УДК 004.056
doi: 10.26583/bit.2024.1.06

Виктор С. Горбатов[1], Александр С. Эрдниев[2]
[1]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[2]Московский университет МВД России имени В.Я. Кикотя, ул. Академика Волгина, 12, Москва, 117437, Россия
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

СОВЕРШЕНСТВОВАНИЕ ПОДГОТОВКИ КАДРОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ*

Аннотация. Ведомственная система подготовки кадров МВД России накопила значительный опыт обучения специалистов по различным образовательным программам в области обеспечения информационной безопасности. За прошедшее десятилетие в данной области в силу различных факторов произошли значительные изменения, в частности, в аспекте ее государственного регулирования на основе директивных положений Доктрины информационной безопасности России, и они придали новый импульс по актуализации и адаптации этих изменений в существующих образовательных программах. Такая работа ведется «широким фронтом» вузами России, подведомственными Минобрнауки России, в рамках одноименного Учебно-методического объединения. Очевидна также необходимость решения данной задачи и на ведомственном уровне, в частности, в рамках системы подготовки кадров МВД России. В настоящей работе изложены результаты этапа предпроектного обследования объекта разработки, в качестве которого выступает вариативная часть соответствующих программ, разработанных на базе федеральных образовательных стандартов. На основе данного обследования предполагается дальнейшая разработка и реализация мероприятий по повышению качества подготовки кадров в области обеспечения безопасности информационной инфраструктуры органов внутренних дел. Объектом исследования является процесс подготовки кадров для ОВД, а предметом – повышение качества этого процесса в сфере обеспечения безопасности информационной структуры ОВД. Для достижения соответствия квалификационных требований к отдельным категориям должностей органов внутренних дел с новыми нормативными характеристиками, сформулированными государственными регуляторами, в статье рассмотрен отечественный опыт ведущих вузов и иностранный опыт образовательной подготовки специалистов в сфере информационной безопасности. Основой формулирования предложений по модернизации вариативной части образовательных программ для подготовки специалистов по защите информационной инфраструктуры органов внутренних дел является опыт проектирования отечественных профессиональных стандартов по защите информации и отдельные иностранные инициативы.

Ключевые слова: высшее образование, компетенции, критическая информационной инфраструктура, органы внутренних дел, образовательная программа, федеральный государственный образовательный стандарт.

Для цитирования: ГОРБАТОВ, Виктор С.; ЭРДНИЕВ, Александр С. СОВЕРШЕНСТВОВАНИЕ ПОДГОТОВКИ КАДРОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 100–119, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1604. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.

Благодарности. Работа проводится в рамках выполнения договора о взаимном сотрудничестве между НИЯУ МИФИ и Московским университетом МВД России имени В.Я. Кикотя от 12 июля 2023 г. № 394.

Viktor S. Gorbatov[1], Aleksandr S. Erdniev[2]
[1]National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
[2]Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot, 12 Akademika Volgina str., Moscow, 117997, Russia
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

Improving the training of specialists to ensure the security of the information infrastructure of the internal affairs authorities*

Abstract. The departmental personnel training system of the Ministry of Internal Affairs of Russia has significant experience in training specialists in various educational programs in the field of information security. Over the past decade, due to various factors, significant changes have taken place in this area, particularly in its state regulation based directive provisions for the Russian Information Security Doctrine. And they have also given a new impetus to the actualization and adaptation of these changes in existing educational programs. Such work is being carried out «on a broad front» by Russian universities subordinate to the Ministry of Education and Science of the Russian Federation, within the framework of the Educational and Methodological Association of the same name. There is also an obvious need to solve this problem at the departmental level, in particular, within the framework of the personnel training system of the Ministry of Internal Affairs of Russia. This paper presents the results of the pre-design survey, which is a part of the relevant educational programs developed on the basis of federal educational standards. Based on this survey, it is planned to further develop and implement measures to improve the quality of training in the field of managing information infrastructure security for Russian internal affairs authorities. The object of the study is to improve the quality of this process in the field of managing the security of the information for the Department of Internal Affairs. In order to achieve qualification requirements for certain categories within the internal affairs bodies, the article examines the domestic experience of leading Russian and international universities in educational training of specialists in the field of information security. The basis for the formulation of proposals for the modernization of the variable part of educational programs for the training of specialists in the protection of the information infrastructure of internal affairs authorities is the experience of designing domestic professional standards for the protection of information and individual foreign initiatives.

Keywords: higher education, competencies, critical information infrastructure, internal affairs agencies, educational program, federal state educational standard.
For citation: GORBATOV, Viktor S.; ERDNIEV, Aleksandr S. Improving the training of specialists to ensure the security of the information infrastructure of the internal affairs authorities IT Security (Russia), [S.l.], v. 31, no. 1, p. 100–119, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1604. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.

*Acknowledgement. The work is carried out within the framework of the implementation of the agreement on mutual cooperation between the MEPhI Research Institute and the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot dated July 12, 2023 № 394.

Введение

За прошедшее десятилетие в отечественной системе обеспечения информационной безопасности происходят «тектонические» изменения. В частности, значительно повысился уровень государственного регулирования на основе новой редакции Доктрины информационной безопасности[1], утвердившей в качестве одной из основных задач

[1]Доктрина информационной безопасности РФ. Утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.

обеспечение «…устойчивости социально-экономического развития…» страны. К основным определяющим факторам такого процесса можно отнести не только резкое, в том числе информационное, противостояние с недружественными странами, но и глубокая цифровизация всех сфер жизнедеятельности российского общества. Не обходят стороной эти факторы и органы внутренних дел (ОВД) как разновидности силовой государственной службы Российской Федерации. Преобразования последних лет позволили ОВД автоматизировать практически все процессы оказания государственных услуг, оцифровку реестров значимой информации, в том числе персональных данных. Происходит активное внедрение автоматизированных систем управления (АСУ) для обеспечения охраны общественного порядка и безопасности граждан. Такая активная цифровизация органов государственного управления требует наличия у представителей власти определенного набора новых профессиональных знаний, умений и навыков по обеспечению устойчивости цифровых управленческих процессов. Это, в свою очередь, обуславливает актуальность задачи детального изучения процесса подготовки кадров в этом направлении для ОВД, существенным элементом которого является разработка и внедрение новой вариативной части образовательной подготовки специалистов сил обеспечения информационной безопасности ОВД, учитывающей реализацию новых подходов государственного регулирования в этой области.

Решение данной задачи и является целью настоящего исследования, объект которого – процесс подготовки кадров ОВД, а предмет – повышение качества этого процесса в сфере обеспечения безопасности информационной структуры ОВД.

Одним из самых значимых изменений прошедшего десятилетия стало введение механизмов государственного регулирования в области информационной безопасности на основе таких понятий как «критически важные объекты» (КВО)[2] и критическая информационная инфраструктура[3] (КИИ). Подробный анализ этого феномена и его влияния на совершенствование государственной системы защиты информации проведен в [1]. Системный анализ действующей нормативно-правовой базы, разработанной на основе указанных выше понятий, показывает, что ее подходы, методы и требования, по умолчанию, могут и должны быть использованы для развития любой системы безопасности независимо от ведомственной принадлежности, а тем более для ОВД. Именно этот фактор определяет актуальность основной цели, объекта и предмета проводимого исследования по совершенствованию ведомственной системы подготовки кадров по обеспечению безопасности информационной инфраструктуры на основе предпроектного обследования объекта и предмета исследования.

Практическая значимость достижения поставленной цели состоит в обеспечении соответствия квалификационных требований (компетенций) к отдельным категориям должностей ОВД с новыми нормативными характеристиками, сформулированными государственными регуляторами в области обеспечения информационной безопасности. В качестве основы для формулирования предложений по модернизации указанной выше вариативной части образовательных программ предлагается применить опыт проектирования отечественных профессиональных стандартов, а также отечественный

[2]Указ Президента России № 803 от 3 февраля 2012 г. «Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов Российской Федерации».

[3]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

опыт ведущих вузов и иностранный опыт образовательной инициативы по подготовке специалистов в сфере кибербезопасности[4] [2].

В рамках проводимого исследования заданы следующие научно-исследовательские **задачи**:

1. Определение сущности понятия КИИ ОВД.
2. Аналитический обзор ведомственной и отечественной систем подготовки кадров по безопасности КИИ.
3. Анализ методических основ подготовки кадров по безопасности КИИ ОВД как методологической базы развития вариативной части соответствующих образовательных программ.

1. Сущность понятия «КИИ органов внутренних дел»

Изучение смыслового наполнения понятия «КИИ органов внутренних дел» может претендовать на логическую завершенность при рассмотрении его через призму эволюции соответствующего блока нормативно-правового регулирования, представленной в [1], его целей и задач по введению новых организационных механизмов практической реализации.

Общая проблема выделения КИИ, в том числе в сфере ОВД, тесно связана с пониманием сущности его субъектов и объектов, заданной основным законодательным актом[3]. Согласно его нормам отечественное понятие КИИ определяется совокупностью субъектов и объектов, в число которых входят также «…сети электросвязи, используемые для организации взаимодействия таких объектов». При этом действующие правовые нормы задают исчерпывающие перечни этих ключевых понятий, что приводит к определенной сложности адаптации новых организационно-нормативных механизмов на основе указанного законодательства применительно к сфере ОВД. Организации системы МВД России не входят в исчерпывающий перечень субъектов указанного законодательства. Поэтому применение к сфере ОВД его основных положений напрямую представляется несостоятельным и нужно определенное обоснование такой возможности.

Разрешение этой коллизии можно построить на основе анализа упомянутого выше директивного акта[3], в котором ключевым понятием является «безопасность КВО», а также даны легальные определения понятий КВО и КИИ Российской Федерации. В аспекте нашего исследования целесообразно привести положение из этого документа: КИИ РФ «…– совокупность АСУ КВО и обеспечивающих их взаимодействие информационно-коммуникационных систем, предназначенных для решения задач государственного управления, обеспечения обороноспособности, ***безопасности и правопорядка***, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий». Сопоставляя эти директивные положения и законодательные нормы государственного регулирования в сфере безопасности КИИ, можно сделать очевидный вывод, что новые организационно-нормативные механизмы обеспечения такой безопасности не только можно, но и должно использовать применительно к сфере ОВД.

В этом же аспекте значительно проще решается задача выделения объектов КИИ ОВД. В соответствии с п. 7 статьи 2 закона[3], под ними понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ.

Все указанные элементы имеются в информационной инфраструктуре ОВД и, на основании указанной нормы следует сделать вывод о том, что по смысловому

[4]Executive Order no. 13636, «Improving Critical Infrastructure Cybersecurity». DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. (дата обращения: 24.12.2023).

содержанию понятие «КИИ ОВД» соответствует требованиям законодательства о КИИ, хотя как указано выше, объектная часть закона[3] и не отражает субъектную принадлежность описанных информационных систем.

Кроме того, ключевым элементом, определяющим сущность понятия КИИ ОВД, является выполнение задач, связанных с исчерпывающим перечнем сфер жизнедеятельности общества, которые находятся напрямую в ведении ОВД.

Основным нормативным правовым актом, определяющим административно-правовой статус ОВД в системе органов государственной власти (ОГВ) и раскрывающим их полномочия является указ Президента России от 21.12.2016 № 699[5]. В соответствии со статьей 11 Указа к категории полномочий МВД России относится:

– обеспечение функционирования специальных административно-правовых режимов на территории государства (в том числе гражданской, территориальной обороны, мобилизации и контртеррористической операции);

– контроль за распространением наркотических и наркосодержащих, психотропных веществ и их прекурсоров (что напрямую связано и со сферой здравоохранения как субъекта рассматриваемого законодательства);

– координация деятельности по обеспечению безопасности дорожного движения и транспортной безопасности, что также является сферой законодательства о безопасности КИИ.

Таким образом, формальные компоненты функционального назначения подразделений ОВД полностью соответствуют характеристике субъектов КИИ в нотациях понятий КВО[2] и КИИ[3]. Кроме того, информационные системы ОВД содержат следующие категории чувствительных сведений: оперативно-розыскную информацию; информацию об объектах учета государственной инспекции безопасности дорожного движения; криминалистические, дактилоскопические, архивные данные, содержащие информацию о персональных данных граждан Российской Федерации и др.

Систематизацию нормативных правовых оснований, обосновывающих объективность понятия «КИИ ОВД» целесообразно представить через схему, приведенную на рис. 1.

На основе этой схемы можно однозначно выделить в качестве объектов КИИ ОВД информационные системы МВД России, информационно-телекоммуникационные сети ОВД, АСУ ведомств и подразделений МВД России. Основным структурным элементом, ответственным за безопасность КИИ ОВД должен выступать Департамент информационных технологий, связи и защиты информации МВД России (ДИТСиЗИ МВД России)[6].

[5]Указ Президента РФ от 21.12.2016 № 699 (ред. от 17.07.2023) «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации».

[6]Приказ МВД России от 15.06.2021 № 444 (ред. от 27.07.2023) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации».

Рис. 1. Нормативная гармонизация понятия «КИИ органов внутренних дел»

Одним из существенных организационно-нормативных механизмов законодательства о безопасности КИИ, обеспечивающих его эффективность в аспекте госрегулирования, является процедура категорирования объектов с целью определения их значимости и, следовательно, соответствующих требований к системе защиты. На основании постановления Правительства РФ от 8.02.2018 № 127[7], согласно п. 3 Правил категорированию подлежат «объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ». Исходя из позиции законодателя[8], что основной из важнейших функций ОВД является административно-позитивная деятельность, объекты КИИ ОВД способствуют обеспечению управленческих инициатив, направленных на защиту законных прав и интересов граждан.

Задать объекты КИИ ОВД поможет также исследование, рассматривающее содержательное наполнение информационных систем ОВД [3]. В них представлены данные о: «статистической, учетно-регистрационной информации, для организации оперативно-розыскной деятельности, производства следственных действий, проведения криминалистических исследований, управления подразделениями ОВД».

Административно-правовой статус подразделений ОВД определяет порядок формирования информационных систем на федеральном уровне, в исключительных случаях (например, аппаратно-программный комплекс «Безопасный город») на уровне федерального субъекта. Подобная трактовка позволяет соотнести информационные системы МВД России с Перечнем показателей критериев значимости объектов КИИ, установленных в рассмотренном выше Постановлении Правительства РФ. По категориям значимости допустимо выделить такие, как социальная значимость, политическая значимость, значимость для обеспечения безопасности и правопорядка.

[7]Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

[8]Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации».

По уровню категорий подпадают такие показатели, как:

– прекращение или нарушение функционирования объектов транспортной инфраструктуры;

– отсутствие доступа к государственной услуге;

– прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия);

– прекращение или нарушение функционирования пункта управления или ситуационного центра;

– прекращение или нарушение функционирования информационной системы в области обеспечения безопасности государства и правопорядка.

В соответствии с установленным порядком категорированию подлежат все объекты КИИ соответствующих субъектов, что приводит к значительному увеличению трудоемкости мероприятий по их защите. Учитывая, тем не менее, актуальность задачи обеспечения безопасности КИИ ОВД, для снижения этого недостатка нового механизма можно воспользоваться опытом Росатома[9], согласно которому устанавливается единая 3-я категория значимости для всех объектов КИИ и соответствующие защитные требования.

Совокупность большинства информационных систем ОВД в настоящий момент сконцентрирована в Единой информационной системе ограниченного доступа МВД России (ИСОД МВД России), которая обеспечивает реализацию информационно-справочного функционала единой информационно-телекоммуникационной сети МВД России [4, с. 140].

К структурным информационным системам ИСОД МВД России относятся:

– сервисы обеспечения повседневной деятельности ОВД;

– сервисы обеспечения оперативно-служебной деятельности.

Обеспечивают функционирование информационных систем следующие компоненты:

– система централизованной обработки данных;

– интегрированная мультисервисная коммуникационная сеть;

– подсистема обеспечения информационной безопасности;

– подсистема обеспечения взаимодействия подразделений ОВД с населением страны.

Понимание структурных элементов позволяет определить операторов информационных систем, формальных администраторов и подразделения, обеспечивающие безопасность информационной инфраструктуры. В ОВД подразделения, обеспечивающие насыщение системы значимой информацией зачастую не являются ее пользователями и не обеспечивают техническую защиту эксплуатируемой информации.

Так за информационное наполнение большинства сервисов отвечает Главный информационно-аналитический центр МВД России (ГИАЦ МВД России). В отдельных элементах операторами информационных систем выступают подразделения Центрального аппарата МВД России (ЦА МВД России). Организация функционирования информационных систем МВД России представлена на рис. 2.

[9]Единые отраслевые методические указания по категорированию объектов критической информационной инфраструктуру Госкорпорации «Росатом». Приказ Госкорпорации «Росатом» от 08.06.2020 № 1/591-П.

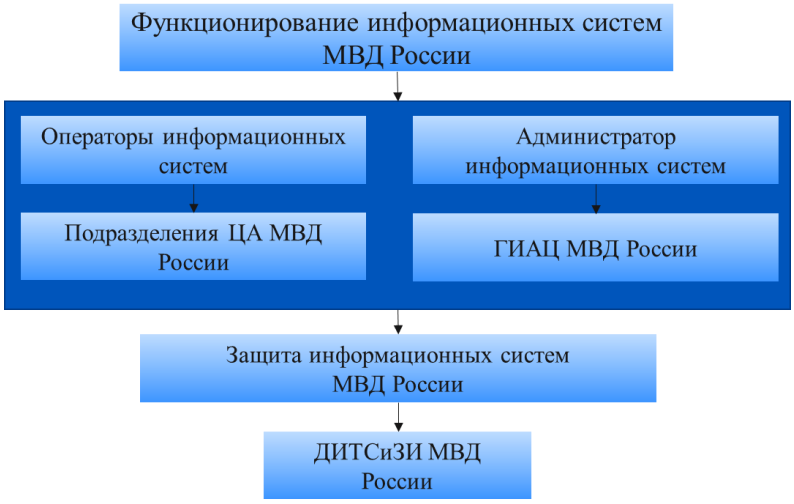

Рис. 2. Организация функционирования информационных систем МВД России

Исходя из предложенной организации функционирования информационных систем МВД России, допустимо сделать вывод о том, что подготовка специалистов по защите информации, а также сотрудников, отвечающих за защиту КИИ ОВД, находится в ведении таких подразделений-заказчиков, как ДИТСиЗИ МВД России и ГИАЦ МВД России.

2. Опыт подготовки специалистов по безопасности КИИ

2.1 Компетентностный подход

Отечественная система подготовки квалифицированных специалистов базируется на компетентностном подходе, по которому в рамках образовательного процесса формируются три вида компетенций: универсальные, общепрофессиональные и профессиональные. В дальнейшем в ходе реформирования высшей школы в соответствии с Указом[3] предполагается дополнительное введение так называемых базовых компетенции, но, учитывая, что их статус находится пока на уровне предложений, в данном случае они не рассматриваются.

Универсальные компетенции связаны с мировоззрением личности, ценностными установками и ориентирами, а также формируют способность к адаптации и творческому мышлению. К общепрофессиональным компетенциям относятся знания, умения и навыки по направлению специальности с учетом развития области профессиональной деятельности, без привязки к конкретным трудовым функциям. Профессиональные компетенции ориентированы на выполнение конкретных профессиональных задач.

Схожими принципами обладают механизмы подготовки кадров для сферы информационной безопасности в системе образования в США [5, с. 4], в национальной системе образования республики Куба [6, с. 530] или на основе высшего образования в Индии [7, с. 55]. Позиция иностранных государств ориентируется на создание определенной системы квалификационных рамок, исходя из анализа рынка труда и потребности бизнеса в конкретных навыках будущего квалифицированного специалиста.

Рассмотрим, каким образом нормативно решается данная проблема в российской системе высшего образования.

В Трудовом Кодексе Российской Федерации[10] содержатся нормы, определяющие порядок формулирования трудовых функций, а также требований к квалификации, необходимых для всех категорий работников, выполняющих отдельные виды профессиональной деятельности. Согласно статье 195.3 Кодекса в качестве нормативного инструмента выступает профессиональный стандарт. В российском классификаторе профессиональных стандартов содержатся четыре вида нормативных документов, раскрывающих характеристики обобщенных трудовых функции специалиста по защите информации. К ним относятся:

– специалист по защите информации в телекоммуникационных системах и сетях[11];
– специалист по безопасности компьютерных систем и сетей[12];
– специалист по защите информации в автоматизированных системах[13];
– специалист по технической защите информации[14].

Обобщенные трудовые функции по этим профессиональным стандартам представлены в табл. 1.

Необходимость изучения положений профессиональных стандартов обосновывается нормами законодательства Российской Федерации об образовании[15]. Так в статье 11 указанного закона определяется взаимозависимость профессиональных стандартов и политики в сфере профессионального образования. Профессиональные трудовые функции задают содержание федеральных государственных образовательных стандартов высшего образования (ФГОС ВО), а вместе с ними соответствующие учебно-методические комплексы (УМКД) подготовки квалифицированных кадров для выполнения специализированной профессиональной деятельности.

Представленные профессиональные стандарты могут быть соотнесены с такими действующими ФГОС ВО, как:

– 10.03.01 Информационная безопасность;
– 10.05.01 Компьютерная безопасность;
– 10.05.02 Информационная безопасность телекоммуникационных систем;
– 10.05.03 Информационная безопасность автоматизированных систем;
– 10.05.04 Информационно-аналитические системы безопасности;
– 10.05.05 Безопасность информационных технологий;
– 10.04.01 Информационная безопасность.

Представленные ФГОС ВО определяют подготовку специалистов по информационной безопасности как по программам специалитета, так и в рамках бакалавриата и магистратуры.

В положениях данных ФГОС ВО содержатся принципы организации образовательного процесса, основным из которых является разделение программного блока УМКД на две основные части: базовую и вариативную. Базовая часть содержит дисциплины, направленные на формирование универсальных и общепрофессиональных компетенций, содержание которых определяется требованиями Минобрнауки России.

[10]«Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ.
[11]Приказ Минтруда России от 14 сентября 2022 № 536н «Специалист по защите информации в телекоммуникационных системах и сетях».
[12]Приказ Минтруда России от 14 сентября 2022 № 533н «Специалист по безопасности компьютерных систем и сетей».
[13]Приказ Минтруда России от 14 сентября 2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах».
[14]Приказ Минтруда России от 09 августа 2022 № 474н «Специалист по технической защите информации».
[15]Федеральный закон от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации».

Вариативная же часть формируется образовательной организацией самостоятельно и исходит из принципа специализации программы обучения, а также потребности по конкретным профессиональным функциям будущего квалифицированного специалиста.

Таблица 1. Обобщенные трудовые функции профессиональных стандартов, связанных с информационной безопасностью

Профессиональный стандарт	Пример трудовых функций
Специалист по защите информации в телекоммуникационных системах и сетях	– выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НД и компьютерных атак; – обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации и т.д.
Специалист по безопасности компьютерных систем и сетей	– администрирование средств защиты информации в компьютерных системах и сетях; – оценивание уровня безопасности компьютерных систем и сетей; – разработка программно-аппаратных средств защиты информации компьютерных систем и сетей; – техническое обслуживание средств защиты информации в компьютерных системах и сетях и т.д.
Специалист по защите информации в автоматизированных системах	– обслуживание систем защиты информации в автоматизированных системах, используемых, в том числе, на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости; – обеспечение защиты информации в автоматизированных системах, используемых, в том числе, на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации и т.д.
Специалист по технической защите информации	– проведение работ по установке и техническому обслуживанию средств защиты информации; – проведение работ по установке и техническому обслуживанию защищенных средств обработки информации; – производство, сервисное обслуживание и ремонт средств защиты информации от утечки по техническим каналам; – производство, сервисное обслуживание и ремонт средств защиты информации от несанкционированного доступа и т.д..

Достижение задачи, поставленной в данной статье, не может претендовать на логическую завершенность без ориентира на перспективу развития профессионального образования в области обеспечения информационной безопасности, активно прорабатываемой отечественными вузами в рамках соответствующего Учено-методического объединения (УМО). Так, в материалах Пленума северо-западного отделения УМО проанализировано содержание ФГОС ВО 4+ нового поколения [8]. Существенным изменением в новых образовательных стандартах является отступление от программ бакалавриата в пользу базового высшего образования и специализированного высшего образования. Наличие в новых ФГОС индикаторов сформированности компетенций актуализирует потребность в определении не только универсальных, базовых и общепрофессиональных компетенций, но и тех знаний и умений, которые относятся к специализированной профессиональной деятельности. При этом в нормах ФГОС ВО нового поколения, как и в действующих ФГОС, содержатся положения, в

соответствии с которыми профессиональные компетенции, относящиеся к специализированной деятельности, задаются профессиональными стандартами. Исключение составляют программы подготовки кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка. Профессиональные компетенции по данным программам определяются на основе квалификационных требований к профессиональной подготовке, устанавливаемой профильным ведомством, что дополнительно задает повышение актуальности исследуемых задач с учетом опыта разработки ФГОС нового поколения.

2.2 Требования к специалистам по безопасности КИИ ОВД

Нормы материального права в сфере высшего образования определяют и механизм формирования требований к квалифицированным специалистам. В соответствии с ним отечественная квалификационная рамка для ОВД представляется в виде систематизированных квалификационных требований по конкретным видам профессиональной деятельности и программ, формируемых образовательными организациями самостоятельно с учетом положений ФГОС ВО (см. рис. 3).

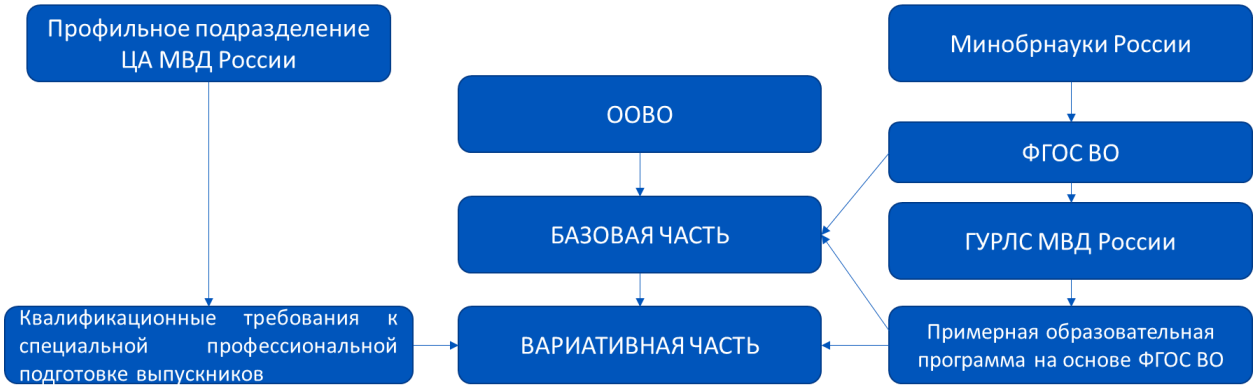

Рис. 3. Национальная квалификационная рамка для ведомственной подготовки кадров

Представленная схема позволяет сделать вывод о том, что квалификационные требования к специалистам по обеспечению безопасности КИИ ОВД определяются профильными подразделениями ЦА МВД России. Однако требования к специалистам также исходят из тех проблем, с которыми сталкивается заказчик в процессе повседневной служебной деятельности, в связи с чем проанализируем различные публикации по обеспечению информационной безопасности в ОВД.

Так исследование вопросов обеспечения информационной безопасности в ОВД при работе с различными информационными системами в [9] связывает наличие большого количества инцидентов с низким уровнем профилактики противодействия несанкционированному доступу к конфиденциальной информации. В качестве решения этой проблемы предлагается подготовка квалифицированных специалистов на базе образовательной системы МВД России, для которых приоритетным профессиональным навыком будет способность выполнять задачи по проектированию системы защиты информации объектов информатизации и информационных систем.

В [10, с. 126] и [4, с. 144] отмечают недостаточную квалификацию специалистов ОВД, обеспечивающих защиту КИИ в аспектах нормативно-организационного характера. Так формулируемые регламенты и иные акты публичного управления содержат системные ошибки и недоработки, способствующие совершению должностных нарушений. Оба автора видят решение в формировании навыков у сотрудников по

разработке нормативно-методических и организационно-распорядительных документов, регламентирующих работу по защите информации.

В исследовании проблем эффективного информационно-аналитического обеспечения деятельности ОВД [11, с. 81] обосновывается необходимость проведения комплекса кадровых мероприятий, направленных на организации подготовки кадров и повышения квалификации, связанную с формированием навыка применения информационно-аналитических систем в повседневной деятельности. Также в ОВД выделяется значительная потребность в специалистах по техническому обслуживанию аппаратных, программных, программно-аппаратных средств защиты информации.

Одним из факторов необходимости обеспечения информационной безопасности в ОВД является «компьютеризация процесса управления» [12, с. 80]. Справедлива позиция, по которой нарушение целостности и конфиденциальности служебной информации угрожает эффективной организации служебной деятельности подразделений ОВД. Решение задач по обеспечению защиты КИИ ОВД связывается с формированием ряда таких компетенций у сотрудников, как:

– способность выполнять задачи по проектированию программно-аппаратных средств защиты информации компьютерных систем и сетей;

– способность разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей;

– способность проводить работы по установке и техническому обслуживанию защищенных технических средств обработки информации;

– способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, проводить анализ принятых мер по защите информации, разрабатывать предложения по повышению их эффективности.

По результатам ведомственного мониторинга [13, с. 40] угроз информационной безопасности выявлено, что для ОВД наиболее актуальной угрозой является «проникновение в информационные системы вредоносного кода». Данное обстоятельство обуславливает необходимость формирования у специалистов таких навыков, как: способность устанавливать, настраивать и эксплуатировать технические системы защиты информации, а также способность управлять информационной безопасностью автоматизированной системы.

В отдельных исследованиях значительное внимание уделяется обеспечению физической защите информации [14, с. 61], при этом особого внимания заслуживают различные каналы утечки речевой информации (акустические, виброакустические и т.д.). Для обеспечения физической защиты информации требуется формирование таких навыков, как: выполнение работ связанных с реализацией локальных политик информационной безопасности, способность анализировать возможные уязвимости и обосновывать актуальные угрозы безопасности информации, а также наличие навыков аттестации объектов информатизации.

Таким образом, в различных исследованиях формулируется пул необходимых компетенций для квалифицированного специалиста, отвечающего за защиту информации в ОВД. По сути, все перечисленные навыки сводятся к четырем видам защиты информации и отражаются в виде набора компетенций.

В 2021 г. для определения содержательного наполнения образовательного процесса разработаны и утверждены квалификационные требования к специальной профессиональной подготовке выпускника федеральных государственных образовательных организаций, находящихся в ведении МВД России, по двум группам укрупненных специальностей: 10.05.03 Информационная безопасность

автоматизированных систем и 10.05.05 Безопасность информационных технологий в правоохранительной сфере. В них заданы четыре группы квалификационных требований к специальной профессиональной подготовке выпускников образовательных организаций высшего образования, находящихся в ведении МВД России.

К ним относятся:

– разработка автоматизированных систем в защищенном исполнении;

– технологии защиты информации;

– информационно-аналитическое обеспечение правоохранительной деятельности;

– оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации.

Все представленные квалификационные требования являются типовыми для ОВД. Первое представляет набор компетенций в рамках реализации ФГОС ВО 10.05.03 Информационная безопасность автоматизированных систем. Последние три требования направлены на определение компетенций при реализации образовательной программы в рамках ФГОС ВО 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Система квалификационных требований представлена в табл. 2.

Анализ содержания указанных выше квалификационных требований позволяет сделать ряд выводов. Так требования по трудовым функциям специалиста по разработке автоматизированных систем в защищенном исполнении более детализированы в сравнении с квалификационными требованиями по другим представленным трудовым функциям. Однако присутствует дублирование отдельных компетенций в различных задачах профессиональной деятельности, что, по нашему мнению, является избыточным. Требования к выпускникам, обучаемым, в рамках ФГОС ВО 10.05.05 Безопасность информационных технологий в правоохранительной сфере также представлены конкретными задачами профессиональной деятельности, но формируемые компетенции и отражают в первую очередь деятельность сотрудника полиции, а не специалиста по информационной безопасности.

Следует обратить внимание на формулировку квалификационных требований к выпускникам, в которой присутствует такое определение, как «специальная профессиональная подготовка».

Профессиональное образование в интересах ОВД осуществляется в рамках двух основных этапов: профессиональное обучение и освоение навыков, необходимых для выполнения специализированных трудовых функций. Под «специализированными» в данном контексте понимается специализация в соответствии с освоением компетенций по основной образовательной программе. Для выполнения задач профессиональной деятельности функционал выпускника связывается с компетенциями по должности сотрудника полиции. Отсюда следует сделать вывод о наличии избыточной информации в квалификационных требованиях в действующей редакции и недостаточную конкретизацию специализированных профессиональных компетенций.

Таблица 2. Соотношение задач профессиональной деятельности с ключевыми компетенциями

Специализация	Задачи профессиональной деятельности выпускника	Ключевые компетенции
10.05.03 Информационная безопасность автоматизированных систем		
Разработка автоматизированных систем в защищенном исполнении	научно-исследовательские	навыки научно-исследовательской деятельности
	проектные	разработка систем защиты информации, аттестация объектов информатизации, использование криптографических средств защиты информации
	контрольно-аналитические	исследования и проверки объектов информатизации, контроль работоспособности средств защиты информации
	организационно-управленческие	компетенции на основании ФЗ «О полиции»
		планирование и организация аттестации объектов информатизации
	эксплуатационные	администрирование информационных систем, защита информации, управление информационной безопасностью
10.05.05 Безопасность информационных технологий в правоохранительной сфере		
Технологии защиты информации в правоохранительной сфере	проектно-технологические	проектирование систем защиты информации, разработка моделей угроз информационной безопасности
	эксплуатационные	администрирование информационных систем, защита информации, управление информационной безопасностью
	аналитические	способен применять информационно-аналитические системы в повседневной деятельности
	правоохранительные	обязанности сотрудника полиции
	оперативно-служебные	защита объектов информатизации
		компетенции сотрудника полиции
	организационно-управленческие	управление в сфере внутренних дел
		организации защиты информации
	правоприменительные	обязанности сотрудника полиции
Информационно-аналитические обеспечение правоохранительной деятельности	проектно-технологические	проектировать и разрабатывать требования к программно-аппаратным средствам защиты информации
	эксплуатационные	установка и обслуживание защищенных технических средств обработки информации
	аналитические	способен применять информационно-аналитические системы в повседневной деятельности
	правоохранительные	обязанности сотрудника полиции
	оперативно-служебные	использование технологий искусственного интеллекта
		компетенции сотрудника полиции
	организационно-управленческие	управление в сфере внутренних дел
		управление подразделениями в сфере информационных технологий
	правоприменительные	обязанности сотрудника полиции
Оперативно-техническое обеспечение расследования и раскрытия преступлений в сфере компьютерной информации	проектно-технологические	проектировать и разрабатывать требования к программно-аппаратным средствам защиты информации
	эксплуатационные	установка и обслуживание защищенных технических средств обработки информации
	аналитические	способен применять информационно-аналитические системы в повседневной деятельности
	правоохранительные	обязанности сотрудника полиции
	оперативно-служебные	оперативно-техническое обеспечение оперативно-розыскной деятельности
		обязанности сотрудника полиции
	организационно-управленческие	управление в сфере внутренних дел
		управление подразделениями в сфере информационных технологий
	правоприменительные	обязанности сотрудника полиции

Содержание квалификационных требований в существующей редакции не в полной мере отражает именно специализированные компетенции, необходимые для выполнения отдельных трудовых функций. Отсюда возникают затруднения в формировании образовательных программ в части их вариативного наполнения.

Схожая дисгармония при разработке профессиональных стандартов описана в исследовании, направленном на изучение вопросов подготовки кадров для обеспечения безопасности объектов КИИ [15, с. 57–59]. Авторами предложено решение по гармонизации профессиональных стандартов, основанное на иерархии квалификационных требований от общетрудовых функций до трудовых действий по конкретной специальности. Предложенное решение может послужить основой и для разработки квалификационных требований для сотрудников ОВД. Так общетрудовые функции допустимо насытить компетенциями, связанными с деятельностью сотрудника полиции, на уровне деятельности по профессии задать компетенции, связанные со сферой защиты КИИ и информационной безопасности в целом. На уровне конкретных трудовых функций и специализированных трудовых действий отразить компетенции, связанные со специализацией по профессиональной деятельности.

Дальнейшее исследование и рекомендации по разработке требований к специалистам по обеспечению безопасности КИИ ОВД должны быть гармонизированы с требованиями соответствующих ФГОС ВО нового поколения.

2.3 Система ведомственной подготовки кадров по безопасности КИИ

В сфере внутренних дел за образовательную деятельность отвечает кадровое подразделение МВД России[16]. На сайте Главного управления по работе с личным составом МВД России (ГУРЛС МВД России)[17] представлена вся система ведомственной подготовки кадров органов внутренних дел. Исходя из предложенной системы, подготовку кадров для обеспечения защиты КИИ органов внутренних дел осуществляют следующие вузы:

– Московский университет МВД Росси имени В.Я. Кикотя;
– Санкт-Петербургский университет МВД России;
– Краснодарский университет МВД Росси;
– Воронежский институт МВД России.

Отдельные программы повышения квалификации, связанные с защитой информации реализует Всероссийский институт повышения квалификации МВД России. Однако в связи с тем, что данная образовательная организация не реализует подготовку кадров по программам высшего образования, интереса в рамках проводимого исследования не представляет. На основании норм приказа МВД России от 2 августа 2013 г. № 591[18] за профиль подготовки по направлениям информационной безопасности в ОВД отвечает Воронежский институт МВД России.

Содержание направлений подготовки, общая характеристика образовательных программ по направлению информационной безопасности представлена на официальных сайтах образовательных организаций, в разделах «Кандидатам на обучение». Исходя из

[16]Постановление Правительства РФ от 26 июля 2010 г. № 537 «О порядке осуществления федеральными органами исполнительной власти функций и полномочий учредителя федерального государственного учреждения.
[17]Официальный сайт ГУРЛС МВД России. URL: https://гурлс.мвд.рф. (дата обращения: 24.12.2023).
[18]Приказ МВД России № 591 от 2 августа 2013 г. «О внесении изменений в приказ МВД России от 29 августа 2012 г. № 820 «О профилизации образовательных учреждений МВД России».

предельных цифр приема, опубликованных на сайтах образовательных организаций[19], следует сделать вывод о том, что наибольшее количество поступающих и направлений подготовки, несмотря на профилизацию вузов, числится за Московским университетом МВД России имени В.Я. Кикотя.

Система направлений подготовки по обеспечению информационной безопасности в интересах органов внутренних дел представлена в табл. 3.

Таблица 3. Характеристика направлений подготовки ведомственных вузов

ФГОС ВО	Специализация / профиль подготовки
Воронежский институт МВД России	
10.05.01 Компьютерная безопасность	информационно-аналитическая и техническая экспертиза компьютерных систем
10.05.02 Информационная безопасность телекоммуникационных систем	сети специальной связи
Московский университет МВД России имени В.Я. Кикотя	
10.05.03 Информационная безопасность автоматизированных систем	разработка автоматизированных систем в защищенном исполнении
10.05.05 Безопасность информационных технологий в правоохранительной сфере	компьютерная экспертиза
	технология защиты информации в правоохранительной сфере
	информационно-аналитическое обеспечение правоохранительной деятельности
	оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации
Краснодарский университет МВД России	
10.05.05 Безопасность информационных технологий в правоохранительной сфере	технология защиты информации в правоохранительной сфере
Санкт-Петербургский университет МВД России	
10.05.05 Безопасность информационных технологий в правоохранительной сфере	компьютерная экспертиза
	технология защиты информации в правоохранительной сфере

3. Методические основы подготовки кадров по безопасности КИИ ОВД

Анализ организации подготовки кадров в ведомственных вузах МВД России позволяет сделать вывод о том, что процесс образовательной деятельности осуществляется на основе четырех действующих ФГОС ВО:

– 10.05.01 Компьютерная безопасность;
– 10.05.02 Информационная безопасность телекоммуникационных систем;
– 10.05.03 Информационная безопасность автоматизированных систем;
– 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Содержание специализаций в рамках реализуемых ФГОС ВО позволяют ограничить предмет исследования.

Так, профиль подготовки «Информационно-аналитическая и техническая экспертиза компьютерных систем» в рамках ФГОС ВО 10.05.01 Компьютерная

[19]Официальный сайт МосУ МВД России имени В.Я. Кикотя. URL: https://mvd.ru/upload/site116/folder_page/021/109/438/2023/PTsP_2024__na_sayt_1.pdf (дата обращения: 24.12.2023).

безопасность[20], а также профиль «Компьютерная экспертиза» в рамках ФГОС ВО 10.05.05 Безопасность информационных технологий в правоохранительной сфере[21] направлены на исследование совершившихся инцидентов. Таким образом, формируемые в рамках данных направлений подготовки компетенции связаны не с предотвращением, то есть защитой КИИ, а с изучением последствий атаки на информационную инфраструктуры.

Профиль подготовки «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации» в рамках ФГОС ВО 10.05.05 Безопасность информационных технологий в правоохранительной сфере направлен на приобретение «атакующих», а не защитных навыков. Оперативно техническое обеспечение предполагает работы в противоправной среде, где требуются навыки превентивного мероприятия, что противоречит принципам организации защиты КИИ.

Таким образом, защита КИИ ОВД обеспечивается подготовкой специалистов в рамках образовательных программ, представленных в табл. 4.

Таблица 4. Направления подготовки по безопасности КИИ ОВД

ФГОС ВО	Специализация / профиль подготовки
10.05.02 Информационная безопасность телекоммуникационных систем	сети специальной связи
10.05.03 Информационная безопасность автоматизированных систем	разработка автоматизированных систем в защищенном исполнении
10.05.05 Безопасность информационных технологий в правоохранительной сфере	технология защиты информации в правоохранительной сфере

Однако, даже поверхностное изучение квалификационных требований к выпускникам по обозначенным профилям подготовки, прошедшим обучение по обозначенным специальностям, вызывает определенные вопросы. Так, квалификационные требования по ТЗИ представляют урезанную характеристику специалистов по разработке автоматизированных систем в защищенном исполнении. Данное условие обосновано наводит на предположение об идентичности содержания образовательных программ и УМКД по двум обозначенным направлениям подготовки. Вместе с тем, содержательное наполнение специальности «Сети специальной связи» представлено в виде «урезанной» компетентностной модели специалиста по защите информации. Подобная позиция обосновывается ограниченностью понятия «специальная связь» в органах внутренних дел.

Изучение экосистемы образовательной подготовки кадров по обеспечению информационной безопасности [16, с. 26] позволяет сделать выводы, по которым образовательная парадигма «определяется на базе интеграции учебного, научно-исследовательского и производственного процессов и практикоориентированности обучения». Таким образом, обосновывается необходимость ориентации образовательной деятельности на потребность рынка труда. В нашем случае качество подготовки кадров по безопасности КИИ ОВД во многом зависит от точности и конкретизации заказа по уровню квалификации выпускника. Поэтому детализированные по критериям специальной

[20]Приказ Минобрнауки РФ от 26.11.2020 № 1459 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.01 Компьютерная безопасность» (Зарегистрировано в Минюсте РФ 15.02.2021 N 62491).

[21]Приказ Минобрнауки РФ от 26.11.2020 № 1461 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере» (Зарегистрировано в Минюсте РФ 22.12.2020 N 61703).

профессиональной подготовки выпускника квалификационные требования позволят определить содержательное наполнение, в первую очередь, вариативной части образовательного процесса.

Разработка концептуальной модели компетентности специалиста по обеспечению информационной безопасности [17, с. 57] позволяет содержательно наполнить отдельные виды компетенций и определить учебные дисциплины в соответствии с профилем подготовки квалифицированных специалистов.

Мы полагаем, что использование схожей модели в разработке программ для специалистов по безопасности КИИ ОВД повысит качество образовательного процесса.

Заключение

Проведенное предпроектное исследование в целях модернизации вариативной части образовательных программ по направлению информационная безопасность в рамках подготовки специалистов по безопасности КИИ ОВД позволяет сделать ряд выводов:

– Понятие КИИ ОВД в целом имеет нормативно-правовое обоснование.

– Информационные системы и ресурсы данных органов государственной службы в полной мере соответствуют статусу объекта КИИ.

– За обеспечение функционирования и безопасности объектов КИИ ОВД отвечает отдельное структурное подразделение МВД России.

– Обучение специалистов по обеспечению безопасности КИИ ОВД сосредоточено в вузах, находящихся в ведении МВД России.

– Содержание профессиональных образовательных программ основывается на требованиях ФГОС ВО и квалификационных требованиях к специальной профессиональной подготовке выпускника.

– Перспектива введения ФГОС ВО 4+ должна придать существенный импульс ведомственному образованию в вопросах не только разработки новых образовательных программ, гармонизированных с новыми стандартами, но и потребует от профессионального сообщества более основательно подойти к разработке новых квалификационных требований к специализированной профессиональной подготовке на основе вариативной части УМКД.

Несмотря на детальную формализацию образовательного процесса в системе ОВД, существуют ряд позиций, изменение которых позволит повысить уровень подготовки необходимых специалистов по обеспечению безопасности КИИ. Так изменение структуры и содержания квалификационных требований к специальной профессиональной подготовке выпускника позволит определить рамки образовательной подготовки, а содержательное наполнение профессиональных компетенций под задачи профессиональной деятельности обеспечит впоследствии детальную проработку вариативной части соответствующего УМКД.

СПИСОК ЛИТЕРАТУРЫ

1. Наталичев Роман В. и др. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. – EDN: JIMDXU.
2. Мельников Дмитрий А.; Гавдан Григорий П.; Корсаков Иван А. К вопросу о цели и задачах национальной образовательной инициативы сша в области кибербезопасности. Безопасность информационных технологий, [S.l.], т. 25, № 2, p. 23–37, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.2.02. – EDN: XRDYBF.

3. Завгородний Е.Н. Развитие системы обеспечения информационной безопасности в органах внутренних дел. StudNet. 2021, т. 4, № 7, с. 82. – EDN: PIWDUW.
4. Крупина М.А. Административно-правовые аспекты использования прикладных сервисов единой системы информационно-аналитического обеспечения деятельности Министерства внутренних дел Российской Федерации. Вестник Нижегородского университета им. Н.И. Лобачевского. 2023, № 2, с. 138–146. DOI: http://dx.doi.org/10.52452/19931778_2023_2_138. – EDN: VIKHLM.
5. Luswata J., Zavarsky P., Swar B. and Zvabva D. Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol. 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada. 2018, p. 1–5. DOI: 10.1109/BSC.2018.8494686.
6. Bárbara María Carvajal Hernández, I Silvia Colunga SantosII Manuel N. Montejo LorenzoIII «Information competence in professional training». Humanidades Médicas 2013;13(2), p. 526–545. URL: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-81202013000200013 (дата обращения: 13.12.2023).
7. Anupa Chaudhary and Sumit Prasad «Training for Development of Professional Education» 2018 International Journal of Innovation, Management and Technology. April 2018, v. 2, no. 2, p. 162–165. URL: https://www.researchgate.net/publication/338479269_Training_for_Development_of_Professional_Education (дата обращения: 13.12.2023).
8. Хорев А.А. Методический подход к формированию индикаторов компетенций в федеральном государственном образовательном стандарте высшего образования четвертого поколения по информационной безопасности. Методы и технические средства обеспечения безопасности информации. 2023, № 32, с. 178–180. – EDN: TDRIGU.
9. Ефремов А.Ф. Проблемы обеспечения информационной безопасности в системе МВД России при работе с базами данных. Вопросы российского и международного права. 2020, т. 10, № 11-1, с. 229–235. DOI: 10.34670/AR.2020.76.82.048. – EDN: MBHTUU.
10. Баторов Б.О. Некоторые проблемы нормативно-правового регулирования защиты информации в органах внутренних дел Российской Федерации и пути их разрешения. Труды Академии управления МВД России. 2022, № 2(62), с. 121–127. DOI: 10.24412/2072-9391-2022-262-121-127. – EDN EOCSJV.
11. Пашнин А.В. Информационное обеспечение Министерства внутренних дел Российской Федерации: характеристика и особенности. Безопасность дорожного движения. 2021, № 3, с. 79–82. – EDN: SZNKWH.
12. Воронич В.В., Грачев М.И., Локнов А.И., Примакин А.И. Подготовка и переподготовка кадров в области информационной безопасности для правоохранительных органов. Региональная информатика и информационная безопасность: Сборник трудов, Санкт-Петербург, 26–28 октября 2016 года. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. Том Выпуск 2. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2016, с. 80–84. – EDN XEYLMF.
13. Обеспечение информационной безопасности в органах внутренних дел: учебное пособие. Барнаул: Барнаульский юридический институт МВД России, 2019. – 63 с. URL: http://dot.kostacademy.kz/bible/files/480772721.pdf (дата обращения 13.12.2023).
14. Апульцин В.А., Гонов Ш.Х., Лебедев В.Н., Петрова В.Ю. Информационные технологии управления и организация защиты информации: курс лекций. М.: Академия управления МВД России. 2021. – 72 с. URL: https://mvd.ru/upload/site120/folder_page/015/122/996/Apultsin_Gonov_na_sayt.pdf (дата обращения: 13.12.2023).
15. Горбатов Виктор С.; Дураковский Анатолий П.; Лобанов Максим И. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 54–68, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.4.04. – EDN: FHLDCE.
16. Поляков В.В., Жданова Е.А. Экосистема опережающей подготовки кадров для сферы информационной безопасности. Проблемы правовой и технической защиты информации. 2022, № 10, с. 26–29. – EDN: CVEADO.
17. Васильева Д.С., Шабурова А.В. Модель компетентности специалиста по информационной безопасности в современных условиях. Интерэкспо Гео-Сибирь. 2020, т. 6, № 1, с. 53–59. DOI: 10.33764/2618-981X-2020-6-1-53-59. – EDN: NRRKLT.

REFERENCES:

[1] Natalichev Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 28, no. 3, p. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01 (in Russian). – EDN: JIMDXU.

[2] Melnikov Dmitriy A.; Gavdan Grigory P.; Korsakov Ivan A. To the issue about the purpose and objectives the USA National initiative for cybersecurity education. IT Security (Russia), [S.l.], v. 25, no. 2, p. 23–37, 2018. ISSN 2074-7136. – EDN: XRDYBF (in Russian).
[3] Zavgorodny E.N. Development of the information security system in the internal affairs bodies. StudNet. 2021, v. 4, no. 7, p. 82 (in Russian). – EDN PIWDUW.
[4] Krupina M.A. Administrative and legal aspects of the use of application services of the unified system of information and analytical support for the activities of the ministry of internal affairs of the russian federation. Bulletin of the Nizhny Novgorod University named after N.I. Lobachevsky. 2023, no. 2, p. 138–146. DOI: 10.52452/19931778_2023_2_138. – EDN: VIKHLM (in Russian).
[5] Luswata J., Zavarsky P., Swar B. and Zvabva D. Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol. 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada. 2018, p. 1–5. DOI: 10.1109/BSC.2018.8494686.
[6] Bárbara María Carvajal Hernández, I Silvia Colunga SantosII Manuel N. Montejo LorenzoIII «Information competence in professional training». Humanidades Médicas 2013;13(2), p. 526–545. URL: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-81202013000200013 (accessed: 13.12.2023).
[7] Anupa Chaudhary and Sumit Prasad «Training for Development of Professional Education» 2018 International Journal of Innovation, Management and Technology. April 2018, v. 2, no. 2, p. 162–165. URL: https://www.researchgate.net/publication/338479269_Training_for_Development_of_Professional_Education (accessed: 13.12.2023).
[8] Khorev A.A. Methodological approach to the formation of competence indicators in the federal state educational standard of higher education of the fourth generation on information security. Methods and technical means of ensuring information security. 2023, no. 32, p. 178–180 (in Russian). – EDN: TDRIGU.
[9] Efremov A.F. Problems of ensuring information security in the system of the Ministry of Internal Affairs of Russia when working with databases. Issues of Russian and international law. 2020, v. 10, no. 11-1, p. 229–235. DOI: 10.34670/AR.2020.76.82.048. – EDN: MBHTUU.
[10] Batorov B.O. Some problems of regulatory and legal regulationof information protection in the internal affairs bodiesof the russian federation and ways to resolve them. Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2022, № 2(62), p. 121–127. DOI: 10.24412/2072-9391-2022-262-121-127 (in Russian). – EDN: EOCSJV.
[11] Pashnin A.V. Information supply of the Ministry of the internal affairs of the Russian Federation: characteristics and features. Road safety. 2021, no. 3, p. 79–82 (in Russian). – EDN: SZNKWH.
[12] Voronich V.V., Grachev M.I., Loknov A.I., Primakin A.I. Training and retraining of personnel in the field of information security for law enforcement agencies. Regional Informatics and information security: Proceedings, St. Petersburg, October 26-28, 2016. St. Petersburg Society of Informatics, Computer Technology, Communication Systems and management. Volume Issue 2. St. Petersburg: St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems. 2016, p. 80–84. – EDN: XEYLMF (in Russian).
[13] Ensuring information security in the internal affairs bodies: a textbook. – Barnaul: Barnaul Law Institute of the Ministry of Internal Affairs of Russia, 2019. – 63 p. URL: http://dot.kostacademy.kz/bible/files/480772721.pdf (accessed: 13.12.2023) (in Russian).
[14] Apeltsin V.A., Gonov Sh.Kh., Lebedev V.N., Petrova V.Yu. Information technologies of management and organization of information protection: a course of lectures. M.: Academy of Management of the Ministry of Internal Affairs of Russia. 2021. – 72 p. URL: https://mvd.ru/upload/site120/folder_page/015/122/996/Apultsin_Gonov_na_sayt.pdf (accessed: 13.12.2023) (in Russian).
[15] Gorbatov Viktor S.; Durakovskiy Anatoly P.; Lobanov Maxim I. On professional standards for personnel training on safety of critical information infrastructure objects. IT Security (Russia), [S.l.], v. 26, no. 4, p. 54–68, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.04 (in Russian). – EDN: FHLDCE.
[16] Polyakov V.V., Zhdanova E.A. Ecosystem of advanced training for the field of information security. Problems of legal and technical protection of information. 2022, no. 10, p. 26–29 (in Russian). – EDN: CVEADO.
[17] Vasilyeva D.S., Shaburova A.V. Competence model of an information security specialist in modern conditions. Interexpo Geo-Siberia. 2020, v. 6, no. 1, p. 53–59. DOI: 10.33764/2618-981X-2020-6-1-53-59 (in Russian). – EDN: NRRKLT.

Поступила в редакцию – 25 декабря 2023 г. Окончательный вариант – 10 февраля 2024 г.
Received – December 25, 2023. The final version – February 10, 2024.