УДК 338.23:004.056.53

**Киреева Н. В., Поздняк И. С., Салмин А. А.**

# ВОПРОСЫ РЕАЛИЗАЦИИ НАЦИОНАЛЬНОЙ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА» В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Наталья Валерьевна Киреева***
*кандидат технических наук, доцент*
*kireeva@psuti.ru*
*ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара*
***Ирина Сергеевна Поздняк***
*кандидат технических наук*
*i.pozdnyak@psuti.ru*
*ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара*
***Алексей Александрович Салмин***
*кандидат технических наук*
*salmin.a@bk.ru*
*ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара*

# ISSUES OF IMPLEMENTATION OF THE NATIONAL PROGRAM "DIGITAL ECONOMY" IN THE FIELD OF INFORMATION SECURITY

***Natalya Valeryevna Kireeva***
*Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara*
***Irina Sergeevna Pozdnyak***

*Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara*

***Alexey Alexandrovich Salmin***

*Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara*

***Аннотация**. Национальная программа «Цифровая экономика» России имеет большое значение для будущего России и ее развития. Важной частью данной программы является информационная безопасность, которая тесно связана с современной жизнью человека. Национальная программа позволяет популяризировать информационные технологии и осуществить защиту информации. В статье рассматривается сущность информационной безопасности, ее взаимосвязь с образовательным и научным процессами и дальнейшем трудоустройстве с учетом компетентсного подхода для формирования будущего страны в рамках национальной программы.*

***Abstract** The national program "Digital Economy" of Russia is of great importance for the future of Russia and its development. An important part of this program is information security, which is closely related to modern human life. The national program makes it possible to popularize information technologies and protect information. The article examines the essence of information security, its relationship with educational and scientific processes and further employment, taking into account the competence approach for shaping the future of the country within the framework of the national program.*

***Ключевые слова**: национальная программа, информационная безопасность, образовательные ресурсы, высшее образование.*

***Keywords**: national program, information security, educational resources, higher education.*

Развитие цифровых технологий очень сильно влияет и воздействует на все отрасли экономики страны. Одной из основных задач в этом случае является создание новой технологической основы для развития экономики и соци-

альной сферы, а именно повышение качества жизни граждан при широком использовании цифровых технологий. Важное место занимает цифровизация системы образования, которая должна охватить широкий спектр вопросов, включая использование в образовательных организациях управление на основе анализа данных, онлайн-приложений и сервисов, внедрение цифровых образовательных инструментов и многое другое [1]. Современное высшее образование в настоящее время ориентировано на цифровую трансформацию образовательного процесса, обеспечивающую переход к новому технологическому укладу при реализации образовательных программ. Отдельным и стратегически важным направлением в этом случае становится сфера информационной и кибербезопасности, ориентированной на обучение специалистов по актуальным направлениям подготовки и специальностям в рамках укрупнённой группы «Информационная безопасность» при реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» [2].

Данный факт приводит к появлению особенностей реализации образовательных программ в сфере информационной безопасности (ИБ).

Одной из главных задач является разработка образовательных программ высшего и среднего профессионального образования в соответствии с федеральными государственными образовательными стандартами с учетом профтандартов в области ИБ.

В свою очередь профессиональные стандарты ориентированы на реализацию некоторых определенных функций:

- выявить производственные возможности работников;
- разработать образовательные стандарты для профессионального образования;
- разработать программы повышения квалификации;
- провести независимую оценку квалификации.

Известным фактом является высокие уровень и интенсивность развития сферы инфокоммуникационных технологий (ИКТ). Неотъемлемой частью совершенствования ИКТ являются вопросы обеспечения информационной безопасности [3]. Подготовка специалистов в этой отрасли достаточно своеобразна и учитывает необходимость воспитания у учащихся навыков, которые определяются огромным набором необходимых знаний в некоторых областях, таких как ИКТ, вычислительная техника, менеджмент, нормы и право на законодательном уровне и множество других. ФГОСы и профессиональные стандарты выдвигают выпускникам в области информационной безопасности ряд высоких требований. При этом требуется внедрение новых инновационных образовательных технологий. В таких ситуациях множество проблем связано со сложностью перехода от практики к теории. Особое внимание необходимо уделять воспитанию среди учащихся некоторых профессиональных навыков, связанных с возможностью применения полученных знаний в решении профессиональных задач. В сфере ИБ особое место занимает совокупность методов и способов при организации защиты информации в целом. На сегодняшний день остается проблема разработки продуктов отечественного производства, а также их внедрения и грамотной настройки при построении комплексных систем защиты информации на предприятии. Связано это в первую очередь с тем, что рассматривается довольно широкий круг задач, которые ориентированы на законодательную базу, проработку организационных вопросов, техническое обеспечение и многое другое.

Развитие и совершенствование технологий в области цифровых коммуникаций обязательно влечет возникновение некоторых рисков и угроз, учитываемых при развитии цифровой экономики, в частности:

- проблемы сохранения цифровых данных,
- угрозы безопасности личности человека, организациям и государству, которые связанны с созданием достаточно разветвленных иерархических инфокоммуникационных систем,
- рост количества компьютерных злоумышленников,

- задержка в развитии информационных технологий, которые были бы конкурентоспособны в сравнении с системами ведущих иностранных государств,
- слабая научная эффективность исследований, которые связанны с развитием информационных технологий и перспективой внедрения,
- недостаточный уровень продвижения отечественных конкурентоспособных разработок,
- низкий уровень обеспеченности кадрами информационной безопасности.

Область информационной безопасности, которая включается в стратегию развития цифровой экономики, поможет достичь необходимое состояние защищенности от различных видов информационных угроз и пользователям, и обществу, и государству. Чтобы решить данную задачу надо реализовать следующие условия:

- создать единую, устойчивую и безопасную инфокоммуникационную структуру Российской Федерации во всех областях информационного пространства;
- обеспечить защиту, как правовую, так и организационную, личностей пользователей, организаций и государственных потребностей при реализации задач цифровой экономики;
- обеспечить учет национальных интересов в международных документах, касающихся информационной безопасности, которые создают условия для того, чтобы Россия стала мировым лидером в экспорте услуг и технологий, связанных с информационной безопасностью.

Исследование рынка труда практически всех отраслей экономики показало, что по значительному количеству востребованных на рынке труда профессий в области ИБ подготовка специалистов осуществляется в недостаточном объеме. В связи с этим необходима актуализация профессиональных и образовательных стандартов в сфере информационной безопасности, в частно-

сти, относительно инфокоммуникационных технологий [4]. На текущий момент времени для реализации указанных задач применяются федеральные государственные образовательные стандарты высшего образования нового поколения, ориентированные на подготовку кадров по программам высшего образования, в том числе программы бакалавриата и специалитета.

Как часть общей системы национальной безопасности, информационная безопасность в современных условиях приобретает все большее значение. В немалой степени это связано с быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, экономическую жизнь и развитие общества становятся все более мощными.

Ключевым элементом технологического развития является усиление фундаментальных и прикладных исследований, направленных на разработку методов и средств информационной безопасности. Тем не менее, стоит отметить, что в настоящее время существует пять основных групп научных проблем, которые способствуют обеспечению безопасности Российской Федерации:

- проблемы информационной безопасности на гуманитарной основе;
- проблемы информационной безопасности на научно-технической основе;
- проблемы, связанные с кадровым обеспечением информационной безопасности.

Гуманитарная проблема информационной безопасности может быть решена путем:

- – формирования общих методологических основ обеспечения информационной безопасности, включая определение закономерностей развития информационной сферы как важного фактора современного общества, развития информационной безопасности как междисциплинарной отрасли научных знаний, интеграция ее с другими дисциплинами,

- – разработки и обоснования критерий и методов оценки состояния информационной безопасности с точки зрения решения основных социально-политических проблем страны на данном этапе, а также разработать пути и средства использования информационной сферы для решения основных социально-политических проблем страны.
- законы об информационной безопасности, включая правовое регулирование, обеспечение и защиту интересов личности и общества в информационной сфере, а также законы об информационном обеспечении государственной политики Российской Федерации, поддержка отечественной информационной индустрии и современных информационных технологий, правовое обеспечение телекоммуникаций и информационной безопасности, а также международно-правовые нормы в области информационной безопасности;
- обеспечение безопасности индивидуального, группового и массового сознания, включая информационную и психологическую безопасность личности и общества, понимание роли вопросов информационной безопасности в социальных процессах современного общества [5].

Для решения кадровых вопросов в области информационной безопасности необходимы следующие шаги:

- создание общих методологических основ кадрового обеспечения информационной безопасности, включая разработку и изучение механизмов государственного регулирования подготовки кадров в области информационной безопасности, анализ и обоснование тематической области подготовки кадров в области информационной безопасности как междисциплинарной отрасли науки и оценку подходящих тем для исследований, изучение возможностей использования современных образовательных технологий для повышения эффективности распространения знаний в области информационной безопасности, разработки научно-образовательного и методического обеспечения непрерывного обучения в области информационной безопасности;
- подготовка кадров в области информационной безопасности при поддержке организационной и нормативной базы;

- разработка структуры технологического сопровождения кадровой подготовки в сфере информационной безопасности, включая разработку специальных методик, специализированной и учебной литературы, создание эффективных инструментов применяющихся в современных технологиях образовательного процесса.

Беря во внимание необходимость в высококвалифицированных специалистах по информационной безопасности, требуется продолжить работу по выстраиванию действенной экосистемы подготовки сотрудников высшей квалификации [6].

Основной принцип подготовки кадров в сфере информативной безопасности, который является общим, — организация профессиональной подготовки на базе высшего образования, так как, сначала должно быть получено фундаментальное образование в какой-то области, чтобы в дальнейшем на этой базе получить дополнительные компетенции в области информационной безопасности.

Поэтому развитию подготовки специалистов высшей квалификации, включая овладение необходимыми компетенциями, в высших учебных заведениях необходимо уделять особое внимание. Для того чтобы сегодня реализовать научные исследования в области информационной безопасности, специалисты должны получить в вузе высшее фундаментальное образование, к которому добавляются необходимые элементы и компетенции, связанные со специализацией в сфере информационной безопасности. В связи с этим перед научным и профессиональным сообществами стоят сложные, наукоемкие и многогранные задачи по разработке и внедрению систем максимального обеспечения информационной безопасности.

Таким образом, в настоящее время для своевременного предупреждения и нейтрализации угроз информационной безопасности наиболее сильно ощущается необходимость применения объединенных усилий высшего образования, научных, государственных и промышленных кругов.

### *Список литературы*

1. *О Стратегии* развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203. Текст: электронный // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW _216363/.

2. *Об утверждении* программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р. Текст: электронный // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW _221756/.

3. *О системе* управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»): постановление Правительства РФ от 02.03.2019 № 234. Текст: электронный // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW _319701/.

4. *Кантышев, П.* Сбербанк и ЦБ спорят, кто главный по кибербезопасности: ЦБ хочет часть полномочий Сбербанка в «Цифровой экономике» / П. Кантышев, А. Еремина, С. Ястребова. Текст: электронный // Ведомости. URL: https://www.vedomosti.ru/finance/articles/2018/10/31/785328-sberbank-i-tsb-sporyat. Дата публикации: 31 октября 2018.

5. *Минзов, А. С.* Информационная безопасность в цифровой экономике / А. С. Минзов, А. Ю. Невский, О. Ю. Баронов. Текст: электронный // ИТНОУ: информационные технологии в науке, образовании и управлении. 2018. № 3 (7). С. 52–59. URL: https://cyberleninka.ru/article/n/Infor-matsionnaya-bezopasnost-v-tsifrovoyekonomike.

6. *Асаул, В. В.* Обеспечение информационной безопасности в условиях формирования цифровой экономики / В. В. Асаул, А. О. Михайлова. Текст: электронный // Теория и практика сервиса: экономика, социальная сфера, тех-

нологии. 2018. № 4 (38). С. 5–9. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-vuslovi-yah-formirovaniya-tsifrovoy-ekonomiki.

УДК [371.014.3:004]:[371.7:004.056]

**Поляков В. П.**

# ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОТЕЧЕСТВЕННОГО ОБРАЗОВАНИЯ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

***Виктор Павлович Поляков***
*доктор педагогических наук, профессор*
*polvikpal@mail.ru*
*Федеральное государственное бюджетное научное учреждение «Институт стратегии развития образования Российской академии образования, Россия, Москва*

# DIGITAL TRANSFORMATION OF NATIONAL EDUCATION AND ENSURING INFORMATION SECURITY OF THE PERSON

***Viktor Pavlovich Polyakov***
*Federal State Budgetary Scientific Institution «Institute for Education Development Strategy of the Russian Academy of Education», Russia Moscow*

***Аннотация.*** *Одной из важнейших задач в условиях трансформации системы российского образования является удовлетворение общественных запросов в создании надежных научно-педагогических, правовых, методических и организационных механизмов для обеспечения информационной безопасности субъектов образовательного процесса, недопущение вреда от опасных информационных воздействий на психическое, нравственное или физическое состояние личности.*