to form parents' skills in positive mediation instead of a prohibition policy.

3. Each producer of digital content must ensure the confidentiality of children's personal data, not allow their use for advertising and other purposes. For this: schools and other children's organizations that have a bank of information about children should take measures to ensure the inviolability of these data; – all companies producing digital content for children must ensure the integrity of data and, in case of violation of this principle, directly and clearly inform the child or his parents about this; – prohibit requiring the input of personal data from a child for the purpose of advertising by establishing strict ethical protocols; – increase the degree of confidentiality when encrypting children's data and decrypt them only for the protection of the child by special law enforcement agencies.

4. Explain and educate children about safety precautions when working online, developing their digital literacy. For this: include the discipline of digital literacy in the school curricula; – use only proven safe online learning methods when teaching children; – organize special vocational training centers where children from disadvantaged families can receive digital education and learn digital literacy; – to develop the relevant skills and abilities of teachers, regularly conducting advanced training; – create online libraries accessible to all children; – children should understand that when sharing content on social networks, information ceases to be confidential and learn not to put yourself and your interlocutors at risk; – children should be able to

adjust privacy settings when working online; – it is necessary to instill in children the habits of psychologically competent communication on the network, they must understand that it is better to communicate, showing empathy, sympathy and not entering into conflicts; – adults, especially parents, should be a model of correct and safe online behavior.

5. The private sector of the digital economy should increase its responsibility for the information that comes to them from children. For this: it is necessary to prevent the appearance of harmful material, especially related to violence against children; – provide children with access to educational, educational and entertainment content without discrimination; – developers of digital content should follow the principle of design safety, focusing on ethical standards; – especially for parents, it is necessary to offer a set of simple and effective security tools with which they can create a comfortable virtual environment for their children.

6. The standards and regulations that are currently being developed for the digital industry are aimed at the adult consumer, although children make up a third of Internet users. When developing standards, it is necessary to take into account, first of all, the interests of the safety of children, on whose well-being the future of our society depends. For this: it is necessary to study the needs and interests of children in digital content and encourage them to speak out on these issues; – identify cases of violation of the needs of children in access to the Internet and eliminate them; – include in the national policy issues related to the creation of a comfortable and safe digital environment for children as the most important issues affecting the future of the whole society.

По результатам проведения пресс-конференции были сделаны следующие выводы.

Не надо ограничивать ребенка в использовании цифровых технологий, но необходимо более внимательно относиться к ребенку и обучать его цифровой гигиене (использованию цифровых устройств без нанесения вреда своему здоровью). Ребенок должен уметь пользоваться устройствами, находясь в комфортной позе, делать перерывы, не пользоваться устройствами во время важных

---

действий, например, переходя через дорогу. Родители должны регулярно отслеживать, каким контентом пользуется ребенок и формировать у него умение узнавать вредоносную информацию и избегать её.

Необходимо более тщательно исследовать влияние цифровых устройств на детей различных возрастных и социальных групп.

### *Вывод*

Таким образом, можно сделать вывод о том, что актуальная рабочая программа по иностранному языку для журналистов должна включать в себя такие дисциплины как информационная грамотность и цифровая безопасность, которые целесообразно преподавать с целью сформировать новую компетенцию у будущих журналистов, призванных не только обеспечить собственную безопасность в цифровой среде и безопасность тех средств массовой информации, на которые они работают, но и сформировать и поддерживать информационную безопасность всего социума. При этом необходимо уделить особое внимание изучению стандартов цифровой безопасности, в дальнейшей разработке которых будущие журналисты смогут принять активное участие. Для повышения эффективности формирования компетенции, связанной со знанием цифровой безопасности на занятиях по иностранному языку в неязыковом вузе, предпочтительно обратиться к обучающим деловым играм, примеры которых приведены в статье.

### *Список литературы*

1. Блохина Н.Ю. Современные образовательные технологии в рамках реализации федерального проекта «Цифровая образовательная среда» / Н.Ю. Блохина, Г.А. Кобелева. – Киров, 2020. – 70 с.
2. Кириленко В.П. Развитие медиабизнеса в условиях глобальной цифровизации / В.П. Кириленко, Е.Ю. Колобова // Управленческое консультирование. – 2021. – №2. – С. 127–142. – DOI 10.22394/1726-1139-2021-2-127-142. – EDN КСХПК
3. Ляхова Е.Г. Обучение иностранному языку в неязыковом вузе как процесс формирования билингвальной картины мира в рамках компетентностного

и контекстного подходов / Е.Г. Ляхова // Обзор педагогических исследований. – 2022. – Т. 4., №1. – С. 41–45. – EDN PAPJWO

4. Организация объединённых наций по промышленному развитию. Стандарты и цифровая информация. Эффективное управление в цифровую эпоху. ЮНИДО, 2021. – 17 с [Электронный ресурс]. – Режим доступа: [https://hub.unido.org/sites/default/files/publications/V2\\_RUSSIAN\\_Standard\\_digital\\_transformation\\_ONLINE\\_FINAL.pdf](https://hub.unido.org/sites/default/files/publications/V2_RUSSIAN_Standard_digital_transformation_ONLINE_FINAL.pdf) (дата обращения: 07.07.2023).

5. Сагитова Р.Р. Веб-квест технологии в обучении иностранным языкам / Р.Р. Сагитова, А. Гайнуллина // Казанский вестник молодых ученых. – 2019. – №5 (13) [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/veb-kvest-tehnologii-v-obuchenii-inostrannym-yazykam/viewer> (дата обращения: 02.07.2023).

6. Храпов С.А. Философия рисков цифровизации образования: когнитивные риски и пути создания безопасной коммуникативно-образовательной среды / С.А. Храпов, С.В. Баева // Вопросы философии. – 2021. – №4. – С. 17–26. DOI 10.21146/0042-8744-2021-4-17-26. EDN BQFETT

7. Цацкина Е.П. О лингвистической подготовке кадров по информационной безопасности на этапе перехода к цифровой экономике / Е.П. Цацкина, Н.Ю. Мороз, Е.Г. Ляхова // Обзор педагогических исследований. – Т. 3., №6. – С. 162–167.

8. Чевтаева Н.Г. Цифровизация в коммуникации участников образовательного процесса / Н.Г. Чевтаева // Стратегии развития социальных общностей, институтов и территорий. – Екатеринбург: Изд-во Урал. ун-та, 2021. – Т. 1. – С. 374–378. – EDN PKEPAJ

9. ЮНИСЕФ. Положение детей в мире, 2017 год: дети в цифровом мире. – С. 40 [Электронный ресурс]. – Режим доступа: <https://www.unicef.org> (дата обращения: 02.07.2023).

---

**Ляхова Елена Георгиевна** – канд. пед. наук, доцент, доцент ФГАОУ ВО «Российской университет транспорта», Россия, Москва.

*Глаголев Александр Борисович* – старший преподаватель ФГАОУ ВО «Российской университет транспорта», Россия, Москва.

*Душина Ирина Владимировна* – старший преподаватель ФГАОУ ВО «Российской университет транспорта», Россия, Москва.

---