Вестник Тамбовского университета. Серия: Гуманитарные науки
2022. Т. 27. № 4 http://journals.tsutmb.ru/humanities/
Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki = Tambov University Review. Series: Humanities
2022, vol. 27, no. 4 http://journals.tsutmb.ru/humanities-eng/
ISSN 1810-0201 (Print) ISSN 2782-5825 (Online)

Перечень ВАК, РИНЦ, Ulrich's Periodicals Directory, EBSCO, SciLIT, CrossRef

Научная статья
УДК 378.147+811.111+004
DOI 10.20310/1810-0201-2022-27-4-1009-1019

Обеспечение информационной безопасности студентов в процессе использования проектной методики в обучении иностранному языку в университете

Илона Алексеевна ЕВСТИГНЕЕВА, Максим Николаевич ЕВСТИГНЕЕВ, Виталий Владимирович КЛОЧИХИН*
ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина»
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33
*Адрес для переписки: cta124@yandex.ru

Аннотация. В современных условиях глобализации происходит всеобщая информатизация во всех сферах жизнедеятельности общества. Информатизация процесса обучения стала доминирующим направлением в модернизации отечественной системы высшего образования. Внедрение новых информационно-коммуникационных технологий в образовательный процесс приводит к возникновению совершенно новых видов информационных угроз и рисков, игнорирование которых ведет к дестабилизации процесса обучения и нарушению психического и физического здоровья обучающихся. В этой связи обеспечение информационной безопасности является одним из основных условий эффективного образовательного процесса. Обеспечение информационной безопасности основывается на определении реальных и потенциальных угроз в информационном пространстве. Дана классификация основных видов информационных угроз. Выявленные угрозы, в совокупности с положениями нормативных документов Российской Федерации, предусматривают формирование компетенции преподавателя в области обеспечения информационной безопасности. Выявлены содержательные аспекты компетенции, которые отражают особенности актуальных на каждом этапе обучения информационных угроз и рисков. На основе содержательных аспектов компетенции сформулированы рекомендации для преподавателей и обучающихся по обе с-печению информационной безопасности в рамках процесса обучения иностранному языку .

Ключевые слова: информационная безопасность, информатизация образования, сетевое обучение, компетенция преподавателя, угрозы информационной безопасности

Для цитирования: *Евстигнеева И.А., Евстигнеев М.Н., Клочихин В.В.* Обеспечение информационной безопасности студентов в процессе использования проектной методики в обучении иностранному языку в университете // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2022. Т. 27, № 4. С. 1009-1019. https://doi.org/10.20310/1810-0201-2022-27-4-1009-1019

Original article
DOI 10.20310/1810-0201-2022-27-4-1009-1019

Ensuring students' information security in the process of using the project method in foreign language teaching at the university

Ilona A. EVSTIGNEEVA, Maksim N. EVSTIGNEEV, Vitaliy V. KLOCHIKHIN*
Derzhavin Tambov State University
33 Internatsionalnaya St., Tambov 392000, Russian Federation
*Corresponding author: cta124@yandex.ru

Abstract. In contemporary conditions of globalization, there is a general informatization in all spheres of society. Informatization of the learning process has become the dominant direction in the modernization of the national system of higher education. The introduction of new information and communication technologies in the educational process leads to the emergence of completely new types of information threats and risks, ignoring which leads to destabilization of the learning process and students' mental and physical health disorders. In this regard, ensuring information security is one of the main conditions for an effective educational process. Ensuring information security is based on the identification of real and potential threats in the information space. The classification of the main types of information threats is given. The identified threats, in conjunction with the provisions of the regulatory documents of the Russian Federation, provide for the development of a teacher's competence in the field of information security. The content aspects of competence are revealed, which reflect the features of information threats and risks that are relevant at each stage of teaching. Based on the content aspects of competence, recommendations are formulated for teachers and students on ensuring information security as part of the process of foreign language teaching.

Keywords: information security, informatization of education, online learning, teacher competence, information security threats

For citation: Evstigneeva I.A., Evstigneev M.N., Klochikhin V.V. Obespecheniye informatsionnoy bezopasnosti studentov v protsesse ispol'zovaniya proyektnoy metodiki v obuchenii inostrannomu yazyku v universitete [Ensuring students' information security in the process of using the project method in foreign language teaching at the university]. *Vestnik Tambovskogo universiteta. Seriya: Gumanitarnye nauki – Tambov University Review. Series: Humanities*, 2022, vol. 27, no. 4, pp. 1009-1019. https://doi.org/10.20310/1810-0201-2022-27-4-1009-1019 (In Russian, Abstr. in Engl.)

АКТУАЛЬНОСТЬ

Наряду с транснациональной идеей глобализации современного общества единое информационное пространство для всех жителей земного шара становится реальностью. В таких условиях особая роль в обеспечении жизнедеятельности отводится знаниям и информации, а стабильность функционирования общества зависит от качества технологических и информационных решений. Вместе с тем этот процесс имеет двойственный характер: с одной стороны, развитие современного общества невозможно без глобальной информатизации, а с другой стороны, возрастает уровень информационного воздействия на социум.

Стремительное развитие цифровых интернет-технологий не могло не отразиться в

государственной политике в области образования. Так, в принятом Федеральном законе «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ[1], в образовательных учреждениях должны быть созданы условия для функционирования информационной образовательной среды. Цифровизация образовательного процесса стала одним из доминирующих направлений совершенствования российской системы образования, направленного на разработку новых методических систем, технологий, методов и средств обучения в современном информационном обществе. В совокупности с внедрением компетентностого подхода в отечественном образовании, направленного на практическое применение полученных знаний, умений и навыков, заставили методистов по новому воспринять роль обучающихся в образовательном процессе, в рамках которого обучающиеся выступают в качестве активного участника поиска и отбора информации для последующего ее практического применения. Таким образом, информатизация образования затрагивает весь процесс обучения, от цифровизации образовательных учреждений и разработки специального программного обеспечения до приобретения студентами новых компетенций в информационной сфере. Под информатизацией образования в широком понимании этого термина понимается «целенаправленно организованный процесс обеспечения сферы образования методологией, технологией и практикой создания и оптимального использования научно-педагогических, учебно-методических разработок, ориентированных на реализацию возможностей средств информационных и коммуникационных технологий (ИКТ), применяемых в комфортных и здоровьесберегающих условиях» [1, с. 106].

В контексте лингвистического образования информатизация образования осуществляется в основном в похожих с другими направлениями подготовки условиях. Однако обучение иностранному языку имеет свою специфику, особенности которой должны отражаться в основных положениях информатизации лингвистического образования. В этой связи под информатизацией лингвистического образования понимается «комплекс мер по обеспечению всего процесса обучения и овладения иностранным языком и культурой страны изучаемого языка методологией, технологиями разработки новых учебных и учебно-методических материалов, методиками использования новых информационных и коммуникационных технологий в обучении, подготовкой и переподготовкой педагогических кадров, способных широко использовать потенциал информационных технологий на практике в здоровьесберегающих условиях» [2, с. 4].

Информатизация общества в целом и внедрение новых информационно-коммуникационных технологий во все сферы жизнедеятельности общества в частном приводят к возникновению совершенно новых видов угроз и рисков здоровой жизнедеятельности личности, связанных с фальсификацией информации, искажением реальности, разрушением личностных ценностей и образа жизни, манипулированием сознанием, развязыванием информационных войн. В подобных условиях современная личность теряет свою идентичность, размываются ценностные ориентиры. В этой связи приобретают актуальность вопросы обеспечения информационной безопасности личности субъекта образовательного процесса.

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ

Ключевым понятием в данном исследовании является «информационная безопасность». Стоит отметить, что термин «информационная безопасность» видоизменялся по мере появления и развития информационных технологий. Если в середине XX веке информационная безопасность отождествлялась с безопасным хранением и передачей секретной государственной информации, то уже в конце XX века наравне с бурным развитием информационно-коммуникационных

[1] Об образовании в Российской Федерации: федеральный закон от 29.12.2012 № 273-ФЗ. Доступ из СПС «КонсультантПлюс».

технологий понятие «информационная безопасность» претерпело серьезные изменения для более точного описания данной проблемы в условиях информатизации общества. В настоящее время сам концепт информационной безопасности многогранен и в научной литературе рассматривается с разных точек зрения – технологической, политической, социальной и педагогической.

В основу технологического подхода к определению понятия «информационная безопасность», прежде всего, заложены положения об обеспечении безопасности функционирования информационных систем, лицензировании и сертификации интернет-ресурсов, использовании криптографических механизмов для передачи информации и т. п. По определению В.Н. Ясенева, информационная безопасность подразумевает «защиту информации от внесения в нее изменений неуполномоченными лицами; сохранность ценных данных; надежность работы компьютера; сохранение тайны переписки в электронной связи» [3, с. 146]. Схожее по содержанию определение встречается в работе А.Н. Асаул – «совокупность средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа» [4, с. 74]. Приведенные определения отражают сущность информационной безопасности, с точки зрения технологического подхода – это защита информационной инфраструктуры. Однако данный подход к определению понятия «информационная безопасность» является ограниченным, поскольку не учитывает наличие не менее важных субъектов информационных отношений, таких как личность, общество, государство.

В нормативных документах Российской Федерации под информационной безопасностью подразумевается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина»[2]. Информационная безопасность является одним из компонентов национальной безопасности Российской Федерации, что предполагает защиту национальных интересов в информационной сфере. Одним из таких интересов, согласно Доктрине информационной безопасности Российской Федерации, являются «интересы личности в информационной сфере, заключающиеся в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность»[3]. Таким образом, реализация прав и свобод личности в информационной сфере признается одной из составляющих информационной безопасности России.

Многие ученые в своих исследованиях отмечали, что информационная безопасность является не только техническим явлением, но также обладает социальным характеристиками [5; 6]. Данное понятие невозможно рассматривать только в рамках использования технических средств и технологий по защите информации. Информационная безопасность является комплексным понятием, и ее обеспечение тесно связано с социальными явлениями. В своем исследовании С.А. Матяш отмечает, что именно на общество ложится роль в обеспечении информационной безопасности личности и государства «от воздействия на них особого вида угроз, выступающих в форме организованных либо стихийно возникающих информационных потоков, осуществляемых в интересах регрессивных, реакционных или экстремистски настроенных политических и социальных сил, и направленных на осознанную деформацию общественного и индивидуального сознания» [6, с. 72]. Похожей точки зрения придерживается Л.И. Шершнев, указывая на то, что вопросы обеспечения информацион-

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. С. 1. URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (дата обращения: 16.03.2022).

[3] Там же. С. 4.

ной безопасности – это способность государства, общества и социальной группы «обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания жизнедеятельности, устойчивого функционирования и развития, противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей» [7, с. 50]. В приведенном определении также указывается на невозможность обеспечения абсолютной информационной безопасности, так как всегда, в условиях взаимодействия в информационной среде, будут существовать остаточные риски.

Другая группа ученых, наоборот, указывает на ведущую роль личности в обеспечении информационной безопасности и связывает с умениями самостоятельного выявления и идентифицирования угроз информационного воздействия и умениями преодоления негативных последствий информационного воздействия [8]. В данном случае обеспечение информационной безопасности зависит от умений и навыков обучающегося распознать и нивелировать информационную опас-ность.

С педагогической точки зрения И.В. Роберт рассматривает информационную безопасность личности субъекта образовательного процесса как совокупность условий, при которых внешняя информационная среда, и в том числе информационно-коммуникационные технологии не оказывают негативного влияния на физическое и психическое здоровье обучающихся [9]. В свою очередь, П.В. Сысоев рассматривает обеспечение информационной безопасности как вид деятельности, при этом акцентируя внимание на том, что данная деятельность должна затрагивать всех участников образовательного процесса: обучающихся, преподавателей и родителей. Целью обеспечения информационной безопасности выступает «предотвращение утечки личной информации и несанкционированного, преднамеренного или непреднамеренного воздействия на личность обучающегося со стороны третьих лиц, ведущего к моральному или материальному ущербу» [10, с. 17].

Анализ приведенных определений термина «информационная безопасность» показывает, что защита личности от негативного информационного воздействия является одной из первостепенных задач государства, социума и самой личности, решение которой заключается в создании оптимальных условий для деятельности в информационной среде. В образовательном процессе результативное обеспечение информационной безопасности ведет как к повышению эффективности самого процесса обучения, так и сохранения физического и психического здоровья обучающихся. Обеспечение информационной безопасности является не единовременной мерой, а продолжающимися постоянными действиями всех участников образовательного процесса.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для обеспечения результативной комплексной информационной безопасности, в первую очередь, следует отметить негативные факторы, представляющие угрозу образовательному процессу. Фактором риска является наличие следующих компонентов в образовательной среде: а) несанкционированного доступа к персональным данным и их разглашение; б) противозаконного контента, направленного на разрушение ценностных ориентиров и замедление нравственного развития обучающихся; в) цифровых элементов, преднамеренно созданных с целью нарушения психофизиологического состояния обучающихся; г) манипулятивного контента, направленного на ограничение возможностей и дезориентацию обучающихся в цифровом пространстве.

Обеспечение информационной безопасности обучающихся, прежде всего, основывается на выявлении и сдерживании реальных и потенциальных рисков и угроз в сфере информационного пространства. Наравне с интенсивным развитием цифровых технологий уровень и спектр рисков и угроз в информационной образовательной среде многократно возрос. В сфере обеспечения ин-

формационной безопасности одним из центральных понятий является понятие угрозы. В соответствии с Доктриной информационной безопасности Российской Федерации угрозой является «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»[4], то есть угрозой информационной безопасности являются факторы, сдерживающие реализацию прав и свобод личности в информационной сфере. Угрозы информационной безопасности могут быть классифицированы по следующим признакам:

а) по аспектам информационной безопасности:

– *угрозы конфиденциальности информации* возникают в том случае, если информация становится доступной лицам, не располагающим правомерными полномочиями к представляемой информации (персональные данные, интеллектуальная собственность, телефонные разговоры и т. п.);

– *угрозы доступности информации* возникают в тех случаях, когда действия направлены на запрет или на затруднение доступа к информационным ресурсам;

– *угрозы целостности информации* возникают в случаях несанкционированного изменения данных в информационных системах;

б) по расположению источника угроз:

– *внутренние* (причина информационной угрозы располагается внутри системы);

– *внешние* (причина информационной угрозы располагается вне системы);

в) по характеру воздействия на информационные ресурсы:

– *активные* (устройство и содержание информационной системы не претерпевают изменений);

– *пассивные* (устройство и содержание информационной системы претерпевают изменения);

г) по уровню угроз:

– *низкий* (незначительные негативные последствия);

– *средний* (негативные последствия);

– *высокий* (существенные негативные последствия);

– *критический* (причинение значительного вреда здоровью, потеря жизни);

д) по природе возникновения:

– *естественные* (угрозы вызваны непреднамеренным воздействием на информационную систему физических явлений или природных процессов);

– *искусственные* (угрозы вызваны умышленной деятельностью человека).

Вид образовательной деятельности обучающихся в рамках сетевого обучения является обусловливающим фактором определения типа информационных угроз, воздействию которых обучающийся наиболее подвержен, и следовательно, определяются пути защиты. Следует отметить, что связи между участниками информационного образовательного процесса также находятся под угрозой негативного информационного воздействия. Поскольку в рамках информационного образовательного процесса происходит взаимодействие всех его участников, то информационное воздействие можно рассматривать как угрозу всему процессу обучения, достижения его целей и задач. В этой связи выделяются четыре основных этапа оценки информационных рисков: 1) «инвентаризация информационных ресурсов, включенных в сферу оценки; 2) идентификация угроз, связанных этими ресурсами; 3) распределение по степени вероятности и потенциальным последствиям реализации угроз для субъектов сетевого обучения и их связей; 4) определение средств контроля для снижения уровня предполагаемых угроз или полной их ликвидации» [11, с. 47]. Специфика обеспечения информационной безопасности заключается в том, что наравне с изучением организационных, правовых и технологических аспектов информационной защиты следует также воспитывать в обучающихся нравственное и ответственное поведение при взаимодействии с информационными ресур-

[4] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. С. 1. URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (дата обращения: 16.03.2022).

сами, при неправильном использовании которых обучающиеся могут причинить материальный и физический вред не только себе, но и другим участникам сетевого образовательного процесса. Противодействием негативным проявлениям информационной среды должно стать формирование ответственной формы сетевого поведения обучающихся.

КОМПЕТЕНЦИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализ угроз и рисков взаимодействия обучающихся в информационном пространстве, а также положения Доктрины информационной безопасности Российской Федерации предусматривают формирование и развитие компетенции педагогических кадров в сфере обеспечения информационной безопасности при применении средств информационно-коммуникационных технологий. Содержание компетенции в области обеспечения информационной безопасности должно определяться в связи с актуальным составом информационных угроз.

Владение основами обеспечения информационной безопасности является одним из основных компонентов ИКТ компетенции преподавателя [12]. Подготовка преподавателей в сфере обеспечения информационной безопасности рассматривается как научное направление и практическая деятельность, направленные на разработку методики, средств и содержания подготовки педагогических кадров любой специальности, работающих в условиях современной информационной среды, владеющих содержательными аспектами информационной безопасности, а также практическими навыкам предотвращения негативного воздействия информации в рамках сетевого обучения.

В основу формирования и развития информационной безопасности личности субъектов образовательного процесса должны быть положены следующие принципы защиты обучающихся: а) защита от внешней агрессивной информации; б) защита от неэтичной информации или информации, нарушающей морально-нравственные ценности обучающихся; в) защита обучающихся от педагогических материалов, реализованных на основе информационно-коммуникационных технологий, не отвечающих педагогико-эргономическим требованиям; г) защита от заимствования авторской интеллектуальной собственности, хранящейся в информационной среде; д) защита физического и психического здоровья обучающихся от негативного воздействия процесса пользования информационно-коммуникационных технологий в рамках сетевого обучения [9].

Содержательные аспекты подготовки преподавателей к обеспечению информационной безопасности должны быть направлены на реализацию эффективного образовательного процесса в рамках сетевого обучения при использовании информационно-коммуникационных технологий и отражать специфику основных проблем в обеспечении информационной безопасности.

На современном этапе развития информационной среды наряду с внедрением технологий метавселенной сознание обучающихся все дальше углубляется в виртуальное пространство. В этой связи выделяются *философские аспекты содержания* компетенции преподавателя в области обеспечения информационной безопасности, направленные, в первую очередь, на развитие представления обучающегося об обманчивой природе виртуального мира, состоящего из вымышленных, искаженных изображений реальности, влекущих к «виртуализации» сознания и отлучения от реальной жизни. А также обращаются к способностям критического мышления обучающихся применительно к информации, добытой из Интернета, интерпретации личности партнера по сетевому общению.

Деятельностный компонент в рамках философских аспектов содержания компетенции в области обеспечения информационной безопасности обучающихся включает:

– выявление и описание признаков «виртуального мира», раскрытие отличительных деталей от реального мира;

– выявление характеристик объектов в виртуальной среде, определение их свойств, связей и процессов их деятельности;

– прекращение общения с сетевым партнером, который умышленно скрывает свою истинную личность.

Глобальное использование новых информационно-коммуникационных технологий в образовательной сфере выдвинуло на передний план проблему нравственных ценностей обучающихся. Как показывает история, внедрение выдающихся технологических достижений, происходящее без соответствующего развития культуры и этики общества, приводит к трагичным последствиям. В этой связи выделяются *этические аспекты содержания* компетенции специалистов в области обеспечения информационной безопасности. В настоящее время в информационной среде существует безграничное количество интернет-сообществ, влиянию которых подвержены обучающиеся. Зачастую контент в таких сетевых сообществах наполнен деструктивной информацией, ориентированной на побуждение к совершению противоправных действий в соответствии с законодательством Российской Федерации, а также информацией, нарушающей моральные ценности обучающихся. Вместе с тем этический аспект компетенции касается вопросов заимствования интеллектуальной собственности, особенно актуальный на этапе проведения научно-исследовательской деятельности обучающихся. Проблемы использования нелегитимной педагогической продукции на основе информационно-коммуникационных технологий, применяемых в процессе сетевого обучения, также входят в состав этического компонента.

Деятельностный компонент в рамках этических аспектов содержания компетенции в области обеспечения информационной безопасности обучающихся включает:

– селекцию агрессивно направленной информации (по ключевым словам, словосочетаниям и т. д.);

– обнаружение противоправной информации, идущей в разрез с законодательством РФ;

– выявление информации, оскорбляющей нравственные ценности обучающихся;

– отбор педагогического контента на базе информационно-коммуникационных технологий, не соответствующего педагогико-эргономическим требованиям;

– выявление информации, в которой содержатся результаты заимствования интеллектуальной собственности.

В условиях сетевого обучения и нахождения в виртуальном пространстве, в рамках *технологического аспекта содержания* компетенции в области информационной безопасности обучающийся должен знать особенности используемых им цифровых средств как объекта и предмета информационной защиты. При этом стоит обратить внимание на роль «человеческого фактора» в обеспечении информационной безопасности, а также иметь представление о существующей угрозе для информационных ресурсов в сферах человеческой деятельности.

Деятельностный компонент в рамках технологического аспекта содержания компетенции в области обеспечения информационной безопасности обучающихся должен включать:

– осуществление сетевого взаимодействия между обучающимся и интерактивными информационно-коммуникационными технологиями;

– визуализацию информации о сетевых образах или цифровых графических интерпретаций;

– интерпретацию сетевых образов в текстовый формат;

– использование программного обеспечения, представляющего сетевые визуальные образы.

В современных условиях обучения иностранному языку с использованием информационно-коммуникационных технологий одной из задач преподавателя становится обеспечение информационной безопасности всего цикла образовательного процесса. Содержание компетенции преподавателя в области обеспечения информационной безопасности должно отражать особенности ак-

туальных на каждом этапе обучения информационных угроз и рисков.

На основе содержательных аспектов компетенции в области обеспечения информационной безопасности следует сформулировать рекомендации для преподавателей и обучающихся по обеспечению информационной безопасности в рамках сетевого обучения.

РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ СЕТЕВОГО ОБУЧЕНИЯ

Разъясните обучающимся список разрешенных и доступных веб-сайтов для выполнения заданий в рамках сетевого обучения;

– объясните правила корректного заимствования интеллектуальной собственности других пользователей сети Интернет;

– объясните обучающимся, что ***нельзя*** скачивать и открывать стороннее программное обеспечение, которое может содержать вирусные программы, открывать письма и вступать в переписку с незнакомыми пользователями, разглашать свои личные данные, сведения о родственниках и близких людях (имена, даты рождения, место жительства, паспортные данные и т. п.);

– зарегистрируйтесь на выбранном для сетевого обучения интернет-ресурсе в качестве модератора и осуществляйте полный контроль над взаимодействием обучающихся;

– разъясните обучающимся правила регистрации пользователей на интернет-ресурсе, чтобы логин и пароль не выдавали персональные данные;

– предложите обучающимся выбрать в качестве своего цифрового обозначения никнейм (вымышленное имя пользователя) для скрытия настоящего имени;

– объясните обучающимся, что логин и пароль являются персональными данными и не должны быть разглашены;

– в процессе сетевого обучения используйте интернет-ресурсы, функции которых позволяют ограничить доступ пользователей;

– стимулируйте обучающихся делиться опытом и давать фидбек взаимодействия в рамках сетевого обучения.

РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ СЕТЕВОГО ОБУЧЕНИЯ

Не используйте свои персональные данные (имя, фамилия, адрес) в процессе сетевого обучения;

– никому не разглашайте свой логин и пароль от учетных записей в сети Интернет;

– для взаимодействия в сетевом пространстве используйте никнейм (вымышленное имя);

– не вступайте в коммуникацию с незнакомыми пользователями, если вам написали первому, уведомите преподавателя;

– не выдавайте незнакомыми пользователям информацию личного характера, не отправляйте им свои фотографии и видеозаписи;

– не загружайте стороннее программное обеспечение (скорее всего, в нем содержатся вирусные программы), не открывайте письма от незнакомых пользователей;

– если у вас возникли сомнения или вопросы, обратитесь к преподавателю.

Информационная безопасность является ключевым элементом, защищающим участников образовательного процесса от негативного влияния информационной среды. Она не должна быть только ограничена техническим и организационным контролем сетевых ресурсов и программного обеспечения, а также ее следует рассматривать в качестве научного направления и практической деятельности по защите субъектов информационной образовательной среды. Вопросы обеспечения информационной безопасности обучающихся должны выделяться и учитываться на каждом этапе процесса обучения с использованием средств информационно-коммуникационных технологий. Поэтому формирование компетенции в области обеспечения информационной безопасности долж-

но являться одной из основных составляющих подготовки современного преподавателя.

Проблема информационной безопасности в перспективе ближайших десятилетий не только не потеряет своей актуальности, но и приобретет еще большую значимость, поскольку развитие и внедрение новых информационно-коммуникационных технологий в сферу лингвистического образования будет только возрастать.

Список источников

1. *Роберт И.В.* Основные направления информатизации образования в отечественной школе // Вестник МГПУ. Серия: Информатика и информатизация образования. 2005. № 5. С. 106-114.
2. *Сысоев П.В.* Информатизация языкового образования: основные направления и перспективы // Иностранные языки в школе. 2012. № 2. С. 2-9.
3. *Ясенев В.Н.* Информационная безопасность в экономических системах. Н. Новгород: ННГУ, 2006. 253 с.
4. *Асаул А.Н.* Организация предпринимательской деятельности. СПб.: АНО ИПЭВ, 2009. 257 с.
5. *Бочаров М.И.* Сетевые сообщества и информационная безопасность в непрерывном образовании средней общеобразовательной и профессиональной школы // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2009. № 4. С. 20-27.
6. *Матяш С.А.* Информационная безопасность личности в современных условиях // Энергия: экономика, техника, экология. 2013. № 8. С. 71-77.
7. *Шершнев Л.И.* Информационная безопасность России // Безопасность. 1993. № 11-12. С. 49-53.
8. *Малых Т.А.* Педагогические условия развития информационной безопасности младшего школьника: автореф. дис. ... канд. пед. наук. Иркутск, 2008. 22 с.
9. *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: сб. науч. тр. М., 2021. С. 151-170.
10. *Сысоев П.В.* Информационная безопасность учащихся при работе в образовательной интернет-среде: современный ответ на вызовы времени // Иностранные языки в школе. 2011. № 10. С. 20-24.
11. *Козлов О.А., Гузикова Л.А.* Информационная безопасность как условие деятельности образовательных организаций // Вопросы методики преподавания в вузе. 2017. Т. 6. № 22. С. 43-50. https://doi.org/10.18720/HUM/ISSN 2227-8591.22.6
12. *Евстигнеев М.Н.* Компетентность учителя иностранного языка в области использования информационно-коммуникационных технологий // Иностранные языки в школе. 2011. № 9. С. 3-9.

References

1. Robert I.V. Osnovnyye napravleniya informatizatsii obrazovaniya v otechestvennoy shkole [The main directions of informatization of education in the national school]. *Vestnik MGPU. Seriya: Informatika i informatizatsiya obrazovaniya – MCU Journal of Informatics and Informatization of Education*, 2005, no. 5, pp. 106-114. (In Russian).
2. Sysoyev P.V. Informatizatsiya yazykovogo obrazovaniya: osnovnyye napravleniya i perspektivy [Informatization of language education: main directions and prospects]. *Inostrannyye yazyki v shkole – Foreign Languages at School*, 2012, no. 2, pp. 2-9. (In Russian).
3. Yasenev V.N. *Informatsionnaya bezopasnost' v ekonomicheskikh sistemakh* [Information Security in Economic Systems]. Nizhniy Novgorod, National Research Lobachevsky State University of Nizhny Novgorod Publ., 2006, 253 p. (In Russian).
4. Asaul A.N. *Organizatsiya predprinimatel'skoy deyatel'nosti* [Organization of Entrepreneurial Activity]. St. Petersburg, Institute for Economic Revival Problems Publ., 2009, 257 p. (In Russian).
5. Bocharov M.I. Setevyye soobshchestva i informatsionnaya bezopasnost' v nepreryvnom obrazovanii sredney obshcheobrazovatel'noy i professional'noy shkoly [Network communities and information security in lifelong education of secondary general education and vocational schools]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Informatizatsiya obrazovaniya – RUDN Journal of Informatization in Education*, 2009, no. 4, pp. 20-27. (In Russian).

6. Matyash S.A. Informatsionnaya bezopasnost' lichnosti v sovremennykh usloviyakh [Information security of the individual in modern conditions]. *Energiya: ekonomika, tekhnika, ekologiya* [Energy: Economics, Technology, Ecology], 2013, no. 8, pp. 71-77. (In Russian).
7. Shershnev L.I. Informatsionnaya bezopasnost' Rossii [Information security of Russia]. *Bezopasnost'* [Security], 1993, no. 11-12, pp. 49-53. (In Russian).
8. Malykh T.A. *Pedagogicheskiye usloviya razvitiya informatsionnoy bezopasnosti mladshego shkol'nika: avtoref. diss. ... kand. ped. nauk* [Pedagogical Conditions for the Development of Information Security of a Junior School Student. Cand. ped. sci. diss. abstr.]. Irkutsk, 2008, 22 p. (In Russian).
9. Robert I.V. Podgotovka pedagogicheskikh kadrov v oblasti informatsionnoy bezopasnosti lichnosti v usloviyakh tsifrovoy transformatsii obrazovaniya [Training of pedagogical staff in the field of information security of the individual in the conditions of digital transformation of education]. *Informatsionnaya bezopasnost' lichnosti sub"yektov obrazovatel'nogo protsessa v tsifrovoy informatsionno-obrazovatel'noy srede* [Information Security of the Individual of the Subjects of the Educational Process in the Digital Information and Educational Environment]. Moscow, 2021, pp. 151-170. (In Russian).
10. Sysoyev P.V. Informatsionnaya bezopasnost' uchashchikhsya pri rabote v obrazovatel'noy internet-srede: sovremennyy otvet na vyzovy vremeni [Information security of students when working in the educational Internet environment: a modern response to the challenges of the time]. *Inostrannyye yazyki v shkole – Foreign Languages at School*, 2011, no. 10, pp. 20-24. (In Russian).
11. Kozlov O.A., Guzikova L.A. Informatsionnaya bezopasnost' kak usloviye deyatel'nosti obrazovatel'nykh organizatsiy [Information security as a condition for the activity of educational organizations]. *Voprosy metodiki prepodavaniya v vuze – Teaching Methodology in Higher Education*, 2017, no. 22, pp. 43-50. (In Russian).
12. Evstigneev M.N. Kompetentnost' uchitelya inostrannogo yazyka v oblasti ispol'zovaniya informatsionno-kommunikatsionnykh tekhnologiy [Competence of a foreign language teacher in the use of information and communication technologies]. *Inostrannyye yazyki v shkole – Foreign Languages at School*, 2011, no. 9, pp. 3-9. (In Russian).

Информация об авторах

Евстигнеева Илона Алексеевна, кандидат педагогических наук, доцент, доцент кафедры лингвистики и лингводидактики, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, ORCID: 0000-0002-1198-0695, ilona.frolkina@mail.ru

Евстигнеев Максим Николаевич, кандидат педагогических наук, доцент, доцент кафедры лингвистики и лингводидактики, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, ORCID: 0000-0003-2664-9134, maxim-evstigneev88@mail.ru

Клочихин Виталий Владимирович, ассистент кафедры лингвистики и лингводидактики, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, ORCID: 0000-0003-4845-6624, cta124@yandex.ru

Информация о конфликте интересов: авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 13.04.2022
Одобрена после рецензирования 06.07.2022
Принята к публикации 09.09.2022

Information about the authors

Ilona A. Evstigneeva, Candidate of Pedagogy, Associate Professor, Associate Professor of Linguistics and Linguodidactics Department, Derzhavin Tambov State University, Tambov, Russian Federation, ORCID: 0000-0002-1198-0695, ilona.frolkina@mail.ru

Maxim N. Evstigneev, Candidate of Pedagogy, Associate Professor, Associate Professor of Linguistics and Linguodidactics Department, Derzhavin Tambov State University, Tambov, Russian Federation, ORCID: 0000-0003-2664-9134, maxim-evstigneev88@mail.ru

Vitaliy V. Klochikhin, Assistant of Linguistics and Linguodidactics Department, Derzhavin Tambov State University, Tambov, Russian Federation, ORCID: 0000-0003-4845-6624, cta124@yandex.ru

Information on the conflict of interests: authors declare no conflict of interests.

The article was submitted 13.04.2022
Approved after reviewing 06.07.2022
Accepted for publication 09.09.2022