



## **О НАУЧНЫХ СПЕЦИАЛЬНОСТЯХ «КИБЕРБЕЗОПАСНОСТЬ» И «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

*Язов Ю.К.<sup>1</sup>*

Изменения структуры системы научных специальностей, определенные приказом Минобрнауки России от 24.02.2021 №118, в части специальностей 1.2.4 «Кибербезопасность» и 2.3.6 «Методы и системы защиты информации, информационная безопасность» вызвали многочисленные дискуссии среди ученых. Что только не предлагалось в ходе этих дискуссий: от разделения объектов исследований (например, объектами для исследований по специальности 1.2.4 предлагалось считать АСУ ТП, робототехнические системы и т.п., а все остальные объекты отнести к сфере специальности 2.3.6) до разделения предметной области по фундаментальным (для специальности 1.2.4) и прикладным (для специальности 2.3.6) аспектам исследований. Это обусловлено не только объективной тенденцией обострения внимания к вопросам обеспечения защищенности функционирования отечественных информационных систем в условиях быстро расширяющегося спектра угроз информационной безопасности, но и тем, что в отечественных документах по терминам и определениям сегодня отсутствует понятие «кибербезопасность».

В этой связи весьма своевременной и очень важной стала статья доктора технических наук, главного редактора журнала «Вопросы кибербезопасности» Маркова А.С., опубликованная в этом году в первом номере указанного журнала, где достаточно подробно описана история возникновения понятия «кибербезопасность» и приведены суждения автора, касающиеся сравнения паспортов специальностей и последних «нормативных и профессиональных стандартов как отражение современных инноваций».

Что касается понятия «кибербезопасность», то ис-

пользованию этого понятия должно предшествовать введение его определения в отечественных документах (нормативных правовых актах, государственных стандартах). Сегодня такого определения нет. Более того с приставкой «кибер» появилось много других нигде не определенных понятий, таких как «киберпространство», «киберугроза», «кибероружие», «кибероперация» и т.д. Такая вакханалия с введением терминов без каких-либо их определений в отечественных документах по терминологии приводит к «размыванию» рассматриваемой предметной области научных исследований по проблематике информационной безопасности. Введенные в американских документах определения, на мой взгляд, не выдерживают никакой критики. Так, например, в одном из базовых нормативных документов США «Концепции возможностей планирования операций в киберпространстве на 2016-2028 годы» [38] понятие «киберпространство» было определено как «глобальный домен в пределах информационной среды, состоящий из взаимозависимых сетевых инфраструктур информационных технологий, включая Интернет, сети связи, компьютерные системы, а также встроенные процессоры и контроллеры». Весьма нестрогое определение, основанное на других, не введенных должным образом понятиях, таких как «информационная среда», «инфраструктура информационных технологий», «глобальный домен в пределах...» и др.

Отечественными специалистами понятие «кибербезопасность» трактуется по-разному. Конечно, его введение, если это состоится, является предметом их договоренности, но при этом нельзя допустить, чтобы область исследований, связанных с обеспечением

<sup>1</sup> Язов Юрий Константинович, профессор Воронежского государственного технического университета, Главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России», Воронеж, Россия. E-mail: yaxoff\_1946@mail.ru

«кибербезопасности», пересекалась с областью исследований, связанных с обеспечением «информационной безопасности».

Тем более это важно учесть при разработке паспорта специальности: ведь получается, что паспорт разрабатывается по специальности с названием, которое нигде не определено. Если посмотреть на проект паспорта по специальности 1.2.4, то легко заметить, что большинство пунктов паспорта охватывается специальностью 2.3.6 и никакой специфики «кибербезопасности» (тем более, что понятие не определено) не видно.

В связи с этим Марков А.С. правильно отметил, во-первых, факт дублирования двух специальностей, во-вторых, то, что сегодня «наиболее дискуссионным становится ... вопрос, каким образом кибербезопасность как прикладная техническая область попала в раздел естественных наук», и в-третьих, то, что факт отнесения кибербезопасности к фундаментальным изысканиям весьма озадачивает специалистов по защите информации, обеспечению безопасности значимых объектов информационной инфраструктуры.

Нельзя отрицать, что развитие фундаментальных исследований в рассматриваемой предметной области сегодня уже востребовано. Это касается таких аспектов исследований, как разработка и совершенствование формальных моделей безопасности, развития новых технологий идентификации и аутентификации процессов и пользователей информационных технологий (в том числе с использованием элементов искусственного интеллекта, биометрии, нейронных сетей и др.), создания защищенного отечественного программного обеспечения, исследования физических явлений и технологий хранения и обработки информации, позволяющих сформировать новые принципы построения систем защиты информации и др., то есть тех аспектов, которые связаны с необходимостью фундаментальных исследований в данной предметной области. В связи с этим новая специальность, на мой взгляд, должна быть направлена на активизацию фундаментальных исследований и названа так, чтобы не вызывать недоумение и неоднозначную трактовку.

Тогда для такой специальности следует разработать соответствующий паспорт, ориентированный на подготовку кандидатов и докторов физико-математических наук в области обеспечения информационной безопасности и содержащий пункты, однозначно соответствующие характеру фундаментальных исследований.

Существующий проект паспорта по специальности 1.2.4 не отвечает этим требованиям. В нем указаны пункты, большинство из которых полностью покрываются специальностью 2.3.6. А это значит, что в статье Маркова А.С. правильно отмечено, что появление схожих паспортов специальностей в сфере информационной безопасности, но разведенных по разным областям науки – естественным и техническим, повлечет распараллеливание научных структур, порождение дилеммы выбора и др.

Наконец, необходимо отметить еще один аспект, связанный с последствием введения двух специальностей, разделенных на две области, касающийся координации исследований фундаментального и прикладного характера. Сегодня нет для этого ни организационных структур (например, межведомственного координационного совета), ни опыта формирования скоординированных планов проведения фундаментальных и прикладных исследований в рассматриваемой области, ни специалистов, ориентированных на фундаментальные исследования, ведь подавляющее большинство из них, как правильно отметил Марков А.С., имеют «конкретные внедрения научных результатов в технических науках и подтвердили их значимость». Возможно, для развития исследований по новой специальности потребуется также изменение или введение новых образовательных программ. Все это весьма осложняет подготовку ученых по новой специальности и вполне оправдано опасение Маркова А.С., что приведет не к добавлению «новой степени свободы научного творчества», а наоборот – окажется «под угрозой строгость научных положений». Тем не менее тенденция развития фундаментальных исследований в области информационной безопасности, на мой взгляд, объективна и правильна. Когда-то надо начинать и это.

