НОВЫЕ ТЕХНОЛОГИИ

DOI: 10.22394/2070-8378-2020-22-6-46-56

Квалификационные требования к государственным служащим в модели цифровых компетенций

НАДЕЖДА МИХАЙЛОВНА СЛАДКОВА, кандидат педагогических наук, директор по развитию
Всероссийский научно-исследовательский институт труда Министерства труда и социальной защиты Российской Федерации (Российская Федерация, 105043, Москва, ул. 4-я Парковая, 29). E-mail: n.sladkova@vcot.info

АНДРЕЙ АЛЕКСАНДРОВИЧ СТЕПАНЕНКО, старший аналитик
Всероссийский научно-исследовательский институт труда Министерства труда и социальной защиты Российской Федерации (Российская Федерация, 105043, Москва, ул. 4-я Парковая, 29). E-mail: andrew.a.stepanenko@gmail.com

ОЛЬГА АЛЕКСАНДРОВНА ИЛЬЧЕНКО, руководитель проектов
Всероссийский научно-исследовательский институт труда Министерства труда и социальной защиты Российской Федерации (Российская Федерация, 105043, Москва, ул. 4-я Парковая, 29). E-mail: o.ilchenko@vcot.info

ВИТАЛИЙ АНАТОЛЬЕВИЧ ШАПОШНИКОВ, кандидат физико-математических наук, заместитель начальника учебно-методического отдела автономной некоммерческой организации дополнительного профессионального образования Центр повышения квалификации «АИС», старший аналитик
Всероссийский научно-исследовательский институт труда Министерства труда и социальной защиты Российской Федерации (Российская Федерация, 105043, Москва, ул. 4-я Парковая, 29). E-mail: Shaposhnikov.Vitalij@yandex.ru

Аннотация: В статье представлено описание подходов к формированию модели цифровых компетенций, принятой за основу G20 в 2016 году, и определению места и роли в ней квалификационных требований по информационной безопасности государственных гражданских служащих. Обосновывается необходимость разработки единого инструментария оценки степени готовности обеспечения информационной безопасности государственными гражданскими служащими.
Ключевые слова: информационная безопасность, государственная служба, квалификационные требования, компетенции по информационной безопасности, модель цифровых компетенций, оценка государственных служащих
Благодарность. Исследование выполнено в рамках государственного задания по теме: «Разработка методического аппарата оценки степени подготовленности государственных гражданских служащих в сфере обеспечения информационной безопасности», 2019–2020 годы

Статья поступила в редакцию 7 сентября 2020 года.

Сладкова Н.М., Степаненко А.А., Ильченко О.А., Шапошников В.А. Квалификационные требования к государственным служащим в модели цифровых компетенций. *Государственная служба*. 2020. № 6. С. 46–56.

QUALIFICATION REQUIREMENTS FOR CIVIL SERVANTS IN THE DIGITAL COMPETENCE MODEL

NADEZHDA MIKHAILOVNA SLADKOVA, Candidate of Sci. (Pedagogy), Development Director
FSBI "All-Russian Scientific-Research Institute of Labor" of the Ministry of Labor and Social Protection of the Russian Federation (29, 4-th Parkovaya St., Moscow, 105043, Russian Federation). E-mail: n.sladkova@vcot.info

ANDREY ALEXANDROVICH STEPANENKO, Senior Analyst
FSBI "All-Russian Scientific-Research Institute of Labor" of the Ministry of Labor and Social Protection of the Russian Federation (29, 4-th Parkovaya St., Moscow, 105043, Russian Federation). E-mail: andrew.a.stepanenko@gmail.com

OLGA ALEKSANDROVNA ILCHENKO, Project Manager
FSBI "All-Russian Scientific-Research Institute of Labor" of the Ministry of Labor and Social Protection of the Russian Federation (29, 4-th Parkovaya St., Moscow, 105043, Russian Federation). E-mail: o.ilchenko@vcot.info

VITALY ANATOLYEVICH SHAPOSHNIKOV, Candidate of Sci. (Physics and Mathematics), Deputy Head of the Educational and Methodological Department of the ANO DPO Central Research Center "AIS", Senior Analyst
FSBI "All-Russian Scientific-Research Institute of Labor" of the Ministry of Labor and Social Protection of the Russian Federation (29, 4-th Parkovaya St., Moscow, 105043, Russian Federation). E-mail: Shaposhnikov.Vitalij@yandex.ru

Abstract: The article describes the approaches to the formation of the digital competence model, adopted as the basis for the G20 in 2016, and determine the place and role of qualification requirements for civil servants regarding information security. The paper argues for the need to develop a unified toolkit for assessing the level of preparedness of state civil servants in the field of information security.
Keywords: information security, civil service, qualification requirements, information security competencies, digital competency model, assessment of civil servants
Acknowledgment. The research was carried out within the framework of the state task on the topic: "Development of a methodological tool for assessing the level of preparedness of state civil servants in the field of information security", 2019 – 2020.

The article was received on September 7, 2020.

Sladkova N.M., Stepanenko A.A., Ilchenko O.A., Shaposhnikov V.A. Qualification requirements for civil servants in the digital competence model. *Gosudarstvennaya sluzhba*. 2020. No. 6. P. 46–56.

Введение

Переход к цифровизации в экономике требует перестройки процессов в ОГВ и компетенций госслужащих[1]. Одним из необходимых качеств работника в период цифровизации во всех сферах деятельности, включая госслужбу, является навык работы с информацией[2] как специфическим предметом труда.

Автоматизация основных процессов деятельности государственных органов власти становится все более распространенной практикой. По опросу, проведенному в 2018 году исследователями Финансового университета при Правительстве Российской Федерации [Васильева, Пуляева, Юдина, 2018. С. 28–42], госслужащими используется целый ряд информационных систем, в том числе Единая информационная система управления кадровым составом государственной гражданской службы РФ (15 % опрошенных), «1С: Кадры (Предприятие)» (10 %); автоматизированная информационная система (далее – АИС) «Кадры Минэкономразвития России», «КонсультантПлюс» (по 4 %), Lotus, АИС «Управление персоналом государственных органов Санкт-Петербурга», «Парус», программный комплекс Аксиок.Net, Смета-кадры (по 2 %), Федеральный портал госслужбы и управленческих кадров и др.

В этой связи становится актуальным вопрос наличия у госслужащих сформированных навыков работы с информацией в цифровой среде, «способности использовать цифровые технологии, инструменты коммуникации и/или сети для получения доступа к информации, управления ею, интеграции, оценивания, создания и передачи информации с соблюдением этических и правовых норм для того, чтобы успешно жить и трудиться в условиях общества знаний» [Digital Transformation…, 2002. С. 5].

В соответствии с моделью цифровых компетенций [Digital Transformation…, 2002. С. 18], включающей перечень необходимых знаний, умений / навыков и мотивационных установок работника в области компьютерной, коммуникативной, медиа, технологической грамотности, Международным советом по ИКТ-компетентности выделяется важность навыков обеспечения информационной безопасности при реализации всех этапов работы с информацией в цифровом пространстве на любом рабочем месте.

Требования к модели и выбору инструментов оценки цифровых компетенций (в том числе для госслужащих) начали обсуждаться в российском экспертном сообществе еще в период разработки и далее на этапе последующего введения в действие программы «Цифровая экономика» [Baimuratova, Dolgova, Imaeva et al., 2018].

Важность выделения в общей модели компетенций государственных служащих блока цифровых компетенций и деления соответствующих квалификационных требований на три уровня – базовые, продвинутые и специальные – подчеркивается исследователями [Васильева, Пуляева, Юдина, 2018. С. 35]. Однако в существующих подходах к описанию цифровых компетенций государственных гражданских служащих отсутствуют отдельно выделенные требования к навыкам обеспечения информационной безопасности. Это ограничивает фокусировку на них, практически исключает необходимость создания средств измерения уровня развития навыков в данной области, а в дальнейшем и их развития.

Следует отметить, что зарубежная практика организации деятельности государственных органов власти во внешней и внутренней информационной среде демонстрирует сложившуюся технологию в предупреждении информационных рисков и инцидентов (Computer Security Act of 1987 (Public Law 100-235), руководство по организации обучения информационной безопасности для государственных служащих NIST Special Publication 500-172 «Computer Security Training Guidelines»[3] и др.). Реализуемые мероприятия направлены на формирование комплекса знаний, умений, поведенческих стереотипов государственных служащих как одного из важнейших факторов обеспечения информационной безопасности.

Для разработки пакета оценочных средств и методики проведения оценки готовности государственных гражданских служащих к обеспечению информационной безопасности были исследованы существующие зарубежные практики работы в области оценки и развития служащих государственного сектора, сформированы подходы к выделению квалификационных требований по обеспечению информационной безопасности на основе цифровой модели компетенций.

Обеспечение информационной безопасности госсектора в мировой практике

Понимание того, что проблема обеспечения информационной безопасности в организациях как государственного, так и частного секторов является основой национальной безопасности Соединенных Штатов Америки, возникло еще до того, как цифровизация стала одним из мировых трендов и до того, как была разработана основа модели цифровых компетенций, принятая в 2016 году на G20. Анализ нормативных актов, регулирующих деятельность в этой области, позволил выделить три этапа, последовательно углубляющих степень проработки проблемы.

1 Паспорт национальной программы «Цифровая экономика Российской Федерации». https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf

2 The Global Competitiveness Report 2015, World Economic Forum. https://www.weforum.org/reports/global-competitiveness-report-2015

3 NIST Special Publication 500-172 «Computer Security Training Guidelines», 1989. https://csrc.nist.gov/publications/detail/sp/500-172/archive/1989-11-01

1 этап (1987–1997 годы). Обозначение проблемы и общих подходов к ее решению

Отправной точкой анализа стал Computer Security Act of 1987 (Public Law 100-235), первый документ, в котором была обозначена важность информационной безопасности в государственном секторе США. Целью Акта было определение минимально допустимого уровня мер обеспечения информационной безопасности в государственных компьютерных системах США, что позволило сформулировать требования к базовому уровню безопасности информации. В данном документе впервые на законодательном уровне было сформулировано требование к обучению всего персонала основам информационной безопасности для снижения влияния человеческого фактора (случайных ошибок, непреднамеренных нарушений правил информационной безопасности и т.п.) на общий уровень информационной безопасности.

На основании положений данного закона Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) разработал руководство по организации обучения информационной безопасности для государственных служащих NIST Special Publication 500-172 «Computer Security Training Guidelines», 1989 [Digital skills..., 2019], определяющее области и уровень получаемых знаний для различных категорий персонала (**рисунок 1**), которое стало обязательным для всех государственных структур США.

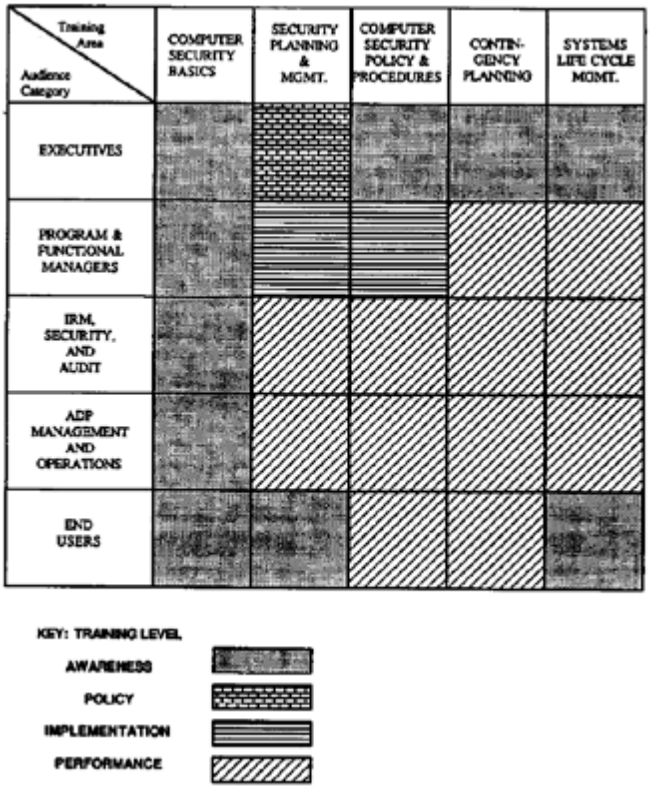
На протяжении почти 10 лет это руководство использовалось при планировании обучения персонала сначала государственных, а затем и коммерческих организаций США основам информационной безопасности.

2 этап (1998–2010 годы). Детализация требований по безопасности государственных систем и формирование модели компетенций для стандартизации требований к квалификации в области информационной безопасности

На основании накопленного на первом этапе опыта специалистами NIST был разработан новый подход к определению требуемых для различных категорий персонала компетенций в области информационной безопасности. Документ NIST Special Publication 800-16 «Information Technology Security Training Requirements: A Role- and Performance- Based Model», 1998, определил требования по обучению, предъявляемые не к конкретным должностным позициям, а к функциональным ролям (обязанностям) персонала, работающего с защищаемой информацией, и содержал две важные новации: разделение персонала организации на несколько типовых ролей сотрудников (в зависимости от необходимого объема знаний) и определение трех уровней квалификации для руководителей непрофильных подразделений и специалистов по информационным технологиям и информационной безопасности: начальный, средний и расширенный (**рисунок 2**).

Рисунок 1. Матрица обучения NIST SP 500-172[1]

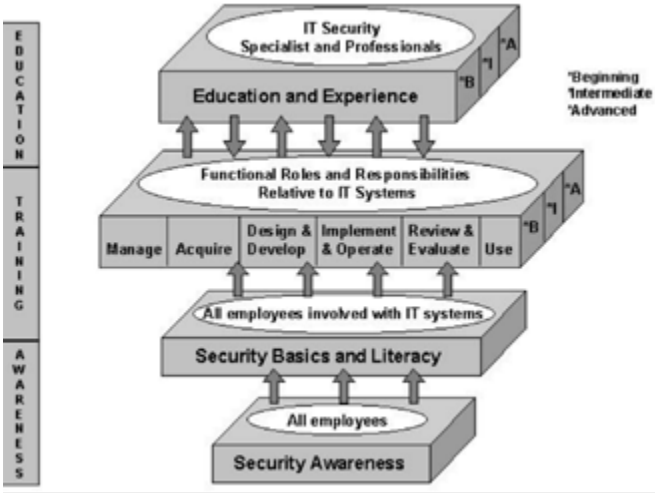
Figure 1. NIST SP 500-172 Training Matrix



1 NIST. https://www.nist.gov/

Рисунок 2. Непрерывное обучение информационной безопасности NIST SP 800-16[1]

Figure 2. NIST SP 800-16 IT Security Learning Continuum



1 NIST. https://www.nist.gov/

Для каждого уровня обучения в документе были определены рекомендуемые перечни изучаемых тем, наиболее подходящие методы обучения, а также типы тестовых (оценочных) средств, используемых для контроля полученных знаний, умений и навыков.

Переход США к концепции электронного правительства сопровождался разработкой целого ряда нормативных документов, в которых вопросам информационной безопасности было уделено повышенное внимание. В частности, в E-Government Act of 2002 (Public Law 107–347) в разделе III Federal Information Security Management Act of 2002 (FISMA) в дополнение к ранее выдвигаемым требованиям по обучению было закреплено введение обязательного периодического тестирования знаний и проверки эффективности выполнения сотрудниками политик и процедур информационной безопасности. Эти требования в дальнейшем были детализированы в документе Office of Management and Budget (OMB) Circular A-130, Appendix III «Security of Federal Automated Information Resources».

Следует отметить, что большинство мер тестирования знаний касалось только тех категорий сотрудников, для которых информационная безопасность не является их специализацией. Отчасти это было связано с достаточно высокой технической сложностью предметной области «информационная безопасность» и связанной с этим сложностью требуемых оценочных средств.

На протяжении ряда лет в США предпринимались попытки привлечения к процессу оценки квалификации специалистов по информационной безопасности независимых организаций. В итоге был сформирован перечень организаций, специализирующихся на сертификации специалистов, и определены типы сертификатов, обладание которыми будет признаваться в качестве подтверждения квалификации специалистов по информационной безопасности. Перечень был впервые утвержден меморандумом для всех государственных организаций США от 13 августа 2008 года “Fact Sheet on Certification and Certificate Programs”, разработанным U.S. Office of Personnel Management.

3 этап (2011 – н.в.). Общегосударственная инициатива по обучению и единая модель компетенций в области информационной безопасности

Следующим важным этапом стало формирование общегосударственной модели компетенций для профильных специалистов в области информационной безопасности. Впервые модель была представлена в документе “Competency Model of Cybersecurity”, разработанном в 2011 году U.S. Office of Personnel Management. Предложенный в документе подход определил наборы компетенций, необходимых ИБ-специалистам нескольких профилей, имеющих различные грейды, и стал первой попыткой стандартизации трудовых функций, выполняемых ИБ-специалистами, унификации требований к их начальной квалификации и определения потребностей в их дополнительном обучении.

Развитием данного подхода, расширенного до всех пользователей информационных систем, стала общегосударственная инициатива США по обучению в области информационной безопасности National Initiative for Cybersecurity Education (NICE). В рамках этой инициативы в 2017 году был разработан документ NIST Special Publication 800-181 “National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework”, который вводит более развитую модель компетенций специалистов по информационной безопасности, выполняющих трудовые функции различных специальностей и ролей. Всего в документе выделены 52 функциональные роли (специализации) работников, занимающихся обеспечением информационной безопасности.

В ЕС работа в области цифровой грамотности населения проводится через создание национальных коалиций по развитию новых умений. Сейчас в ЕС насчитывается 18 таких национальных коалиций, в которых задействованы более 300 участников-разработчиков и более 7 млн граждан. План по развитию цифровых навыков включает 11 мероприятий по использованию инструмента самоанализа SELFIE. В 2018 году создана новая рабочая группа «Цифровое образование, обучение, преподавание, оценивание».

В рекомендациях для граждан ЕС 2018 года [Цифровые навыки…, 2019. С. 22] при определении необходимых знаний и навыков в области информационной безопасности акцент делается на угрозы кибербезопасности в отношении личной информации и связанных с нею рисков – ложных новостей, кибербуллинга и радикализации. В качестве критического риска отмечается нарушение информационной безопасности в системе государственного управления.

Ежегодно, начиная с 2011 года, ENISA проводит в Европе месяц кибербезопасности (European Cyber Security Month), основными мероприятиями которого являются различные тренинги для студентов, граждан Евросоюза, технических экспертов, государственных и частных организаций.

Интересным и масштабным представляется опыт ENISA по реализации программы общеевропейских учений под названием Cyber Europe по управлению кибернетическими инцидентами и кризисами на уровне ЕС для государственного и частного секторов из стран – членов ЕС и ЕАСТ. Технология, лежащая в основе программы, предполагает моделирование масштабных инцидентов кибербезопасности, которые могут перерасти в киберкризисы. Учения предлагают захватывающие сценарии, основанные на реальных событиях, разработанных европейскими экспертами по кибербезопасности. В 2020 году в основу активности положен сценарий[4], связанный со

4 CYBER EUROPE 2020. The European Union Agency for Cybersecurity ENISA. https://www.cyber-europe.eu/img/CE2020_presentation.pdf

здравоохранением, в котором задействуются министерства здравоохранения, больницы, клиники, лаборатории, поставщики электронных услуг здравоохранения. Инциденты перерастают в кризис на всех уровнях: местном, организационном, национальном, европейском. Готовность к обеспечению информационной безопасности, непрерывности бизнеса и процедуры кризисного управления проверяются в игровом, приближенном к реальному, формате.

По итогам исследования уровня цифровой грамотности [Baimuratova, Dolgova, Imaeva et al., 2018], проведенного в 2018 году аналитическим центром НАФИ, которое основано на системе, предложенной в рамках саммита «Группы двадцати» (G20) в апреле 2017 года[5], цифровая грамотность оценивается по пяти направлениям, внутри каждого из которых выделяются три группы требований – к знаниям, навыкам и установкам:

- информационная грамотность;
- компьютерная грамотность;
- медиаграмотность;
- коммуникативная грамотность;
- отношение к технологическим инновациям.

В качестве еще одного примера приведем опыт Канады, здесь Совет по информационно-коммуникационным технологиям описывает модель компетенций, состоящую из детализированных по отдельным характеристикам пяти групп навыков [Skills in the digital economy, 2016. С. 21–24]:

- базовые навыки;
- деловые и межличностные навыки;
- цифровые и технические навыки;
- информационные навыки;
- предпринимательские навыки (включая цифровое предпринимательство).

Анализ зарубежной практики в области совершенствования навыков информационной безопасности в организациях государственного сектора позволил сформировать следующие подходы:

Квалификационные требования по информационной безопасности должны формироваться для нескольких целевых групп госслужащих (в зависимости от степени их вовлеченности в процессы обеспечения информбезопасности, например, специалисты по информационной безопасности, ИТ-специалисты, руководители всех уровней, все остальные госслужащие).

В условиях перехода к цифровой экономике детализация требований по информационной безопасности должна осуществляться с учетом модели требований к информационной безопасности в условиях цифровизации, разработанной на основе концептуальной схемы компетенций в цифровой экономике, предложенной G20.

Квалификационные требования по обеспечению информационной безопасности в модели цифровых компетенций

Согласно версии 3.2 «Методического инструментария по установлению квалификационных требований для замещения должностей государственной гражданской службы»[6], разработанного Министерством труда и социальной защиты РФ документа рекомендательного характера, к квалификационным требованиям относят базовые и профессионально-функциональные (в свою очередь подразделяющиеся на профессиональные и функциональные) требования к образованию, стажу, знаниям и умениям (таблица 1). К базовым, то есть не зависящим от видов деятельности, требованиям к знаниям и умениям относят знание законодательства (основ Конституции Российской Федерации, законодательства о гражданской службе, законодательства о противодействии коррупции); знание русского языка; знания и умения в области информационно-коммуникационных технологий; общие и управленческие умения, свидетельствующие о наличии необходимых профессиональных и личностных качеств (компетенций).

Система квалификационных требований/ Qualification requirements System

Квалификационные требования в области информационной безопасности находятся на стыке знаний законодательства РФ и знаний и умений в области информационно-коммуникационных технологий и имеют определенную специфику для различных должностей. Исходя из этого, было предложено определить две укрупненные целевые группы по должностям государственных гражданских служащих по отношению к информационной безопасности, для которых необходимо сформировать перечни компетенций. Укрупненная группа А – служащие-пользователи и укрупненная группа Б – служащие – специалисты в области информационных технологий, в частности, информационной безопасности.

Служащие из группы А должны знать требования законодательства к их должности в области информационной безопасности, инструкции по ИБ, владеть правилами использования ИТ-технологий, инструментов и т.п.

Для служащих группы Б обеспечение информбезопасности является основным функционалом должности, что предусматривает расширенные требования к их квалификации в обозначенной области.

Таким образом, к пользователям и профессиональным специалистам должны предъявляться разные требования по обеспечению информационной безопасности.

5 Bridging the Digital Divide: Measuring Digital Literacy. G20 Insights, 2017. https://www.g20-insights.org/policy_briefs/bridging-digital-divide-measuring-digital-literacy/

6 Методический инструментарий по установлению квалификационных требований для замещения должностей государственной гражданской службы, версия 3.2. https://www.garant.ru/products/ipo/prime/doc/71755218/

Таблица 1. Методический инструментарий по квалификационным требованиям

Table 1. Methodological tools for qualification requirements

	Квалификационные требования		
	Базовые	Профессионально-функциональные	
		Профессиональные	Функциональные
Образование	уровень образования	специальность (направление подготовки) профессионального образования	–
	ст. 12 Федерального закона № 79-ФЗ	ст. 12 Федерального закона № 79-ФЗ + справочник	
Стаж	продолжительность	по специальности (направлению подготовки)	–
	Указ Президента Российской Федерации № 16 / закон субъекта Российской Федерации		
Знания и умения	Законодательство: Конституция Российской Федерации; государственная служба; противодействие коррупции	в зависимости от области и вида деятельности	в зависимости от функциональных обязанностей
	Русский язык		
	Информационно-коммуникационные технологии		
	Общие и управленческие умения Профессиональные и личностные качества (компетенции)		

Поскольку для руководителей разного уровня и для «рядовых» сотрудников должен обеспечиваться разный уровень доступа к информации, то целесообразно разделить укрупненную группу служащих – пользователей ИТ-технологий на две группы – А1 и А2:

- группа А1: все гражданские служащие (кроме ИТ-специалистов, специалистов по информационной безопасности и руководителей);
- группа А2: руководители всех уровней.

Требования к направлению подготовки (специальности) профессионального образования государственных гражданских служащих группы А определяются требованиями к замещению должности, квалификационные требования по ИБ являются дополнительными.

Укрупненную группу Б также можно разделить на группы Б1 и Б2:

Группа Б1: ИТ-специалисты с квалификацией по информационным технологиям, задействованные в процессах обеспечения информбезопасности. Этой группе служащих требуется специализированная подготовка по укрупненным группам специальностей и направлений подготовки (УГСНП): «Компьютерные и информационные науки», «Информатика и вычислительная техника», «Электроника, радиотехника и системы связи». Подготовка ИТ-специалистов по учебным дисциплинам в области информационной безопасности предусмотрена соответствующими образовательными стандартами.

Группа Б2: специалисты по информационной безопасности. Данной группе госслужащих требуется обязательная специализированная подготовка по укрупненной группе специальностей и направлений подготовки «Информационная безопасность».

В соответствии с системой квалификационных требований (**таблица 1**) компетенции в области информационной безопасности:

- для всех категорий госслужащих (группы А и Б) относятся к базовым квалификационным требованиям, находящимся на стыке знаний законодательства РФ и знаний и умений в области информационно-коммуникационных технологий;
- для госслужащих, непосредственно занимающихся обеспечением информационной безопасности в органах государственной власти (группы Б1 и Б2), дополнительно составляют часть профессионально-функциональных квалификационных требований.

В рамках исследования были проанализированы более 30 нормативных актов, разработанных Федеральной службой по техническому и экспортному контролю (ФСТЭК) России, ФСБ России, Центральным Банком России и Минтруда России, которые прямо или косвенно фиксируют требования к квалификации и уровню знаний в области информационной безопасности. Наиболее полно вопросы компетенций в области информационной безопасности прописаны в документах ФСТЭК России для государственных информационных систем[7] и для объектов критической информационной инфраструктуры[8]. Дополнительно

7 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 года № 17 (в ред. приказа ФСТЭК России от 15 февраля 2017 года № 27).

8 Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Утверждены приказом ФСТЭК России от 21 декабря 2017 года № 235; Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом ФСТЭК России от 25 декабря 2017 года № 239 (в ред. приказа ФСТЭК России от 9 августа 2018 года № 138 и приказа ФСТЭК России от 26 марта 2019 года № 60).

следует отметить документы ФСБ России и Национального координационного центра по компьютерным инцидентам (НКЦКИ)[9], регламентирующих работу Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), которые имеют ограничительную пометку «Для служебного пользования».

Анализ указанных документов позволил сделать вывод, что в целом прослеживается аналогичный принятому в США подход к разделению на требования к общему повышению осведомленности по информационной безопасности для всех работников и требования, предъявляемые к профильным специалистам. Нормативное регулирование в данной области по степени проработки проблемы предположительно соответствует середине 2-го этапа в США.

Следует отметить, что формирование детализированных перечней компетенций по информационной безопасности для различных целевых групп и их последующее согласование и утверждение на текущем уровне развития нормативно-правовой базы не регламентировано и крайне затруднено.

В связи с отсутствием единого документа, объединяющего и систематизирующего все необходимые требования по информационной безопасности, при разработке общей модели компетенций (**таблица 2**) были выделены квалификационные требования, сформулированные в разных нормативно-правовых актах и соответствующие доменам модели цифровых компетенций G20[10].

Содержательную основу модели компетенции «Информационная безопасность» составили знания и умения, приведенные в Справочнике квалификационных требований к специальностям, направлениям подготовки, знаниям и умениям, необходимые для замещения должностей с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих[11].

Требование обеспечения информационной безопасности относится к числу важнейших требований, включенных в Справочник. Этим объясняется, в частности, и включение требования знания основных нормативных правовых актов по информационной безопасности в профессионально-функциональные квалификационные требования в самостоятельном разделе «П.16.2. Вид профессиональной служебной деятельности “Регулирование в сфере обеспечения информационной и сетевой безопасности”» этого Справочника.

В предложенной модели компетенции «Информационная безопасность» каждая целевая группа имеет свой перечень требований к знаниям и умениям госслужащих по информационной безопасности.

Для обеспечения информационной грамотности каждый служащий из группы А должен владеть базовым понятийным аппаратом информационной безопасности, знать и применять в повседневной деятельности:

- требования законодательства РФ: основные законы; специальные, ведомственные нормативно-правовые акты в отношении разных видов служебной информации, степени ответственности за нарушение требований по работе со служебной информацией;
- правила информационной безопасности и защиты информации и безопасной работы с ИТ-сетью, ПК, копировальными аппаратами и другими техническими средствами.

Компьютерная грамотность любого служащего группы А должна быть на уровне знаний и пользовательского применения:

- основы безопасной работы с использованием средств автоматизации (выбор, установление, смена, сохранность пароля на служебном ПК; использование флеш-карт, копировальных и других устройств);
- правил информационной безопасности на своем рабочем месте и в процессе работы с внешними инстанциями.

Медиаграмотность является существенной компетенцией госслужащих группы А, отражающей знания и умения:

- пользования поисковыми системами в информационной сети Интернет для получения информации для подготовки служебных документов;
- получения информации из правовых баз данных, федерального портала проектов нормативных правовых актов;
- поиска информации при обязательной проверке ее на достоверность и полноту.

Коммуникативная грамотность служащих из группы А отражает знания и пользовательское применение:

- правил обращения и приемов по безопасности информации при работе со служебной информацией, включая правила использования электронной подписи, кодов, ключей и т. д.;

9 Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Регламентирующий документ ФСБ России от 27 декабря 2016 года (документ ограниченного доступа); Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Регламентирующий документ НКЦКИ (документ ограниченного доступа).

10 Bridging the Digital Divide: Measuring Digital Literacy. G20 Insights, 2017. https://www.g20-insights.org/policy_briefs/bridging-digital-divide-measuring-digital-literacy/

11 О подготовке Справочника в соответствии с частью 8 статьи 12 Федерального закона от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» было объявлено в письме Минтруда России от 26 апреля 2017 года № 18-1/10/В-3260. Обновленная версия Справочника подготовлена на основе предложений государственных органов, поступивших в Минтруд России в 2018 года – I квартале 2019 года.

Таблица 2. Модель требований к информационной безопасности с учетом квалификационных требований, согласованных с Минтрудом России. Составлено авторами

Table 2. Model of information security requirements based on qualification requirements agreed with the Ministry of labor of Russia. Compiled by the authors

Предметная область требований	Знания	Умения
А. Информационная грамотность	Глоссарий по цифровизации и информационной безопасности	Применение правил безопасной работы с разными видами служебной информации, каналами получения и распространения информации
	Законодательство РФ	
	Основные НПА	
	Специальные НПА	
	Ведомственные НПА	
	Национальные, межгосударственные и международные стандарты в области информационной безопасности	
	Основы информационной безопасности и защиты информации, в том числе по работе со служебной информацией	
	Основные угрозы безопасности информации	Формирование требований по информационной безопасности, разработка положений, инструкций, регламентов для специалистов ИТ и ИБ
	Модель нарушителя и принципы формирования политики безопасности	
Б. Компьютерная грамотность	Основы безопасной работы с использованием средств автоматизации	Соблюдение правил информационной безопасности при работе на ПК, в сети, с флеш-носителями и др.
	Основы защиты информации в операционных системах, базах данных и сетях	Установка и оптимальное использование встроенных средств защиты
	Технологии защиты информации:	Установка, обеспечение сохранности (исключение потери и дублирования), использование пароля на служебном ПК. Разработка правил и проверка электронной подписи
	- идентификация, аутентификация и авторизация, в том числе правила использования паролей на служебном ПК;	
	- защита от НСД;	Внедрение и настройка средств защиты Эксплуатация средств защиты
	- защита от вредоносного кода;	
	- сетевая безопасность;	
	- защита от атак;	
	- управление уязвимостями; - криптографическая защита информации; - резервное копирование;	
	- защита от утечек по техническим каналам	
	Построение защищенных систем и сетей	Проектировка, внедрение, аттестация, аудит защищенных систем
	Управление информационной безопасностью	Эксплуатация защищенной информационной системы
	Контроль и аудит информационной безопасности	
В. Медиаграмотность	Пользование поисковыми системами в информационной сети Интернет	Поиск и получение информации (PRAVO.GOV.RU); поиск и проверка достоверности и полноты информации, полученной из Интернета
	Получение информации из правовых баз данных, федерального портала проектов нормативных правовых актов	
Г. Коммуникативная грамотность	Правила безопасности информации при работе со служебной информацией и использовании информационно-телекоммуникационной сети Интернет; со служебной электронной почтой и служебными ПК	Формирование правил по информационной безопасности, разработка положений, инструкций, регламентов для пользователей, в том числе по работе: - с электронной подписью; - в сети Интернет; - с персональными данными. Проведение внутренних семинаров по коммуникативной грамотности для пользователей. Соблюдение правил ИБ
	Работа в системе межведомственного и ведомственного электронного документооборота, информационно-телекоммуникационных сетях	Соблюдение правил работы в системах и сетях
Д. Грамотность по технологическим инновациям	Мировые тенденции развития цифровизации	Грамотность и безопасность работы с новыми технологиями

- правил обращения и приемов по безопасности в использовании информационно-телекоммуникационной сети Интернет, в социальных сетях, при обращении со ссылками, для предупреждения заноса вирусов, при использовании информации, содержащей персональные данные.

Требования к грамотности по технологическим инновациям служащих группы А определяют действия пользователя по отношению к использованию новых, предлагаемых к распространению на открытом рынке ИТ-технологий и устройств, и ответственность за риск несанкционированного доступа к служебной информации через новое устройство или ПО.

Для обеспечения *информационной грамотности* специалисты по ИТ и информационной безопасности (группа Б) должны владеть полным понятийным аппаратом в области ИБ, знать и применять (в части, их касающейся) в повседневной деятельности:

- требования законодательства РФ: основные законы; специальные, ведомственные нормативно-правовые акты;
- национальные, межгосударственные и международные стандарты в области информационной безопасности;
- основные угрозы безопасности информации;
- модель нарушителя и принципы формирования политики безопасности;
- правила информационной безопасности и защиты информации и безопасной работы с ИТ-сетью, ПК, копировальными аппаратами и другими устройствами;
- технологию формирования требований к информационной безопасности в органах государственной власти.

Компьютерная грамотность любого госслужащего группы Б должна включать следующие знания и умения:

- основы безопасной работы с использованием средств автоматизации;
- основы защиты информации в операционных системах, базах данных и сетях;
- правила информационной безопасности на своем рабочем месте и в процессе работы с внешними инстанциями;
- использование встроенных средств защиты;
- внедрение и настройка средств защиты;
- эксплуатация средств защиты;
- проектирование, внедрение и аттестация защищенных систем;
- эксплуатация защищенной информационной системы;
- технологии защиты информации:
- идентификация, аутентификация и авторизация;
- защита от несанкционированного доступа;
- защита от вредоносного кода;
- сетевая безопасность;
- управление уязвимостями;
- криптографическая защита информации;
- резервное копирование;
- защита от утечек по техническим каналам.

Медиаграмотность служащих группы Б отражает следующие знания и умения:

- пользование поисковыми системами в информационно-коммуникационной сети Интернет;
- получение информации из правовых баз данных, федерального портала проектов нормативных правовых актов;
- поиск информации при обязательной проверке ее на достоверность и полноту.

Коммуникативная грамотность специалистов группы Б отражает требования к знаниям и их применению в области:

- контроля соблюдения правил работы в системах и сетях всех госслужащих;
- правил обращения и приемов по безопасности информации при работе со служебной информацией;
- правил обращения и приемов по безопасности в использовании информационно-телекоммуникационной сети Интернет;
- требований к системе межведомственного и ведомственного электронного документооборота, информационно-телекоммуникационным сетям, организации юридически значимого документооборота[12];
- корректного применения электронной подписи (проверка электронной подписи).

Грамотность в использовании / применении технологических инноваций ИТ-специалистов и специалистов по информационной безопасности распространяется на требования проактивно изучать, знать мировые тенденции в области цифровизации, обеспечивать безопасность введения в практику пользования госслужащими нового программного обеспечения, технологии или устройства.

В целом модель компетенции «Информационная безопасность» (**таблица 2**) является достаточно общей и отражает место компетенций по информационной безопасности в модели цифровых компе-

12 Постановление Правительства Российской Федерации от 28 декабря 2011 года № 1184 (ред. от 2 февраля 2019 года) «О мерах по обеспечению перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде» (вместе с «Правилами обеспечения перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде при предоставлении государственных услуг»).

Рисунок 3. Корреляция уровня развития компетенций госслужащих по информационной безопасности со степенью зрелости процессов обеспечения информационной безопасности в органе государственной власти (ОГВ). Составлено авторами

Figure 3. Correlation of the level of development of civil servants' competencies in information security with the degree of maturity of information security processes in the state authorities (ОГВ). Compiled by the author



тенций G20. Эта модель может стать основой для формирования детализированных перечней компетенций по информационной безопасности для различных целевых групп. Следует отметить, что с учетом важности вопросов обеспечения информационной безопасности в органах государственной власти именно государство должно определить детализированные подходы и требования к специалистам разного профиля, а также к разработке инструментов оценки компетенций, прежде всего в отношении госслужащих.

Возможные способы оценки компетенций в области информационной безопасности

На основе подходов образовательных организаций была сформирована рекомендуемая модель проведения оценки по информационной безопасности, включающая в себя:

- рекомендуемые квалификационные требования (компетенции) по информационной безопасности;
- фонды оценочных средств, предназначенные для проверки компетенций (контрольные задания или иные материалы);
- методические материалы, определяющие процедуры оценивания в необходимых контрольных точках для проведения оценки работника (от отбора на «входе» до использования в процессе аттестационной процедуры).

В рамках научно-исследовательской работы «Разработка методического аппарата оценки степени подготовленности государственных гражданских служащих в сфере обеспечения информационной безопасности»[13] на основе этого подхода были разработаны пакет оценочных средств и методика проведения оценки готовности государственных гражданских служащих, более подробно представленные в других работах авторов.

В ходе опытной эксплуатации были получены положительные результаты при проверке степени подготовленности государственных гражданских служащих, которые по характеру своей деятельности не занимаются вопросами обеспечения информационной безопасности.

По результатам пилотного внедрения оценочных инструментов на площадках двух федеральных органов и органов исполнительной власти двух субъектов Российской Федерации была подтверждена корректность включения разного набора квалификационных требований к госслужащим разных групп как неотъемлемой части модели цифровых компетенций.

При апробации методического комплекса была выявлена закономерность между уровнем автоматизации и цифровизации органа в целом и уровнем развития компетенций государственных служащих в области информационной безопасности. Количество неправильных ответов оцениваемых служащих в органах государственной власти с более низкой степенью зрелости процессов по информационной безопасности и уровнем автоматизации процессов деятельности явно больше в сравнении с количеством неправильных ответов госслужащих в органах государственной власти с более высоким уровнем автоматизации (**рисунок 3**).

При этом было выявлено, что для проверки уровня знаний и умений госслужащих, непосредственно занимающихся обеспечением информационной безопасности, квалификации проверяющего персонала в органах государственной власти недостаточно. Возможным вариантом решения этой проблемы может стать привлечение внешних квалифицированных специалистов. Однако существенным препятствием для этого является отсутствие в настоящее время законодательного регулирования механизмов оценки компетенций в области информационной безопасности.

Возможным путем решения данной проблемы может стать привлечение центров независимой оценки квалификации. Правовую основу такой оценки вне рамок государственной службы заложил Федераль-

13 Рег. № НИОКТР АААА-А19-119091190073-1

ный закон от 3 июля 2016 года № 238-ФЗ «О независимой оценке квалификации». В настоящее время система независимой оценки квалификации находится в стадии становления и развития, идет процесс создания центров независимой оценки квалификации по направлениям деятельности. В перспективе у органов государственной власти появится возможность привлечения к оценке квалификации специалистов по информационной безопасности профессиональных оценщиков, что позволит существенно повысить качество проводимой оценки, а также снизить затраты на ее проведение.

Заключение

В настоящее время каждый специалист должен обладать определенным набором компетенций по информационной безопасности, тем более если речь идет о государственных служащих. Авторами в ходе исследования было наглядно продемонстрировано, что компетенции в области информационной безопасности являются неотъемлемой частью цифровых компетенций. Проведен анализ зарубежных подходов к определению квалификационных требований по информационной безопасности, а также российских нормативных документов и практик в этой области. По результатам исследования были разработаны модели и подходы, которые позволили сформировать перечни квалификационных требований по информационной безопасности для различных категорий государственных гражданских служащих, разработаны фонд оценочных средств и методические материалы, определяющие процедуры оценивания.

Проведенная опытная эксплуатация подтвердила правильность разработанного подхода и позволила определить направления дальнейшего совершенствования предложенного инструментария оценки, а также выявила определенные проблемы, связанные со сложностью оценки квалификации профильных специалистов. Для решения выявленных проблем предложено использовать успешный зарубежный опыт привлечения независимых центров оценки квалификации.

Представленные авторами модели, перечни квалификационных требований и оценочные средства позволят определять и адресно повышать уровень профессиональных компетенций государственных гражданских служащих в области информационной безопасности как части более общих цифровых компетенций. Системная целенаправленная работа в этой области положительно скажется на способностях государственных служащих адаптироваться к условиям быстрых изменений цифровой экономики в Российской Федерации и в целом на обеспечении информационной безопасности в органах государственного управления.

Литература

Баймуратова Л.Р., Долгова О.А., Имаева Г.Р. и др. Цифровая грамотность для экономики будущего. М.: Издательство НАФИ, 2018.

Васильева Е.В., Пуляева В.Н., Юдина В.А. Развитие цифровых компетенций государственных гражданских служащих Российской Федерации. *Бизнес-информатика*. 2018. № 4 (46). С. 28–42.

Цифровые навыки и компетенция, цифровое и онлайн обучение. Европейский фонд образования, Турин, 2019. https://www.etf.europa.eu/sites/default/files/2019-08/dsc_and_dol_ru_0.pdf

Digital Transformation – A Framework for ICT Literacy. A Report of the International ICT Literacy Panel. Educational Testing Service, 2002. https://www.ets.org/Media/Research/pdf/ICTREPORT.pdf

Skills in the digital economy – Where Canada stands and the way forward. The Information and Communications Technology Council, 2016. https://www.ictc-ctic.ca/wp-content/uploads/2016/05/Skills-in-the-Digital-Economy-Where-Canada-Stands-and-the-Way-Forward-.pdf

References

Baimuratova L.R., Dolgova O.A., Imaeva G.R. et al. Digital literacy for the economy of the future. Moscow: NAFI Publishing house, 2018.

Vasilyeva E.V., Pulyaeva V.N., Yudina V.A. Development of digital competencies of state civil servants of the Russian Federation. *Biznes-informatika*. 2018. No. 4 (46). P. 28–42.

Digital skills and competence, digital and online learning. European Foundation for education, Turin, 2019. https://www.etf.europa.eu/sites/default/files/2019-08/dsc_and_dol_ru_0.pdf

Digital Transformation – A Framework for ICT Literacy. A Report of the International ICT Literacy Panel. Educational Testing Service, 2002. https://www.ets.org/Media/Research/pdf/ICTREPORT.pdf

Skills in the digital economy – Where Canada stands and the way forward. The Information and Communications Technology Council, 2016. https://www.ictc-ctic.ca/wp-content/uploads/2016/05/Skills-in-the-Digital-Economy-Where-Canada-Stands-and-the-Way-Forward-.pdf