Евгений Б. Белов[1], Владимир П. Лось[2], Анатолий А. Малюк[3]
[1]ФУМО ВО ИБ,
Мичуринский просп., 70, г. Москва, Россия
e-mail: umoib@yandex.ru, https://orcid.org/0000-0003-4854-1220
[2]Центр исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА,
Вернадского просп., 78, г. Москва, Россия
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

ЦИФРОВАЯ ЭКОНОМИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.01

Аннотация. Тенденции развития глобального информационного общества свидетельствуют о возрастании потребности в специалистах, обладающих высокой информационной культурой, в том числе обладающих знаниями и навыками обеспечения информационной безопасности. В Доктрине информационной безопасности Российской Федерации развитие и совершенствование системы соответствующей подготовки кадров заявлено в качестве одного из первоочередных мероприятий по реализации государственной политики в области формирования цифровой экономики. Подготовка кадров в данном случае должна предусматривать два направления – профессиональное и массовое обучение. В свою очередь, профессиональное обучение может быть основным и дополнительным. Основная цель массового обучения – формирование в обществе культуры информационной безопасности, недостаточный уровень которой отмечен в Доктрине информационной безопасности как одна из основных информационных угроз. Исходя из этого, в статье рассматриваются все актуальные сегодня проблемы как профессионального, так и массового обучения. При этом подчеркивается важность реализации парадигмы непрерывного образования (образования в течение всей жизни).

Таким образом, основная цель данной статьи заключается в раскрытии важнейших проблем обеспечения непрерывного процесса формирования современной культуры информационной безопасности с использованием возможностей всех звеньев образовательной системы.

Ключевые слова: информационная безопасность, кадровое обеспечение отрасли информационной безопасности, осведомленность по вопросам информационной безопасности, профессиональное и массовое обучение в области информационной безопасности, культура информационной безопасности.

Для цитирования: БЕЛОВ, Евгений Б.; ЛОСЬ, Владимир П.; МАЛЮК, Анатолий А. ЦИФРОВАЯ ЭКОНОМИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 6-22, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1157>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.01.

Evgeny B. Belov [1], Vladimir P. Los [2], Anatoly A. Malyuk [3]
[1]FUMO VO IB,
Michurinsky prosp., 70, Moscow, Russia
e-mail: umoib@yandex.ru, https://orcid.org/0000-0003-4854-1220
[2]Center for the Study of the Problems of Personnel Supply in the Information Security Industry RTU MIREA,
Vernadsky prosp.,78, Moscow, Russia
e-mail: los-vladimir@yandex.ru, https://orcid.org/0000-0003-4038-4048
[3]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute)
Kashirskoe sh.,31, Moscow, Russia
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

The digital economy and actual problems of the improvement of the training system in the field of information security

DOI: http://dx.doi.org/10.26583/bit.2018.4.01

Abstract. Trends in the development of the global information society indicate an increasing need for professionals with well established information culture, including those with knowledge and skills to ensure information security. The development and improvement of the system of appropriate training is stated in the Doctrine of information security of the Russian Federation as one of the priority measures for the implementation of the state policy in the field of digital economy. Training in this case should include both professional and mass training. In turn, the professional training can be basic and additional. The main goal of mass education is to form a culture of information security in society, which insufficient level of was noted in the Doctrine of information security as one of the main information threats. Therefore, the paper deals with the whole spectrum of the current problems of both professional and mass training. The importance of implementing the paradigm of continuous education ("lifelong learning") is emphasized.

Thus, the main purpose of this paper is to reveal the most important problems of ensuring the continuous process of formation of modern culture of information security using the capabilities of all components of the educational system.

Keywords: information security, staffing of the information security industry, information security awareness, professional and mass training in the field of information security, information security culture.

For citation: BELOV, Evgeny B.; LOS, Vladimir P.; MALYUK, Anatoly A. The digital economy and actual problems of the improvement of the training system in the field of information security. IT Security (Russia), [S.l.], v. 25, n. 4, p. 6-22, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1157>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.01.

Введение

Процесс формирования глобального информационного общества развивается нарастающими темпами. Сегодня мы являемся свидетелями широкого внедрения принципиально новых инструментов управления экономическими системами как на уровне отдельных государств, так и во всемирном масштабе. Появился даже новый термин «цифровая экономика», подразумевающий использование возможностей современных информационно-коммуникационных технологий (ИКТ) в обеспечении функционирования экономической системы. С другой стороны, цифровая экономика подразумевает также реализацию на основе концепции искусственного интеллекта систем поддержки принятия решений, базирующихся на широком спектре цифровых прогностических моделей.

Понятно, что указанные процессы с новой силой ставят проблему обеспечения информационной безопасности. Положительный эффект от реализации процессов цифровизации экономики возможен только в безопасной информационной среде. Иначе последствия такой «цифровизации» могут оказаться просто катастрофическими.

В Доктрине информационной безопасности Российской Федерации, принятой в декабре 2016 года, четко констатируется тот факт, что проблемы информационной безопасности (ИБ) перестали сегодня быть узкой областью исключительной компетенции специальных служб и все больше становятся предметом внимания достаточно образованной части населения. Тенденции информатизации мирового сообщества свидетельствуют о возрастании потребности в специалистах, обладающих высокой информационной культурой, владеющих новейшими информационными технологиями, умеющих применять их в своей профессиональной деятельности и обладающих знаниями и навыками обеспечения ИБ. Согласно Доктрине развитие и совершенствование системы соответствующей подготовки кадров, работающих как собственно в сфере обеспечения ИБ России, так и в других сферах экономики, широко использующих ИКТ, является одним из первоочередных мероприятий по реализации государственной политики в области формирования цифровой экономики. Подобная подготовка должна в том числе частично компенсировать повсеместное использование импортных средств

вычислительной техники, телекоммуникаций и программного обеспечения. Хотя, конечно же, это не снимает остроты проблемы импортозамещения в этой области.

Таким образом, не вызывает никаких сомнений высокая актуальность проблемы кадрового обеспечения сферы ИБ, а также формирования в обществе культуры информационной безопасности с использованием концепции непрерывного образования [1, 2].

При этом в системе высшего образования базовыми центрами формирования культуры информационной безопасности могут стать:

региональные учебно-научные центры по проблемам информационной безопасности, созданные в 1997 году на базе ведущих учебных заведений;

планируемые к созданию в рамках федерального проекта «Цифровая экономика» многофункциональные окружные учебно-научные (производственные) центры по проблемам обеспечения информационной безопасности для задач цифровой экономики в каждом федеральном округе на базе ведущей образовательной организации высшего образования, реализующей основные образовательные программы в области информационной безопасности;

планируемые к созданию в рамках федерального проекта «Цифровая экономика» межрегиональные центры в области информационной безопасности в системе среднего профессионального образования.

Обозначенные нами проблемы и являются предметом рассмотрения данной статьи.

1. Исторический очерк

Подготовка специалистов – профессионалов в области информационной безопасности в стране имеет, по крайней мере, 70-летнюю историю, если иметь в виду такую ее важнейшую составляющую, как криптография. Однако как целостная система такая подготовка стала складываться только в начале 90-х годов прошлого века. Этому способствовал целый ряд обстоятельств – развитие новых ИКТ, включая глобальные компьютерные сети, повсеместное использование этих технологий частными компаниями и гражданами и т.д. Как следствие, появился, например, большой интерес в негосударственном секторе к вопросам криптографии (особенно сюда следует отнести криптографию с открытым ключом), а также к компьютерной безопасности. Происходившая одновременно реформа высшего образования в стране, состоявшая, в частности, в переходе профессионального образования на Государственные образовательные стандарты (ГОС) в определенной степени стимулировала возникновение отдельного направления подготовки кадров «Информационная безопасность».

Сегодня, по прошествии более 20 лет, нам достаточно понятны процессы в естественнонаучном и техническом направлениях подготовки кадров в области ИБ. Существенно менее понятны они в гуманитарном направлении и на стыке указанных выше. Такая ситуация, по-видимому, достаточно естественна. Действительно, имеется прорыв по техническим составляющим новых информационных технологий. Вопросы же реализации заложенных в этих технологиях возможностей, с одной стороны, в значительной степени зависят от такого социально-экономического фактора, как возможность граждан получить доступ к ним, и от подходов к вопросам управления информационными сетями. С другой стороны, в мировом сообществе имеются различные точки зрения на роль государства в этих вопросах. В том числе высказывается и мнение, что государство несет ответственность за решение проблем, связанных с обеспечением неприкосновенности частной жизни, соблюдением авторских прав, содержанием передаваемой информации и доступом к ней, за электронной торговлей и компьютеризацией образования. При этом указанные проблемы должны решаться одновременно на национальном, региональном и международном уровнях. В настоящее время идет непростой процесс осознания нетехнических составляющих формирующегося информационного общества, а также возможностей, прав и обязанностей личности, общества и государства в нем.

Отметим далее, что к настоящему времени в системе Министерства науки и образования Российской Федерации сложились основы дееспособной системы подготовки специалистов, способных решать задачи обеспечения ИБ страны. Эта стройная, на наш взгляд, система опирается на Федеральное учебно-методическое объединение по образованию в области информационной безопасности (ФУМО ИБ), созданное в 1996 году на базе крупнейшего и известнейшего учебного заведения в этой области – Института криптографии, связи и информатики (ИКСИ) Академии Федеральной службы безопасности Российской Федерации, а также на сеть региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы, созданную Министерством общего и профессионального образования Российской Федерации в 1997 году.

Следует отметить, что российская система подготовки кадров в области ИБ занимает по ряду позиций ведущее положение, по крайней мере, среди европейских стран, о чем свидетельствуют материалы регулярно проводимой международной конференции по образованию в области информационной безопасности (*World Conference on Information Security Education*) [3 - 5].

На сегодняшний день эта система включает в себя следующие составляющие [6]:

- пять федеральных государственных образовательных стандартов (ФГОС) высшего образования и разработанных на их базе основных образовательных программ подготовки специалистов в области ИБ по специальностям: «Компьютерная безопасность», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Информационно-аналитические системы безопасности», «Безопасность информационных технологий в правоохранительной сфере»;
- два федеральных государственных образовательных стандарта высшего образования по направлению «Информационная безопасность» (подготовка бакалавров и магистров);
- три федеральных государственных образовательных стандарта среднего профессионального образования по специальностям: «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем», «Организация и технология защиты информации»;
- федеральное учебно-методическое объединение вузов России по образованию в области ИБ на базе ИКСИ Академии ФСБ России;
- более 100 вузов России различной ведомственной принадлежности, которые ведут образовательную деятельность по подготовке специалистов по указанным специальностям и направлениям;
- 12 министерств и ведомств и их органов управления профессиональным образованием, а также научные организации и учреждения, ведущие научные исследования в данной области, в том числе два головных центра – МГУ им. М.В. Ломоносова и Академия криптографии РФ;
- специальности и направления подготовки (соответствующие образовательные программы, включающие вопросы ИБ), реализуемые в рамках других УМО, смежных с входящими в группу по ИБ;
- 28 региональных учебно-научных центров по проблемам ИБ в системе высшей школы;
- образовательные программы дополнительного образования и соответствующие различные ведомственные курсы переподготовки и повышения квалификации;
- образовательные программы послевузовского образования в данной области (подготовка кадров высшей квалификации по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»).

Таким образом, сегодня можно с уверенностью говорить о сформированном вузовском сегменте образования. Хотя необходимо признать, что здесь еще недостаточна

или просто отсутствует координация усилий между различными УМО, а порой и основными заинтересованными ведомствами. Нет обоснованных решений по сочетанию различных схем и уровней подготовки, увязанных с потребностями соответствующих секторов экономики страны. Остаются проблемы и в области нормативного обеспечения функционирования системы. Все это будет рассмотрено нами ниже в соответствующих разделах данной статьи.

2. Проблемы профессионального обучения

В соответствии с Общероссийским классификатором специальностей по образованию (ОКСО) все интересующие нас ФГОС объединены в настоящее время в отдельную группу специальностей и направлений подготовки в области информационной безопасности (код 2.10.00.00). При этом в классификаторе предусмотрены все уровни подготовки: среднее профессиональное образование, бакалавриат, магистратура, специалитет и аспирантура.

С учетом задач развития цифровой экономики рассмотрим содержательное наполнение актуальных сегодня конкретных программ подготовки (специалитет, бакалавриат, магистратура). Результаты анализа приводят нас к следующим выводам. Особенностью практически всех программ является то, что содержание блока общих математических и естественнонаучных дисциплин отражает более глубокие требования к уровню базовой математической и естественнонаучной подготовки специалиста по информационной безопасности. Дополнительно к присутствовавшим в предыдущих поколениях стандартов математике, информатике, физике и экологии повсеместно добавлены дисциплины «Дискретная математика», «Математическая логика и теория алгоритмов», а также «Теория информации». Введение этих дисциплин в блок фундаментальной подготовки отражает принципиальную ориентацию обучающихся на овладение дискретными моделями, характеризующими информационные процессы, и специфическими для области методами их познания. Это вполне соответствует сформулированным нами компетенциям, требующимся для реализации задач цифровой экономики.

В группе дисциплин программного обеспечения информационных технологий в последнее время формируется более системный взгляд на сущность процессов построения программных комплексов. Программное обеспечение операционных систем и средств их интеграции, систем управления базами данных изучается не столько с функциональной точки зрения, сколько с аналитических позиций. Во главу угла поставлены архитектурные и основные технологические решения, их анализ с точки зрения обеспечения безопасности базирующихся на них информационных технологий. Увеличение числа рассматриваемых вопросов повлекло за собой увеличение общего числа часов, отводимых на изучение перечисленных выше дисциплин.

Ядро всех без исключения учебных программ определяет комплекс общепрофессиональных дисциплин, составляющих научный базис специалиста технологического профиля. Выделение общепрофессионального ядра является принципиальным моментом, характеризующим указанные программы.

Характерной чертой всех проанализированных нами программ является также введение в них общей дисциплины «Основы информационной безопасности», которая задумана как научный и методический фундамент всех дисциплин ядра. В процессе изучения этой дисциплины у студента должно сформироваться общее представление о структуре объекта изучения и основных понятиях теории информационной безопасности, содержании и взаимосвязи вопросов, изучаемых в остальных дисциплинах ядра. Присутствующая во многих программах дисциплина «Теоретические основы компьютерной безопасности» развивает и конкретизирует содержание методов обеспечения безопасности функционирования электронных систем обработки данных. Объектом изучения этой дисциплины является и технология проведения исследования и

проектирования подсистем защиты автоматизированных систем, и методы управления функционированием системы обеспечения безопасности.

Дисциплины «Криптографические методы защиты информации», «Технические средства и методы защиты информации» и «Программно-аппаратные средства обеспечения информационной безопасности» призваны сформировать основной профессиональный инструментарий специалиста по защите информации. Особенностями данных курсов является обязательность проведения практических и лабораторных занятий, на которых студенты должны приобрести реальные навыки применения современных программных и аппаратных средств, изучаемых в соответствующих курсах.

Особые задачи дальнейшего совершенствования содержательного наполнения дисциплин образовательных программ стоят перед дисциплинами «Организационное обеспечение информационной безопасности» и «Правовое обеспечение информационной безопасности». Эти дисциплины имеют своим объектом анализ человеческого фактора как неотъемлемой, а часто и решающей части комплекса мероприятий по обеспечению информационной безопасности любой системы. Анализ многих, в том числе и наиболее громких событий, связанных с нарушением нормальной работы автоматизированных систем, показывает, что прекрасно спроектированные с технической точки зрения системы оказываются достаточно уязвимыми для противоправной деятельности, нацеленной на персонал. Знание основных организационных мер обеспечения защиты объекта и наличие элементарной правовой культуры является необходимым требованием к любому специалисту по защите информации.

В целом анализ современных ФГОС и конкретных образовательных программ по специальностям и направлениям группы 2.10.00.00 позволяет сформулировать следующие выводы.

1. Все образовательные программы в области информационной безопасности характеризует явно выраженная общность структур общеобразовательного цикла дисциплин, что подтверждает их общую идеологию, необходимость их дальнейшего развития в рамках единой организационной структуры. Это основной принцип формирования программ данной группы. Он, вообще говоря, отличается от используемых при формировании образовательных программ других групп специальностей и направлений подготовки.

2. Характерным для всех программ ИБ является наличие в блоке общепрофессиональных дисциплин групп дисциплин, ориентированных на изучение тех или иных методов и средств обеспечения ИБ. К указанным группам относятся:

- дисциплины по общим вопросам обеспечения информационной безопасности;
- дисциплины по организационно-правовым методам обеспечения ИБ;
- дисциплины по криптографическим методам защиты информации;
- дисциплины по инженерно-техническим методам защиты информации;
- дисциплины по безопасности информационных технологий.

Общий объем указанных дисциплин для различных программ составляет в среднем около 30 % от объема блока общепрофессиональных дисциплин.

3. Цикл общепрофессиональных дисциплин базируется на достаточно специализированном естественнонаучном цикле. Характерно, что, по сравнению, например, с родственными программами в области компьютерной техники и информационных технологий, естественнонаучный цикл для специальностей и направлений в области ИБ отличается большим объемом и существенной дискретно-математической составляющей, включающей, как правило, дополнительно 2-3 дисциплины.

4. В то же время, в каждой программе в общепрофессиональном и естественнонаучном циклах имеется блок дисциплин, отражающий специфику предметной области подготовки специалистов, соответствующий профилю их профессиональной деятельности. Это отличие по содержанию различных

образовательных программ составляет примерно 25 – 30 % от объема блоков общепрофессиональных и естественнонаучных дисциплин.

5. Практика показывает, что в соответствии с запросами работодателей в качестве траектории образования наиболее востребованной все-таки оказывается подготовка дипломированных специалистов. Таким образом, с учетом разнообразия предметной области подготовки, различных квалификаций и сроков реализации образовательных программ возникают определенные сложности в формировании направления подготовки бакалавров и магистров. Более того, как вузы, так и потребители особо остро данную проблему не ставят. Вместе с тем с учетом общей концепции развития в стране системы образования ФУМО ИБ совместно с вузами и потребителями специалистов, очевидно, необходимо провести научную проработку вопроса о месте подготовки бакалавров и магистров в решении задач формирования цифровой экономики.

Учитывая, что удовлетворить потребность в специалистах в области обеспечения информационной безопасности можно только на основе комплексного использования возможностей среднего, высшего и дополнительного профессионального образования, как вариант можно было бы предложить систему подготовки и переподготовки кадров по ИБ, представленную на рис. 1. Указанная система создает, на наш взгляд, все необходимые условия для реализации концепции непрерывного образования в данной области.

Как известно, в Доктрине информационной безопасности Российской Федерации (2016 г.) большое внимание уделено анализу угроз информационной безопасности в различных сферах деятельности личности, общества и государства. В современных условиях важное место среди этих угроз занимают:

- деятельность иностранных разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Противодействие именно этим угрозам является, на наш взгляд, основным направлением дальнейшего развития группы 2.10.00.00. Кое-что в этом направлении на сегодняшний день уже сделано. В частности, сюда можно отнести специальность «Противодействие техническим разведкам».

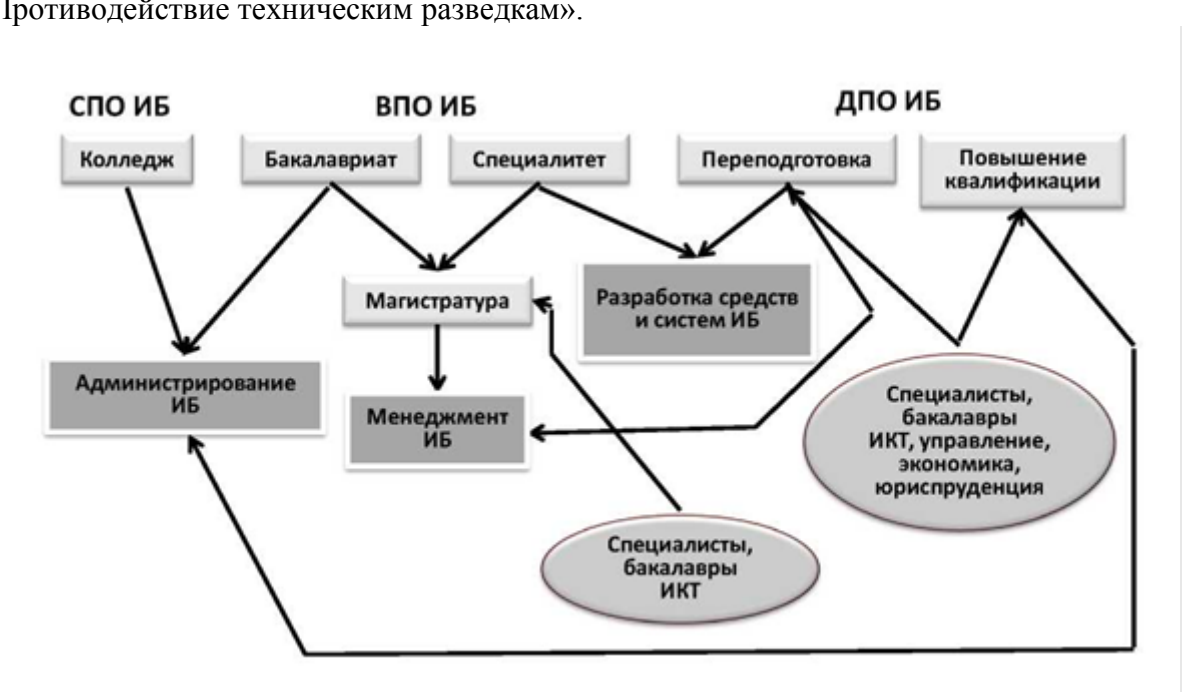

Рис. 1. Система подготовки и переподготовки кадров по ИБ
(Fig. 1. The system of training and retraining of personnel in the field of information security)

Новым направлением здесь может стать специальность с условным наименованием «Технические системы и средства информационного противоборства». Содержание образовательной программы здесь должно определяться моделью противоборства двух противостоящих друг другу контуров управления критическими системами, каждый из которых преследует цель дезорганизации управления противостоящей стороны и сохранения устойчивости своего управления. В рамках такой модели должны рассматриваться различные методы информационного воздействия на технические системы и человека и определяться пути обеспечения информационной безопасности.

В указанных специальностях неминуемо существенно увеличивается роль гуманитарной составляющей. Очевидно, если такие решения будут приняты, то возникает необходимость формирования специального модуля образовательной программы – «Гуманитарные проблемы информационной безопасности».

Нельзя не остановиться и на проблемах ИБ в гуманитарных специальностях и направлениях подготовки, входящих в ОКСО. Еще раз подчеркнем, что сегодня важнейшей задачей является увеличение подготовки специалистов по информационной безопасности гуманитарного профиля. Отметим, что в этом направлении уже более 20 лет активно работает Российский государственный гуманитарный университет, к которому подключился еще ряд вузов (НИЯУ МИФИ, МГУ, СПбГУ), создано несколько специализированных кафедр. Движение здесь очевидно, но, к сожалению, темпы развития этой тематики не соответствуют требованиям, изложенным в Доктрине информационной безопасности Российской Федерации. Не хватает нормативно-правовой базы по отдельным аспектам данной проблемы.

Серьезного внимания заслуживает проблема подготовки кадров для правоохранительных органов по расследованию преступлений в сфере компьютерной информации. Здесь можно отметить работу ряда вузов МВД, открывших вузовскую подготовку юристов с профилем в области ИБ. Однако активность в этом направлении в последнее время снижается, хотя появилась даже новая специальность «Безопасность информационных технологий в правоохранительной сфере». В чем здесь дело? Это тема для отдельного разговора, поскольку не понятно какое полушарие головного мозга должно преобладать при расследовании компьютерных преступлений или в разработке правового регулирования в киберпространстве, гуманитарное или техническое. На наш взгляд, заслуживает внимания симметричный подход, а именно – на базе технического направления давать юридическую специализацию или второе (юридическое) образование.

Другой возможный подход – разработка стандарта на стыке двух направлений (условно «Прикладная юриспруденция»). Подобный стандарт, по-видимому, мог бы быть взят за основу при подготовке специалистов для оперативных подразделений МВД, ФСБ и других силовых структур.

Аналогичную картину можно наблюдать и в области других гуманитарных направлений. Например, в философии – область этических проблем постиндустриального информационного общества или культура информационной безопасности. Можно также говорить о специализациях в области ИБ на базе специальностей и направлений по психологии и социологии.

3. Массовое обучение, формирование культуры информационной безопасности

Как уже отмечалось, формирование глобального информационного общества порождает широчайший спектр новых вызовов и угроз, связанных с активным внедрением современных ИКТ во все сферы деятельности. Чтобы успешно противостоять всему этому потоку негативных воздействий, каждому члену информационного общества необходимо обладать определенным минимумом знаний, соответствующей культурой информационной безопасности и быть готовым к активной борьбе за чистоту ИКТ.

Решению этой задачи может способствовать массовое введение во все образовательные стандарты (общего и профессионального образования, независимо от

специальностей и направлений подготовки) компетенций в области основ обеспечения информационной безопасности. Это даст возможность подготовить обучающихся к деятельности в условиях постиндустриального информационного общества, дать им представление о правовом регулировании отношений в сфере защиты информации, об основных организационных, инженерно-технических и иных мерах защиты.

Помимо прикладного аспекта введение таких компетенций имеет большое социально-воспитательное значение. Они должны быть направлены на формирование нравственных ориентиров в общественной жизни, на воспитание правосознания граждан и в то же время на устранение препятствий в реализации их конституционных прав и свобод в области духовной жизни и информационной деятельности. Подобную новацию, реализуемую в современной отечественной практике подготовки специалистов, следует рассматривать как элемент государственной информационной политики, позволяющей реализовать гармоничное сочетание интересов личности, общества и государства в информационной сфере.

Основой для разработки конкретного содержания соответствующих дисциплин, формирующих необходимые компетенции, может послужить материал резолюции Генеральной Ассамблеи ООН [7], принятой в декабре 2002 года и утвердившей принципы формирования глобальной культуры кибербезопасности. Глобальная культура кибербезопасности в трактовке данной резолюции формируется на основе 9 взаимодополняющих элементов:

- *осведомленности* об угрозах и подходах к обеспечению безопасности информационных систем и сетей;
- *ответственности* пользователей за безопасность информационных систем и сетей сообразно с ролью каждого из них;
- *реагирования*, подразумевающего принятие своевременных и совместных мер по предупреждению инцидентов, затрагивающих безопасность;
- *этики* как учета законных интересов других сторон и признания каждым участником, что его действия или бездействие могут причинить вред другим;
- *демократии* как непременного следования ценностям демократического общества, включая свободу обмена мыслями и идеями и свободный доступ к информации;
- *оценки риска*, предполагающей обязательную оценку потенциального риска любых действий, выявление угроз и факторов уязвимости;
- *проектирования и внедрения средств обеспечения безопасности* как важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;
- *управления обеспечением безопасности* на основе комплексного подхода, охватывающего все уровни деятельности членов информационного общества и все аспекты их операций в информационной сфере;
- *переоценки* как своевременного внесения надлежащих изменений в политику, практику, меры и процедуры обеспечения безопасности.

Отметим еще раз, что сегодня компетентность в сфере информационных технологий и информационной безопасности становится необходимым условием успешной социализации личности в новой информационной среде общества.

4. Единая образовательная среда как средство реализации концепции массового обучения

Развитие российского образования в соответствии с политикой, определенной Законом «Об образовании в Российской Федерации», предполагает формирование углубленных интеграционных и междисциплинарных программ, соединение их с прорывными высокими технологиями, актуализацию и приведение в соответствие с современной проблематикой учебных программ по большинству преподаваемых дисциплин, связанных с информационными технологиями. Среди прочего такая

модернизация предполагает первоочередное внедрение в сферу образования новых информационных технологий, позволяющих существенно повысить качество образовательных процессов, расширить доступность образования и упростить доступ к образовательным ресурсам.

Важным шагом на пути к достижению намеченных целей должно стать создание Единой образовательной информационной среды как принципиально нового механизма передачи, обработки и хранения информации в сфере образования, как средства распространения знаний и интеграции образовательных процессов. Вопрос о формировании такой среды с разной степенью интенсивности обсуждается на протяжении последних десяти лет как на разного рода конференциях и совещаниях, так и в научных и массовых публикациях. Задача эта оказывается непростой, так как предполагает постановку и решение ряда важных экономических и научно-технических проблем. К последним можно отнести следующие проблемы:

- техническую реализацию Единой образовательной среды;
- содержательное наполнение;
- обеспечение информационной безопасности среды.

Первая из этих проблем – техническая реализация Единой образовательной информационной среды – предполагает использование самых современных информационных технологий: широкое внедрение средств вычислительной техники, построение информационно-телекоммуникационных систем, систем распределенной обработки и хранения данных. Методологической основой создания современных крупномасштабных компьютерных информационных систем является концепция открытых систем и распределенной обработки данных. На сегодняшний день концепция открытых систем, основанная на системе международных стандартов и иных нормативных документов международных организаций, является единственным общепризнанным и универсальным подходом к формированию высоко сложных распределенных систем обработки данных и информационных систем на их основе.

Вторая проблема – содержательное наполнение Единой образовательной информационной среды, очевидно, предполагает, что в ней не только размещаются образовательные ресурсы, но и циркулирует большое количество других видов информации, что связано с многообразием функций образовательной среды. Все это требует введения как составной части среды средств и сетей хранения больших массивов информации.

Исключительно большое значение имеет проблема обеспечения информационной безопасности Единой образовательной информационной среды, на которой необходимо остановиться более подробно. Сложность этой проблемы обусловлена не только тем, что сама по себе сфера образования относится к приоритетным областям государственных интересов, но и тем, что Единая образовательная информационная среда является сложным и многофункциональным организационно-техническим комплексом. Очевидно, что эта проблема не может решаться без учета современных методов организации и технической реализации информационных систем. С целью уточнения методов и путей решения этой проблемы необходим анализ научно-методической и нормативно-технической базы в области открытых систем, созданной международными организациями по стандартизации информационных технологий.

Попробуем сформулировать в общих чертах концепцию обеспечения информационной безопасности Единой образовательной информационной среды. Концепция включает два основных аспекта – технический и организационный. Понятно, что технически она должна опираться на общепринятые международным сообществом принципы формирования открытых информационных систем с применением технических средств хранения и обработки больших массивов информации. Применение научно-методического аппарата открытых информационных систем позволяет создать основу единства и доступности формирующейся среды. Разработка политик безопасности основных структурных элементов Единой образовательной среды позволяет подойти к

решению задач обеспечения доступности и целостности информации. При этом необходимо учитывать присутствие в составе среды средств и сетей распределенной обработки и хранения больших массивов информации.

Организационная сторона концепции должна базироваться на действующем российском законодательстве. Таким образом, необходима разработка организационно-распорядительных документов, содержащих рекомендации по организации правоотношений в области охраны интеллектуальной собственности, а также устанавливающих механизмы распространения в среде сведений ограниченного распространения.

Детальный анализ особенностей рассматриваемой нами проблемы приводит к заключению о необходимости расширения самой предметной области обеспечения информационной безопасности в Единой образовательной информационной среде. Со всей очевидностью вскрываются новые существенные аспекты этой проблемы.

Во-первых, очевидно многообразие технических средств и решений, доступных сегодня на рынке информационных технологий. В этой связи весьма актуальной является задача оптимального выбора из этого обширного арсенала технических средств решений, необходимых для формирования Единой образовательной среды. Таким образом, необходима формулировка технической политики безопасности Единой образовательной информационной среды.

Вторая проблема связана с содержательным наполнением новой информационной среды, созданной на базе применения распределенных систем обработки и хранения информации. Развертывание и широкомасштабное применение Единой образовательной среды должно, по-видимому, сопровождаться определенной критической оценкой ценности и возможности применения обращающегося в ней контента.

Здесь, очевидно, необходимо особо отметить, что существует опасность превращения образовательной среды в своего рода «средство массовой дезинформации» и даже орудие ведения «информационных войн» и разрушения психики человека.

В этой связи необходима формулировка политики содержательного наполнения образовательной среды, где проблемы информационной безопасности приобретают особую актуальность. На первый план здесь выходит рассмотрение проблемы информационно-ценностного наполнения созданной новой среды обращения информации.

Третья важная проблема связана с необходимостью получения ответа на вопрос, каковы перспективы и прогнозы дальнейшего развития информационных технологий и средств их реализации. Без ответа на этот вопрос невозможно грамотно и точно сформулировать концепцию развития такой сложной организационно-технической системы, каковой является Единая образовательная информационная среда.

Достоверное прогнозирование будущего развития защищенных информационных технологий как основы цифровой экономики не может быть осуществлено без оценки нынешней роли информационных технологий в современном мире, с учетом как позитивных, так и негативных факторов, порождаемых этим явлением в жизни человеческого общества. Безусловно, появление информационных технологий стало одним из самых существенных этапов развития научно-технического прогресса, внесло коренные изменения во многие сферы деловой деятельности человека, в том числе и в сферу образования. Однако вместе со всеми позитивными тенденциями, которые вносят информационные технологии в развитие человеческого общества, с ними связан большой круг политических, психологических и духовно-нравственных проблем. Информационные технологии поднимают на новый уровень давно стоящую проблему – вместо естественного и гармонического взаимодействия научно-технический прогресс общества и его духовный прогресс становятся тормозом один для другого. Государственная система образования как сфера, ответственная за формирование личностных и гражданских качеств членов общества, особенно чувствительна к этой проблеме.

Четвертая существенная проблема – разработка методов построения прикладных программ и систем на базе Единой образовательной информационной среды, таких как системы защищенного электронного документооборота, системы дистанционного обучения и других систем.

С учетом, с одной стороны, сложности структуры и информационного наполнения среды, а с другой – ее многофункциональности и универсального характера для решения различных классов задач данная проблема также требует для своего решения определенной научно-методической основы. Необходимо проведение исследований, направленных на разработку методов обеспечения устойчивости функционирования и безопасности прикладных программ. Должны быть предусмотрены способы обеспечения доступа к информации даже в таких сложных условиях, когда происходит физическое или логическое прерывания доступа к части узлов распределенной системы. Такие события могут иметь место как в случае возникновения нештатных ситуаций, связанных с разрушением части системы, обрывом каналов связи, диверсионными акциями, так и в случае ошибок персонала, обслуживающего систему, технических сбоев и отказов аппаратуры или программного обеспечения.

Таким образом, анализ проблем информационной безопасности в Единой образовательной информационной среде указывает на то, что роль защиты самих информационных технологий и циркулирующей в них информации с течением времени может и должна возрастать. При этом очевидно, что информационные технологии как организационно-техническая основа формирования новой образовательной среды не имеют альтернативы в обозримом будущем. Следовательно, безопасность, в широком смысле, в перспективе должна превратиться в центральную качественную характеристику информационных технологий в сфере образования.

5. Государственное регулирование и закрепление кадров

В предыдущих разделах статьи уже неоднократно подчеркивалась ведущая роль государства в решении проблемы кадрового обеспечения информационной безопасности. Понятно, что это связано с ее решающей ролью в решении задач национальной безопасности в условиях развития глобального информационного общества.

Исторической иллюстрацией государственного регулирования сферы кадрового обеспечения ИБ является решение Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности от 22.06.1999 № 2.1 «Об основных направлениях совершенствования системы подготовки, повышения квалификации переподготовки кадров в области обеспечения информационной безопасности», сыгравшее ключевую роль в развитии всей системы подготовки кадров в этой области.

Основная тяжесть в выполнении данного решения легла на тогдашнее Министерство образования, а в методическом плане, соответственно, на УМО ИБ. И если в методическом плане на сегодняшний день достигнуты определенные результаты (разработаны новые стандарты, создана отдельная группа специальностей и направлений подготовки, разработаны примерные учебные планы и программы, подготовлен и готовится целый ряд учебно-научных и методических материалов и т.д.), то в направлении нормативного и организационного обеспечения подготовки кадров продолжают оставаться определенные проблемы.

Первое, что необходимо отметить, это несовершенный, на наш взгляд, механизм формирования государственного заказа на подготовку кадров в области информационной безопасности. Причиной здесь является несоответствие между потребностью и выпуском специалистов. Расчеты показывают (см. рис. 2), что в этой области имеют место иногда достаточно серьезные диспропорции.

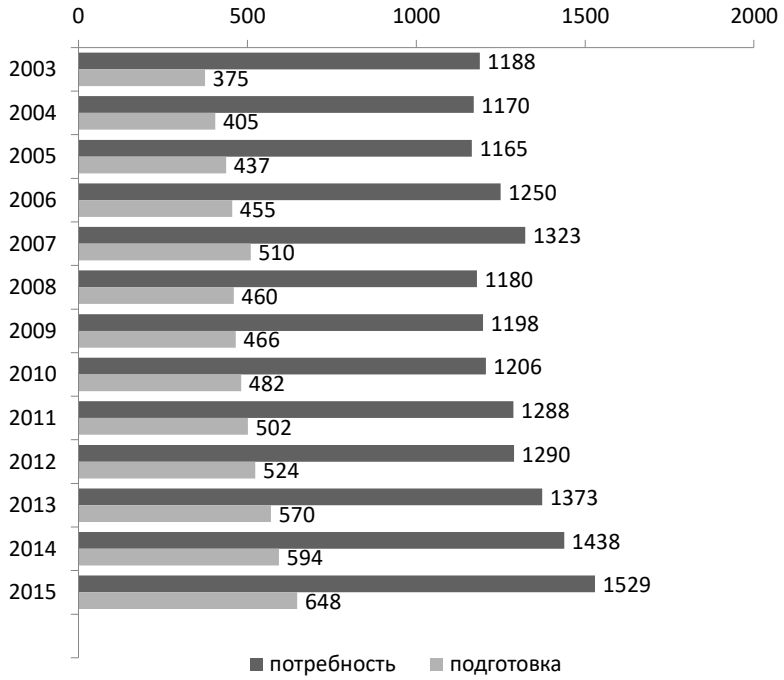

Рис. 2. Потребность и выпуск специалистов по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» (Fig. 2. Demand and graduation of specialists in the specialty «Complex provision of information security of automated systems»)

Объективными условиями возникновения этих диспропорций является неполное соответствие подготовки специалистов потребностям экономики страны. Не считаться с диспропорцией нельзя, поскольку она является причиной, с одной стороны, неполной обеспеченности кадрами, а с другой – роста безработицы или непрофильного использования специалистов. Все это в конечном счете отрицательно сказывается на эффективности развития отраслей экономики и приводит к потерям государственного бюджета. Для того чтобы избежать этих потерь, необходимо обеспечить соответствие между потребностями, подготовкой, трудоустройством и использованием специалистов.

Объективная возможность решения этой задачи заключается в прогнозировании возможных изменений в потребности в специалистах и учете их при формировании государственного заказа на подготовку контрольных цифр приема (КЦП). При этом важное значение имеет научное обоснование заявок на подготовку специалистов, что позволяет корректировать текущие и перспективные планы подготовки специалистов, осуществлять сокращение или расширение выпуска специалистов различных специальностей и направлений, воздействуя на миграцию специалистов, обеспечивая рациональное региональное размещение учебных заведений и т.д.

Причины существования этих да и ряда других проблем, по нашему мнению, заключаются в следующем:

- недостаточно проработаны концептуальные научные проблемы в сфере подготовки кадров в области информационной безопасности;
- отнесение нормативного и ресурсного обеспечения функционирования рассматриваемой системы подготовки кадров, а также вопросов закрепления специалистов в области информационной безопасности к компетенции различных федеральных органов исполнительной власти;
- недостаточное финансирование сферы образования и, как следствие, ограниченность финансовых средств, выделяемых со стороны Минобрнауки России, на проведение НИР по проблемам информационной безопасности, информационное и материально-техническое обеспечение рассматриваемой системы подготовки кадров;

- отставание нормативно-правового обеспечения деятельности в области ИБ.

Отметим еще и такое соображение. При непростой демографической ситуации, сложившейся в мире в целом, общем снижении интереса молодежи к сферам деятельности, связанным с решением инженерных проблем, задача кадрового сопровождения такой критической отрасли, как обеспечение ИБ, с опорой на национальные кадры приобретает первостепенное значение. Понятно, что ее решение требует существенных материальных и финансовых издержек. Вместе с тем в условиях рыночной экономики при решении вопросов развития профессионального образования весьма важной является проблема экономической эффективности затрат на образование. Кстати наиболее интересные результаты в этом направлении были получены в 60 – 70-х годах прошлого века советской экономической школой, возглавляемой академиками С.Г. Струмилиным и А.Г. Аганбегяном. С тех пор эта проблема практически выпала из внимания как отечественных, так и зарубежных экономистов.

Ориентируясь на пословицу, что «Новое – это хорошо забытое старое», попытаемся кратко проанализировать полученные в ту пору результаты и возможность их использования в современных условиях.

Прежде всего следует, на наш взгляд, отметить ошибочное и даже вредное (для обоснования затрат) отнесение образования к сфере услуг. При этом фактически забывается важнейшая социальная значимость образования и его роль в развитии научно-технического прогресса, формировании инновационной экономики.

Представляется, что затраты на образование в узко экономическом смысле аналогичны затратам на средства производства. Они также представляют собой издержки на создание необходимых предпосылок производства. Затраты на образование и на средства производства взаимно дополняют друг друга. Они содействуют созданию материальных и интеллектуальных факторов повышения производительности труда и развития производства. Иначе говоря, затраты на средства производства и на образование есть составные части издержек, которое общество должно нести, чтобы придать живому труду способность производить большее количество потребительных стоимостей. Эта мысль подтверждается рядом публикаций рассматриваемого нами периода [8 - 12].

Таким образом, рассмотрение особенностей воздействия образования на производство позволяет выделить три возможных направления определения экономической эффективности затрат на образование в современных условиях.

Во-первых, затраты на образование работников должны учитываться наряду с другими издержками при определении эффективности капитальных вложений как в масштабе всей экономики, так и по отдельным отраслям и объектам.

Во-вторых, важнейшим обобщающим показателем соотношения между развитием производства и образованием является результат сопоставления объема выпускаемой продукции с суммой кумулятивных общественных издержек на все необходимое образование, которым обладают работники, вовлеченные в производство продукции. Этот показатель сходен с показателем капиталоемкости (фондоемкости), выражающим эффективность использования основных средств производства.

В-третьих, практическое определение экономической эффективности затрат на образование возможно также на основе исчисления потерь общества от недостаточной квалификации кадров в конкретных производственных звеньях экономики.

В этой связи сошлемся на работу [13], посвященную анализу взаимосвязи численности принимаемых на обучение по программам высшего образования УГСНП «Информационная безопасность» и социально-экономических показателей субъектов федерации. Исследование проведено на примере Центрального федерального округа. Оказалось, что численность принимаемых на обучение в большинстве случаев напрямую связана с таким показателем как доля регионального валового продукта субъекта, приходящаяся на душу населения.

Анализ изложенных выше соображений, а также выход проблемы информационной безопасности в ряд важнейших компонентов национальной безопасности, на наш взгляд,

требует разработки и последовательной реализации специальной федеральной целевой программы развития системы подготовки кадров в области информационной безопасности в Российской Федерации.

Представляется, что для координации образовательной деятельности по повышению квалификации и переподготовке преподавательских кадров, реализующих программы в области ИБ, проведения научно-исследовательской работы в данной области было бы целесообразно преобразовать ФУМО ИБ в специальный федеральный учебно-методический комплекс. Это тем более целесообразно, когда одной из форм госрегулирования является мониторинг качества образования, даваемого вузами, который и мог бы взять на себя указанный комплекс.

Для практической реализации эффективной системы оценки качества образования в рамках специальностей и направлений по ИБ необходимо создание развитой нормативной базы как основания для построения оценочных средств и технологий мониторинга качества образования. В настоящее время такая нормативная база существует в виде совокупности федеральных государственных образовательных стандартов.

Для того чтобы ФГОС могли выполнять роль нормативной базы мониторинга в системе оценки качества образования, содержащиеся в них требования (в виде приобретаемых в процессе обучения компетенций) должны быть сформулированы с учетом принципа диагностики (проверяемости, контролируемости).

Необходимо отметить, что на сегодня в ФУМО ИБ реализован ряд положений с целью усиления такой диагностичности, хотя еще далеко не для всех требований. В них, в частности, заданы критерии сформированности умений и знаний у выпускника по уровням «иметь представление», «знать», «уметь», «владеть».

Подготовлены также комплекты контрольных заданий по основным дисциплинам каждого цикла дисциплин по ряду специальностей и направлений (опять же далеко не по всем). Разработаны примерные требования к образовательной среде и образовательному процессу, применяемые при лицензировании вузов. С целью получения оценки качества подготовки специалиста через год его практической деятельности разработана анкета-отзыв потребителя на выпускника.

Таким образом, можно говорить, что в целом нормативная база для мониторинга качества подготовки специалистов в первом приближении имеется.

В дальнейшем необходимо определить, кто и как будет осуществлять данный мониторинг. В соответствии с законодательством Российской Федерации государственный контроль возложен на государственные органы управления образованием (Рособрнадзор). Однако представляется, что наряду с этим необходимо усилить роль ФУМО в области контроля качества высшего образования. В частности, было бы полезно создать на базе ФУМО государственно-общественный центр сертификации качества высшего образования в области ИБ. Для усиления государственного регулирования вопросов подготовки специалистов в состав центра целесообразно включить помимо представителей высшей школы представителей от ФСБ, ФСТЭК и других структур – государственных регуляторов.

Качество высшего образования и качество специалистов в последнее время увязываются с требованиями профессиональных стандартов в области ИБ. Инструментами для оценки такой взаимосвязи должны стать внедряемые в настоящее время процедуры профессионально-общественной аккредитации образовательных программ и независимая оценка квалификаций специалистов.

И несколько слов о закреплении кадров. Очевидно, что какой бы эффективной система подготовки специалистов в области ИБ ни была, она не сможет обеспечить кадрами потребителей (прежде всего госструктуры), если в стране не будет создана эффективная система закрепления кадров. А пока системного решения этой проблемы нет.

Выводы

В целом с учетом всех современных задач кадрового обеспечения ИБ, как того

требует формирование цифровой экономики и реализация положений Доктрины информационной безопасности Российской Федерации, основные направления дальнейшего совершенствования системы подготовки специалистов в области ИБ, на наш взгляд, должны включать следующее:

- поддержку функционирования и дальнейшее развитие группы специальностей и направлений в области ИБ;
- разработку государственных образовательных стандартов и образовательных программ, в том числе и новых, при активном участии министерств и ведомств, регулирующих данную сферу деятельности;
- определение и формирование государственного кадрового заказа, особенно в интересах силовых министерств и ведомств;
- мониторинг использования специалистов в области информационной безопасности;
- формирование при государственной поддержке системы массового обучения культуре информационной безопасности (своего рода «всеобуча», в том числе на основе использования Единой образовательной среды), повышение уровня культуры личной информационной безопасности граждан страны;
- финансовое и материально-техническое обеспечение подготовки специалистов со стороны государства и ведомств, в том числе на условиях кооперации;
- нормативное оформление порядка лицензирования и контроля образовательной деятельности в области информационной безопасности;
- издание и использование в образовательном процессе учебно-методической литературы (в том числе электронных изданий), прошедшей экспертизу в ФУМО и соответствующих ведомствах;
- аттестацию и подготовку педагогических кадров в области защиты информации.

И еще одно замечание. На наш взгляд, серьезно стоит проблема участия ФУМО ИБ в лицензировании вузов по специальностям и направлениям подготовки, не входящим в объединенную группу 2.10.00.00 ОКСО, но напрямую посвященным ИБ, что требует более тесного взаимодействия с УМО или УМС, «смежными» с этой группой.

СПИСОК ЛИТЕРАТУРЫ:

1. Малюк А.А. Формирование культуры информационной безопасности общества // М.: Педагогика. ISSN: 0869-561X. № 3, 2009. С. 33-39. (https://elibrary.ru/item.asp?id=12609790).
2. Павлова Е.Д. Медиаобразование как способ формирования национальной информационной культуры//Приоритетные национальные проекты: первые итоги и перспективы реализации (Отв. ред. Ю.С. Пивоваров). – М.: ИНИОН РАН, 2007.
3. Malyuk A., Tolstoy A. Personnel Training for Information Security Maintenance in Russia // First World Conference on Information Security Education, Sweden, Kista, 1999.
4. Malyuk A., Miloslavskaya N., Tolstoy A. The Russian Experience Information Security Education // Second World Conference on Information Security Education, Perth, Western Australia, 2001.
5. Malyuk A., Miloslavskaya N., Tolstoy A. Teaching undergraduate information assurance in Russia // Third annual World Conference on Information Security Education, Monterey, California, USA, 2003.
6. Малюк А.А. Анализ и прогнозирование потребности в специалистах по защите информации. – М.: Горячая линия – Телеком, 2014.
7. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Создание глобальной культуры кибербезопасности». https://undocs.org/ru/A/RES/57/239
8. Марцинкевич В.И. Образование в США: экономическое значение и эффективность. – М.: Наука, 1967.
9. Жамин В.А. Экономика образования (вопросы теории и практики). – М.: Просвещение, 1969.
10. Волков Ф.М. Воспроизводство квалифицированной рабочей силы в СССР. – М.: Соцэкгиз, 1961.
11. Тольпин Ю.М. Действие закона экономии времени и новая методология его математического анализа.– М.: изд-во МГУ, 1964.
12. Я. Гомберг. Редукция труда. – М.: Экономика, 1965.
13. Лось В.П., Тышук Е.Д. Анализ взаимосвязи численности принимаемых на обучение по программам высшего образования УГСНП «Информационная безопасность» и социально-экономических показателей субъектов федерации (на примере Центрального федерального округа) / «Информация и безопасность», 2017, Т.20, № 3 (4).

REFERENCES:

[1] Malyuk A. Forming culture of society's information security. M.: Pedagogika. ISSN: 0869-561X. № 3, 2009. P. 33-39. (https://elibrary.ru/item.asp?id=12609790). (in Russian).
[2] Pavlova E.D. Media education as a way of formation of national information culture. Prioritetnije nacionalnije projekti: pervije itogi i perspektivi pealizacii. (otv. red. Ju.S. Pivovarov. – M.: INION RAN, 2007. (in Russian).
[3] Malyuk A., Tolstoy A. Personnel Training for Information Security Maintenance in Russia. First World Conference on Information Security Education, Sweden, Kista, 1999.
[4] Malyuk A., Miloslavskaya N., Tolstoy A. The Russian Experience Information Security Education. Second World Conference on Information Security Education, Perth, Western Australia, 2001.
[5] Malyuk A., Miloslavskaya N., Tolstoy A. Teaching undergraduate information assurance in Russia. Third annual World Conference on Information Security Education, Monterey, California, USA, 2003.
[6] Malyuk A.A. Analysis and forecasting of the need for information security specialists. – M.: Goryachaja linija–Telekom, 2014. (in Russian).
[7] Resolution of the UN General Assembly A/RES/57/239 «Creating a global culture of cybersecurity». https://undocs.org/ru/A/RES/57/239. (in Russian).
[8] Marcinkevich V.I. Education in the USA: economic value and efficiency. – M.: Nauka, 1967. (in Russian).
[9] Zhamin V.A. Economics of education (theory and practice). – M.: Prosveschenije, 1969. (in Russian).
[10] Volkov F.M. The reproduction of skilled labor in the USSR. – M.: Socekgiz, 1961. (in Russian).
[11] Tolipin Ju.M. Effect of the law of time saving and new methodology of its mathematical analysis. – M.: Ekonomika, 1964. (in Russian).
[12] Ja. Gomberg. Reduction of labor. – M.: Ekonomika, 1965. (in Russian).
[13] Los V.P., Tischuk Je.D. Analysis of the relationship between the number of students enrolled in higher education programs of areas of education «Information security» and socio-economic indicators of the subjects of the Federation (for example, the Central Federal district). «Informacija i Bezopasnost», 2017, T.20, N 3(4). (in Russian).

Поступила в редакцию – 17 сентября 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – September 17, 2018. The final version – November 01, 2018.