УДК 378.147.88; 004.77
DOI: http://dx.doi.org/10.21686/1818-4243-2019-6-22-29

Д.С. Карпов, А.А. Микрюков, П.А. Козырев

Российский экономический университет имени Г.В. Плеханова, Москва, Россия

Повышение качества подготовки специалистов по направлению подготовки «Информационная безопасность»

Цель исследования. *Целью исследования является обоснование и разработка подхода к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность», на основе повышения качества усвоения учебного материала дисциплин, предусмотренных учебным планом.*

Материалы и методы. *Для достижения поставленной цели предлагается использовать инновационные методы обучения, основанные на применении современных интерактивных образовательных технологий.*

Проведенное исследование основано на анализе и использовании материалов исследований в области применения педагогических технологий в современном образовательном процессе, требований законодательства, обязательных при реализации основных образовательных программ высшего профессионального образования. При подготовке статьи также использовались материалы, полученные авторами в ходе планирования, подготовки, проведения и анализа лабораторных занятий со студентами, обучающимися по направлению подготовки «Информационная безопасность».

Результаты. *Специфика подготовки специалистов по направлению подготовки «Информационная безопасность», обусловленная предъявляемыми к ним высокими требованиями со стороны работодателей, а также сложностью и необходимостью решения проблем, стоящих перед Российской Федерацией в области обеспечения информационной безопасности, заключается в необходимости в получении ими, наряду с фундаментальными знаниями в области информационной безопасности, знаний современных и перспективных технологий защиты информации. Важную роль в повышении качества подготовки специалистов высокой квалификации, профессионально востребованных и способных к саморазвитию в настоящее время играет применение новых подходов к их обучению, основанных на использовании инновационных методов.*

Предложенный подход заключается в освоении обучающимися современных и перспективных технологий защиты информации с применением в ходе организации, подготовки и проведения учебных занятий инновационных методов обучения.

Одной из основных, наиболее важных в практическом, науч- но-исследовательском аспекте, форм проведения занятий в процессе подготовки специалистов по информационной безопасности является лабораторный практикум.

Предложенный подход был апробирован в учебном процессе при планировании, подготовке и проведении лабораторной работы по теме «Создание виртуальной частной сети в виртуальной среде» по дисциплине «Технология обеспечения информационной безопасности». К основным особенностям этого занятия относятся актуальность, наукоемкость и практическая направленность темы занятия, а также его интерактивность.

Результатом применения предложенного подхода стало повышение степени усвоения, широты охвата изучаемого материала и, в итоге, повышение эффективности формирования у обучающихся компетенций, предусмотренных учебным планом.

Заключение. *В результате проведенных исследований был обоснован и разработан подход к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность».*

Предложенный подход, заключающийся в применении инновационных интерактивных методов обучения в ходе организации, подготовки и проведения учебных занятий по актуальным, наукоемким темам, имеющим прикладное значение, был реализован на практике при освоении обучающимися материала дисциплины «Технология обеспечения информационной безопасности», что позволило повысить качество усвоения учебного материала дисциплины и, в конечном итоге, повысить качество подготовки специалистов по направлению подготовки «Информационная безопасность».

Ключевые слова: *информационная безопасность, защита информации, инновационный метод, интерактивный подход, виртуализация, VPN*

Dmitry S. Karpov, Andrey A. Mikryukov, Peter A. Kozyrev

Plekhanov Russian University of Economics, Moscow, Russia

Improving the quality of learning of specialists in the field of learning “Information security”

Purpose of the study. *The aim of the study is to substantiate and develop an approach to improving the quality of training of specialists in the direction of training “Information Security”, based on improving the quality of assimilation of the educational material of the disciplines provided for by the curriculum.*

Materials and methods. *To achieve this goal, it is proposed to use innovative teaching methods based on the use of modern interactive educational technologies.*

The study is based on the analysis and use of research materials in the field of the application of pedagogical technologies in the modern educational process, the requirements of the law, which are mandatory when implementing the main educational programs of higher profes- sional education. In preparing the article, the materials obtained by the authors during the planning, preparation, conduct and analysis of laboratory studies with students studying in the direction of training “Information Security” were also used.

Results. *The specifics of training specialists in the direction of training “Information Security”, due to the high demands placed on them by employers, as well as the complexity and necessity of solving the problems facing the Russian Federation in the field of ensuring information security, lies in the need for them to obtain, along with fundamental knowledge in the field of information se- curity, knowledge of modern and promising information protection technologies.*

An important role in improving the quality of training highly qualified specialists who are professionally in demand and capable of self-development is currently played by the application of new approaches to their training based on the use of innovative methods.
The proposed approach consists in the development by students of modern and promising information protection technologies using innovative teaching methods during the organization, preparation and conduct of training sessions.
One of the main, most important in practical, research aspects, forms of conducting classes in the process of training information security specialists is a laboratory workshop.
The proposed approach was tested in the educational process when planning, preparing and conducting laboratory work on the topic "Creating a virtual private network in a virtual environment" in the discipline "Information Security Technology". The main features of this lesson include the relevance, high technology and practical orientation of the topic of the lesson, as well as its interactivity.
The result of applying the proposed approach was an increase in the degree of assimilation, the breadth of coverage of the studied material and, as a result, an increase in the effectiveness of the formation of students' competencies provided for in the curriculum.
***Conclusion.** As a result of the research, an approach to improving the quality of training of specialists in the field of training "Information Security" was substantiated and developed.*
The proposed approach, which consists in the application of innovative interactive teaching methods during the organization, preparation and conduct of training on relevant, high-tech topics of applied importance, was implemented in practice when students learn the discipline "Information Security Technology", which allowed to improve the quality of assimilation educational material of the discipline and, ultimately, to improve the quality of training of specialists in the direction of training "Information Security".

***Keywords:** Information security, innovative method, interactive approach, virtualization, VPN*

Введение

Современная система образования призвана обеспечить подготовку специалистов высокой квалификации, профессионально востребованных, способных к саморазвитию в условиях информационного общества.

В настоящее время в учебном процессе преимущественно используются традиционные образовательные технологии, ориентированные на усвоение обучающимися фундаментальных теоретических знаний, основанные на пассивном подходе к обучению, что не всегда приводит к наилучшему результату, заключающемуся в формировании у обучающихся необходимых для специалиста знаний, навыков и умений.

В связи с этим необходима модернизация образовательного процесса посредством разработки, внедрения и применения новых подходов к обучению, основанных на применении инновационных методов [1–6].

Основным направлением инноваций становится активизация работы обучающихся, повышение уровня их мотивации к полному и качественному освоению образовательных программ. Инновации в высшем образовании сегодня во многом связаны с применением интерактивных методов обучения. Так при подготовке бакалавров требуется не менее 20%, а при подготовке магистров не менее 40% аудиторных занятий планировать и проводить в интерактивной форме.

Задача внедрения инноваций в учебный процесс является особенно актуальной при подготовке специалистов по направлению подготовки «Информационная безопасность», являющемуся одним из наукоемких направлений подготовки, требующим от обучающихся изучения новых информационных технологий, основанных на современных достижениях науки и техники [7–10].

Инновационный характер учебному занятию придают применяемые в ходе организации и проведения лабораторной работы современные интерактивные образовательные технологии.

Для повышения качества подготовки специалистов по направлению подготовки «Информационная безопасность» предлагается использовать подход, заключающийся в выборе для практических занятий актуальных, наукоемких тем, имеющих прикладное значение, а также в применении инновационных методов обучения в ходе организации, подготовки и проведения учебных занятий, в том числе лабораторных работ.

Подход к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность» и результаты его реализации

Важную роль в повышении качества подготовки специалистов по направлению подготовки «Информационная безопасность» играет изучение современных и перспективных технологий защиты информации с применением инновационных методов обучения.

Лежащая в основе Федеральных государственных образовательных стандартов 3-го поколения компетентностная модель образования предполагает смещение акцентов с использования традиционных образовательных технологий, ориентированных на усвоение фундаментальных теоретических знаний, основанных на пассивном подходе, к обучению на основе использования активного и интерактивного подходов, подразумевающих увеличение доли самостоятельной работы обучающихся. При этом под интерактивностью обучения следует понимать не только использование информационно-компьютерных технологий, но и взаимодействие в ходе обучения с преподавателем, лаборантом, другими обучающимися.

Одной из основных, наиболее важных в практическом

аспекте, форм проведения занятий в процессе подготовки обучающихся по направлению подготовки «Информационная безопасность» является лабораторный практикум. Наряду с другими видами аудиторной практической учебной работы, лабораторный практикум приобретает характер учеб- нонаучной исследовательской деятельности. Помимо практической отработки изучаемого материала на лабораторных занятиях обучающиеся развивают творческую инициативу, осуществляют активную познавательную деятельность, формируют профессиональные интересы.

При разработке рабочих программ и тематических планов изучения дисциплин, предусмотренных учебным планом подготовки специалистов по направлению подготовки «Информационная безопасность», необходимо акцентировать внимание на выборе наиболее актуальных, наукоемких тем учебных занятий, имеющих ярко выраженное прикладное значение. И особое значение это имеет при планировании лабораторных занятий.

Предложенный подход заключается в применении инновационных интерактивных методов обучения в ходе организации, подготовки и проведения учебных занятий по актуальным, наукоемким темам, имеющим прикладное значение.

Этот подход был реализован на практике в ходе планирования, подготовки и проведения лабораторной работы по теме «Создание виртуальной частной сети в виртуальной среде» по дисциплине «Технология обеспечения информационной безопасности», предусмотренной учебным планом подготовки обучающихся по направлению «Информационная безопасность».

В ходе лабораторной работы обучающиеся изучают технологии виртуализации, защиты среды виртуализации, а также технологии виртуальных защищенных сетей VPN.

Основными особенностями этого занятия являются актуальность, наукоемкость и практическая направленность темы занятия, а также его интерактивность.

Актуальность темы занятия обусловлена необходимостью знания будущими специалистами требований и рекомендаций о защите информации, содержащейся в государственных, муниципальных информационных системах, а также в автоматизированных системах в защищенном исполнении, сформулированных в нормативных правовых актах, нормативно-методических документах и в документах нормативно-технического характера, и обладания необходимыми компетенциями для их выполнения.

Так, в [11] отмечается, что «Обеспечение безопасности персональных данных достигается … применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных». В [12] установлены следующие требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных: «В соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы... Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах».

В [13] приведен состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, в который, в частности, входят: «идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; защита среды виртуализации; защита технических средств».

В [14] отмечено, что «Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям».

В [15] сформулирован состав организационных и технических мер защиты информации, реализуемых в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной си-

стемы, в том числе для защиты среды виртуализации.

В [16] сформулированы общие требования к защите информации в автоматизированных системах от утечки по техническим каналам, несанкционированного доступа, преднамеренных и непреднамеренных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней.

«Для решения задач защиты информации в АСЗИ принимаются организационные и технические меры защиты информации в АСЗИ, направленные на нейтрализацию угроз безопасности информации в АСЗИ, которые, в частности, включают организационные и технические меры защиты от НСД к информации» такие, например, как [16]: «идентификацию и аутентификацию субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; обеспечение целостности информации; защиту среды виртуализации»; а также организационные и технические меры защиты каналов передачи информации, в частности, включающие: «использование выделенных каналов передачи информации; криптографическую защиту информации, передаваемой по каналам передачи информации; исключение возможности отрицания отправителем факта отправки информации; исключение возможности отрицания получателем факта получения информации; защиту беспроводных каналов передачи информации» [16].

При решении задач обеспечения защиты информации в автоматизированных системах широкое распространение находят VPN-технологии, применение которых предусмотрено законодательными и нормативными требованиями.

В [13] отмечается, что в случае, если каналы связи (например, локальной вычислительной сети объекта) проходит в пределах контролируемой зоны, мера защиты информации ЗИС.3 должна быть реализована путем установки на границе ЛВС VPN-шлюза и шифрования трафика, передаваемого вовне (за пределы охраняемой зоны). В случае же, когда нет уверенности, что каналы связи проходят по контролируемой территории (то есть имеется возможность подключиться к каналу связи и снять передаваемую информацию), то следует шифровать трафик, начиная с рабочей станции [17].

Мера защиты информации УПД.13 «Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети» может быть реализована путем организации удаленного доступа пользователей с использованием технологии VPN [13].

Мера защиты информации ИАФ.6 «Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)» может быть реализована путем обеспечения доступа внешним пользователям с использованием технологии VPN, что обеспечивает реализацию механизмов их идентификации и аутентификации [13].

По мере развития и совершенствования технологий виртуализации в информационных системах нового поколения необходимость и целесообразность реализации VPN-технологий будет только возрастать.

Наукоемкость темы занятия обусловлена рядом факторов.

Во-первых, проблемы, рассматриваемые в ходе занятия, относятся к «научно-техническим проблемам защиты информационных ресурсов, информационных систем и сетей связи», а именно «проблемам развития и применения средств криптографической и технической защиты информации, а также средств анализа и контроля защищенности объектов информатизации для обеспечения информационной безопасности Российской Федерации в условиях интеграции и конвергенции информационно-телекоммуникационных технологий, развития технологий интернета вещей, облачных вычислений, больших данных» [18]. Таким образом, решение вопросов, рассматриваемых в ходе занятия, можно отнести к приоритетным научным исследованиям в области обеспечения информационной безопасности Российской Федерации, наряду с другими перспективными направлениями исследований [19–20].

Во-вторых, при изучении темы требуется применение междисциплинарного подхода, заключающегося в использовании и интеграции знаний, полученных обучающимися в ходе освоения комплекса учебных дисциплин, таких как «Теория информации», «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации», «Безопасность вычислительных сетей», «Защищенные информационные системы», «Технология построения защищенных автоматизированных систем», «Программно-аппаратные средства защиты информации» и др.

Практическая направленность темы занятия обусловлена прежде всего тем, что обучающиеся в ходе занятия знакомятся и получают навыки работы с современными программными средствами защиты информации, которые будут ими реально использоваться в профессиональной деятельности.

Целью работы является ознакомление обучаемых с методами создания виртуальных

сред, реализующих различные виды соединений VPN и приобретение навыков работы в них.

Лабораторная работа посвящена решению следующих задач:

1) обзор протоколов создания VPN-соединений;

2) анализ существующих программных средств реализации VPN-сервера;

3) выбор программной базы для реализации VPN – соединения в виртуальной среде;

4) выбор операционных систем;

5) анализ и выбор средств виртуализации;

6) создание виртуальной среды;

7) создание виртуальной частной сети в виртуальной среде.

В ходе работы обучающиеся знакомятся и получают навыки работы с программными средствами создания виртуальной среды Virtual Box и VMware Workstation, создания виртуальной частной сети Open VPN с открытым исходным кодом.

Помимо этого, учитывая то, что VPN-решения используют шифрование и являются криптографическими средствами, в ходе занятия рассматриваются отечественные решения (С-Terra, Континент, ViPNet и др.), сертифицированные ФСБ России.

Интерактивность учебного занятия обеспечивается применением в ходе организации и проведения лабораторной работы следующих современных интерактивных образовательных технологий [1–6]:

1. Работа в команде. В ходе занятия осуществляется совместная целенаправленная деятельность обучающихся в малых группах (командах), основанная на сложении результатов индивидуальной работы членов группы с разделением полномочий и ответственности.

2. Анализ проблемных ситуаций. В ходе занятия осуществляется анализ реальных проблемных ситуаций, возникающих в ходе работы и поиск вариантов их решения с последующим выбором наилучшего из них.

3. Модульное обучение. Лабораторная работа является отдельным автономным учебным модулем, который впоследствии интегрируется с другими модулями курса дисциплины.

4. Контекстное обучение. В ходе организации, подготовки и проведения занятия у обучающихся повышается мотивация к усвоению знаний, основанная на осознании связей между конкретным знанием и его прикладным значением.

5. Развитие критического мышления. Образовательная деятельность в ходе занятия направлена на развитие у обучающихся критического, рефлексивного мышления с целью повышения эффективности получения и усвоения ими новых знаний.

6. Проблемное обучение. В ходе подготовки и проведения занятия перед обучающимися очерчиваются проблемы предметной области, на решение которых они должны обратить внимание, что стимулирует обучающихся к самостоятельному освоению знаний.

7. Опережающая самостоятельная работа. В ходе подготовки к занятию обучающиеся самостоятельно осваивают новый материал.

8. Междисциплинарное обучение. В ходе подготовки и проведения занятия обучающиеся используют знания, полученные ими в ходе изучения различных учебных дисциплин, интегрируя их для решения поставленной задачи.

9. Обучение на основе опыта. В ходе подготовки и проведения занятия обучающиеся используют собственный накопленный опыт, ассоциируя его с решаемой задачей, за счет чего активизируется их познавательная деятельность.

10. Использование информационно-коммуникационных технологий. В ходе подготовки и проведения занятия обучающиеся используют электронную информационно-образовательную среду для расширения доступа к образовательным ресурсам, обеспечения взаимодействия с преподавателем, включая контроль и мониторинг текущей работы обучающихся и полученных ими результатов.

Применяемые в ходе организации и проведения лабораторной работы по актуальной, наукоемкой теме, связанной с изучением комплекса перспективных технологий защиты информации, современные интерактивные образовательные технологии придают учебному занятию инновационный характер. Результатом применения предложенного подхода является повышение степени усвоения, широты охвата изучаемого материала и, в итоге, повышение эффективности формирования у обучающихся компетенций, предусмотренных учебным планом.

Заключение

Предложенный в статье подход, заключающийся в применении инновационных методов обучения в ходе организации, подготовки и проведения учебных занятий по актуальным, наукоемким темам, был реализован на практике при освоении обучающимися материала дисциплины «Технология обеспечения информационной безопасности».

Выбор для занятий актуальных, наукоемких тем, имеющих прикладное значение, применение в ходе занятий инновационных интерактивных методов обучения позволили повысить качество усвоения учебного материала дисциплины и, в конечном итоге, повысить качество подготовки специалистов по направлению подготовки «Информационная безопасность».

Литература

1. Веденеева О.А., Савва Л.И., Сайгушев Н.Я. Педагогические технологии в современном образовательном процессе. Учебное пособие. [Электрон. ресурс]. М.: Мир науки, 2016. Режим доступа: https://izd-mn.com/PDF/10UPNPMN16.pdf (Дата обращения: 09.11.19).

2. Сысоева Е. Ю. Инновационные методы обучения в профессиональном образовании // Балтийский гуманитарный журнал. 2018. Т. 7. № 1 (22). С. 299–301.

3. Сысоева Е. Ю. Интерактивные технологии обучения в системе повышения квалификации педагогов // В кн.: Образование и наука: современные тренды: коллективная монография. Гл. ред. О.Н. Широков. Чебоксары: ЦНС «Интерактив плюс», 2016. № 1. 216 с. С. 113–133.

4. Белякова Е.М., Прокопьев А.В. Инновационные методы обучения в образовании // Современные проблемы науки и образования. 2015. № 2 (часть 1).

5. Трофименко А.С. Инновационные методы обучения в высшем образовании [Электрон. ресурс] // Sci-article.ru. 2014. № 13. Режим доступа: http://sci-article.ru/stat.php?i=1408380616

6. Черкасов М.Н. Инновационные методы обучения студентов // Инновации в науке: Сб. ст. по матер. XIV междунар. науч.-практ. конф. Часть II. Новосибирск: СибАК, 2012.

7. Мовчан И.Н. Проблемы подготовки специалистов в области информационной безопасности // Открытое образование. 2013. № 5 (100). С. 78–80.

8. Анурьева Н.С. Современная система образования в области информационной безопасности в Российской Федерации // Вестник Тамбовского университета. Серия Гуманитарные науки. Тамбов. 2018. Т. 23. № 173. С. 111–120.

9. Астахова Л.В., Томилов А.А. Новые задачи подготовки кадров по защите информации в контексте «Доктрины информационной безопасности Российской Федерации» (2016) [Электрон. ресурс] // Современные проблемы науки и образования. 2017. № 2. Режим доступа: https://science-education.ru/ru/article/view?id=26383 (Дата обращения: 09.11.19).

10. Некраха А.В., Русецкая И.А. Особенности преподавания дисциплины «Основы информационной безопасности» в российских вузах // Вестник научных конференций. 2016. № 7–1 (11). С. 89–91.

11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электрон. ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_618011/ (Дата обращения: 09.11.19).

12. Постановление Правительства РФ № от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электрон. ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/ (Дата обращения: 09.11.19).

13. Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электрон. ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520/ (Дата обращения: 09.11.19).

14. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электрон. ресурс] Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (Дата обращения: 09.11.19).

15. Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электрон. ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_147084/ (Дата обращения: 09.11.19).

16. ГОСТ Р 51624 (проект, окончательная редакция) Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования [Электрон. ресурс] Режим доступа: https://fstec.ru/component/attachments/download/2066 (Дата обращения: 09.11.19).

17. Роганов А.А., Борисов Р.С., Карпов Д.С. Системы передачи информации: Учеб. пособие. Часть 1. М.: РГУТИС, 2013. 135 с.

18. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации, утвержденные Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г. [Электрон. ресурс]. Режим доступа: http://www.scrf.gov.ru/security/information/document155/ (Дата обращения: 09.11.19).

19. Раковенко А.А., Карпов Д.С., Гладышев А.И. Распознавания сосудистого русла в подсистеме биометрической аутентификации системы контроля управления доступом автоматизированной системы управления // Труды Шестнадцатой Международной научной конференции «Цивилизация знаний: российские реалии». М.: Российский новый университет, 2015. С. 294–297.

20. Карпов Д. С., Спива А.И. Об одном способе воздействия на информационные ресурсы, имеющих выход в сеть интернет // Материалы международной научно-практической конференции «Ценности и интересы современного общества». Часть 3. Современные парадигмы информационных технологий в развитии общества. М.: Московский государственный университет экономики, статистики и информатики, 2015. С. 88–93.

References

1. Vedeneyeva O.A., Savva L.I., Saygushev N.A. Pedagogicheskiye tekhnologii v sovremennom obrazovatel'nom protsesse. Uchebnoye posobiye.= Pedagogical technologies in the modern educational process. Tutorial. [Internet]. Moscow: World of Science, 2016. Available from: https://izd-mn.com/PDF/10UPNPMN16.pdf (cited: 09.11.19). (In Russ.)

2. Sysoyeva Ye. Yu. Innovative teaching methods in vocational education. Baltiyskiy gumanitarnyy zhurnal = Baltic Humanitarian Journal. 2018; 7; 1 (22): 299-301. (In Russ.)

3. Sysoyeva Ye. Yu. Interaktivnyye tekhnologii obucheniya v sisteme povysheniya kvalifikatsii pedagogov = .V kn.: Obrazovaniye i nauka: sovremennyye trendy: kollektivnaya monografiya. Gl. red. O.N. Shirokov = Interactive learning technologies in the system of advanced training of teachers. In the book: Education and science: modern trends: a collective monograph. Ch. ed. O.N. Shirokov. Cheboksary: Central nervous system «Interactive plus»; 2016. 1. 216 p. P. 113-133. (In Russ.)

4. Belyakova Ye. M., Prokop'yev A.V. Innovative teaching methods in education. Sovremennyye problemy nauki i obrazovaniya = Modern problems of science and education. 2015: 2 (part 1). (In Russ.)

5. Trofimenko A.S. Innovative teaching methods in higher education [Internet].Sci-article.ru. = Sci-article.ru. 2014: 13. Available from: http://sci-article.ru/stat.php?i=1408380616. (In Russ.)

6. Cherkasov M.N. Innovative methods of teaching students. Innovatsii v nauke: Sb. st. po mater. XIV mezhdunar. nauch.-prakt. konf. Chast' II = nnovations in science: Sat. Art. by mater. XIV int. scientific-practical conf. Part II. Novosibirsk: SibAK; 2012. (In Russ.)

7. Movchan I.N. Problems of training specialists in the field of information security. Otkrytoye obrazovaniye = Open Education. 2013; 5 (100): 78-80. (In Russ.)

8. Anur'yeva N.S. The modern education system in the field of information security in the Russian Federation.Vestnik Tambovskogo universiteta. Seriya Gumanitarnyye nauki. Tambov = Bulletin of the Tambov University. Series Humanities. Tambov. 2018; 23; 173: 111-120. (In Russ.)

9. Astakhova L.V., Tomilov A.A. New tasks of training personnel to protect information in the context of the "Doctrine of Information Security of the Russian Federation" (2016) [Internet]. Sovremennyye problemy nauki i obrazovaniya = Modern problems of science and education. 2017: 2 Available from: https://science-education.ru/ru/article/view?id=26383 (cited: 09.11.19). (In Russ.)

10. Nekrakha A.V., Rusetskaya I. A Peculiarities of teaching the discipline «Fundamentals of information security» in Russian universities. Vestnik nauchnykh konferentsiy = Bulletin of scientific conferences. 2016; 7-1 (11): 89-91. (In Russ.)

11. Federal'nyy zakon ot 27.07.2006 No. 152-FZ «O personal'nykh dannykh» = Federal Law of July 27, 2006 No. 152-ФЗ "On Personal Data" [Internet]. Available from: http://www.consultant.ru/document/cons_doc_LAW_618011/ (cited: 09.11.19). (In Russ.)

12. Postanovleniye Pravitel'stva RF № ot 1 noyabrya 2012 g. No. 1119 «Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» = Decree of the Government of the Russian Federation No. 1119 of November 1, 2012 "On approval of the requirements for the protection of personal data during their processing in personal data information systems" [Internet]. Available from: http://www.consultant.ru/document/cons_doc_LAW_137356/ (cited: 09.11.19). (In Russ.)

13. Prikaz FSTEK ot 18 fevralya 2013 g. No. 21 «Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» = Order of the FSTEC of February 18, 2013 No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems" [Internet]. Available from: http://www.consultant.ru/document/cons_doc_LAW_146520/ (cited: 09.11.19). (In Russ.)

14. Federal'nyy zakon ot 27.07.2006 No. 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» = Federal Law of July 27, 2006. No. 149-ФЗ "On Information, Information Technologies and Information Protection" [Internet] Available from: http://www.consultant.ru/document/cons_doc_LAW_61798/ (cited: 09.11.19). (In Russ.)

15. Prikaz FSTEK ot 11 fevralya 2013 g. No. 17 «Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh» = Order of the FSTEC of February 11, 2013. No. 17 "On approval of requirements for the protection of information not constituting state secrets contained in state information systems" [Internet]. Available from: http://www.consultant.ru/document/cons_doc_LAW_147084/ (cited: 09.11.19). (In Russ.)

16. GOST R 51624 (proyekt, okonchatel'naya redaktsiya) Zashchita informatsii. Avtomatizirovannyye sistemy v zashchishchennom ispolnenii. Obshchiye trebovaniya = GOST R 51624 (draft, final edition) Information security. Automated systems in a secure design. General requirements [Internet] Available from: https://fstec.ru/component/attachments/download/2066 (cited: 09.11.19). (In Russ.)

17. Roganov A.A., Borisov R.S., Karpov D.S.

Sistemy peredachi informatsii: Ucheb. posobiye. Chast' 1.= Information transmission systems: Textbook. allowance. Part 1. Moscow: RGUTIS; 2013. 135 p. (In Russ.)

18. Osnovnyye napravleniya nauchnykh issledovaniy v oblasti obespecheniya informatsionnoy bezopasnosti Rossiyskoy Federatsii, utverzhdennyye Sekretarem Soveta Bezopasnosti Rossiyskoy Federatsii N. P. Patrushevym 31 avgusta 2017 g. = The main directions of scientific research in the field of ensuring information security of the Russian Federation, approved by the Secretary of the Security Council of the Russian Federation N.P. Patrushev on August 31, 2017 [Internet]. Available from: http://www.scrf.gov.ru/security/information/document155/ (cited: 09.11.19). (In Russ.)

19. Rakovenko A.A., Karpov D.S., Gladyshev A.I. Vascular bed recognition in the biometric authentication subsystem of an access control system for an automated control system.Trudy Shestnadtsatoy Mezhdunarodnoy nauchnoy konferentsii «Tsivilizatsiya znaniy: rossiyskiye realii» = Transactions of the Sixteenth International Scientific Conference "Knowledge Civilization: Russian Realities". Moscow: Russian New University; 2015: 294-297. (In Russ.)

20. Karpov D.S., Spiva A.I. About one way of influencing information resources that have access to the Internet. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii «Tsennosti i interesy sovremennogo obshchestva». Chast' 3. Sovremennyye paradigmy informatsionnykh tekhnologiy v razvitii obshchestva = Materials of the international scientific-practical conference "Values and interests of modern society". Part 3. Modern paradigms of information technology in the development of society. Moscow: Moscow State University of Economics, Statistics and Informatics; 2015. P. 88-93. (In Russ.)

Сведения об авторах

Дмитрий Сергеевич Карпов
К.т.н., доцент, доцент кафедры прикладной информатики и информационной безопасности, Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: karpov.ds@rea.ru

Андрей Александрович Микрюков
К.т.н., доцент, доцент кафедры прикладной информатики и информационной безопасности, Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: mikrukov.aa@rea.ru

Петр Александрович Козырев
Ассистент кафедры прикладной информатики и информационной безопасности, Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: kozyrev.pa@rea.ru

Information about the authors

Dmitry S. Karpov
Cand. Sci. (Engineering), associate Professor, associate Professor of applied informatics and information security Department, Plekhanov Russian University of Economics, Moscow, Russia
E-mail: karpov.ds@rea.ru

Andrey A. Mikryukov
Cand. Sci. (Engineering), associate Professor, associate Professor of applied informatics and information security Department, Plekhanov Russian University of Economics, Moscow, Russia
E-mail: mikrukov.aa@rea.ru

Peter A. Kozyrev
Assistant of applied informatics and information security Department, Plekhanov Russian University of Economics, Moscow, Russia
E-mail: kozyrev.pa@rea.ru