# ОСОБЕННОСТИ ОЦЕНКИ КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ СЛУЖАЩИХ[1]

**Сладкова Н.М., Ильченко О.А., Степаненко А.А., Шапошников В.А.**[2]

## Аннотация

*Отсутствие системной работы по определению уровня развития компетенций государственных гражданских служащих в области информационной безопасности в условиях цифровизации повышает риски органов государственной власти РФ в данной сфере. Существующие пробелы в законодательстве, в методическом обеспечении со стороны регуляторов, в практике, принятой на государственной службе, и актуальность проблемы, подтвержденная федеральным проектом «Информационная безопасность», обусловили необходимость разработки типового оценочного инструментария и методики оценки компетенций государственных гражданских служащих по информационной безопасности. В статье описаны научно-практические подходы к разработке методического аппарата оценки и результаты его пилотного внедрения в 2019–2020 гг. Предмет исследования – методический инструментарий, включающий оценочные средства (тесты, кейсы), методику и процедуру оценки кандидатов и служащих. Представлены результаты анализа зарубежных практик, опроса востребованности методического инструментария в органах власти, анализа нормативно-правового и методического обеспечения оценки компетенций по информационной безопасности.*

[1] Исследование выполнено в рамках государственного задания по теме: «Разработка методического аппарата оценки степени подготовленности государственных гражданских служащих в сфере обеспечения информационной безопасности» 2019–2020 гг.

[2] *Сладкова Надежда Михайловна* – кандидат педагогических наук, директор по развитию ФГБУ «ВНИИ труда» Минтруда России. Адрес: 105043, Москва, 4-я Парковая ул., д. 29. E-mail: n.sladkova@vcot.info
*Ильченко Ольга Александровна* – руководитель проектов ФГБУ «ВНИИ труда» Минтруда России. E-mail: o.ilchenko@vcot.info
*Степаненко Андрей Александрович* – старший аналитик ФГБУ «ВНИИ труда» Минтруда России. E-mail: andrew.a.stepanenko@gmail.com
*Шапошников Виталий Анатольевич* – кандидат физико-математических наук, старший аналитик ФГБУ «ВНИИ труда» Минтруда России, заместитель начальника учебно-методического отдела АНО ДПО ЦПК АИС. E-mail: Shaposhnikov.Vitalij@yandex.ru

*Даны концептуальные подходы к разработке модели компетенций, оценочных средств и процедур оценки с учетом требований нормативных актов в области информационной безопасности, особенностей целевых групп оцениваемых служащих и назначения оценки. Апробация методического аппарата подтвердила его практическую ценность для органов власти. Предполагается, что применение методического инструментария даст возможность получить необходимую аналитическую информацию для определения задач и выбора программ развития компетенций, что может быть востребованным также в образовательных организациях, занимающихся подготовкой государственных гражданских служащих.*

**Ключевые слова:** информационная безопасность; государственная служба; оценка по информационной безопасности; оценка государственных служащих; методика оценки.

## Введение

Современные реалии актуализируют вопросы информационной безопасности в мировом сообществе. Глобальное информационное пространство состоит из государственных и межгосударственных компьютерных сетей, телекоммуникационных систем, сетей общего пользования, иных трансграничных каналов передачи информации. Его пользователи сегодня – почти половина населения планеты, только в период с 2002 по 2016 гг. их количество возросло с 413 млн до 3,4 млрд (World Population Review, 2021). Глобальная сеть, предоставляя несомненные преимущества, в то же время становится источником угроз для частных, корпоративных и государственных интересов. Одним из впечатляющих примеров хищения государственных секретов является раскрытая в 2013 г. «Лабораторией Касперского» деятельность шпионской сети «Красный Октябрь» (Red October). В течение пяти лет вредоносные программы передавали секреты государственных структур, посольств, научных институтов и других организаций бывших республик СССР, почти всей Западной Европы, Австралии и США (Бураева, 2015). Как отмечают специалисты, данная проблема могла бы не возникнуть в случае повсеместного применения известной технологии комплексного шифрования с использованием алгоритмов SSL/TLS. Однако, по мнению экспертов, помешал прежде всего «человеческий фактор»: организационная инертность, неграмотность, плохая информированность.

Это только один из негативных примеров: количество ежегодно обнаруживаемых в глобальной сети вредоносных объектов исчисляется миллиардами, причем год от года их становится больше примерно на 40% (Бураева, 2015). Стабильность государств в области политики, экономики, социальной сферы все более определяется состоянием национальных информационных ресурсов и способностью использовать и защищать данные.

Доктрина информационной безопасности Российской Федерации (утверждена Приказом Президента РФ от 5 декабря 2016 г. N 646) определяет информационную безопасность как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз,

при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государств».

Являясь одним из основных показателей качества данных или информации (Алексеева, 2015), безопасность не так однозначно трактуется в мировом сообществе, как это может показаться на первый взгляд. Как правило, в государственных стратегиях и реформах видны два ключевых аспекта по работе с данными государства: 1) Data Release – общедоступные данные, публикуются в открытом доступе, 2) Data Sharing – предусматривается обмен данными за счет предоставления доступа к тем данным, которые не могут быть открыты (например, персональные данные, негосударственные данные, на которые государство оказывает влияние и т. д.), инструменты для доступа научных организаций к этим данным[3]. В вопросах, к каким именно данным может быть применен тот или другой подход, возможны расхождения.

Тем не менее в общемировом масштабе можно отметить единодушие, касающееся отношения к данным как к основе современной экономики. Эксперты (см., например: Двинских, Талапина, 2019) приводят градацию компании Gartner по пяти этапам зрелости цифрового правительства (электронное, открытое, датацентричное, полностью цифровое и «умное»). Датацентричное правительство в соответствии с этой градацией в качестве основной технологии использует открытие всех данных, при этом показателем реализации служит количество услуг, предоставляемых на их основе. Очевидна эволюция государственного управления, начавшаяся за рубежом с реформ конца 1970-х – начала 1980-х гг. и приобретшая интернациональный характер, независимо от типа политической системы и уровня развития стран – от Монголии до США (см. об этом: Неделько и др., 2008; Потехин, 2010), включая Россию. В качестве идеологической основы таких изменений называют клиентоориентированный подход на уровне государственных органов и их персонала (Rman, et al., 2020; Мартынова, 2013), по-новому определяющий роль органов управления в жизни общества. При этом государство рассматривается как институт, предоставляющий качественные услуги населению (см. об этом, например: Сидоренко, Барциц, Хисамова, 2019). Среди услуг выделяются услуги, предоставляемые в электронном виде, что особенно важно для развивающихся стран (Shkarlet et al., 2020). Данный подход нашел развитие в концепции «сервисного» государства, неотъемлемыми чертами которой является управление большими данными и цифровизация информации. Получение услуг для граждан и бизнеса без посещения чиновников и органов власти видится перспективой нескольких ближайших лет.

Как отмечалось, развитие цифровизации и оборота данных кроме очевидных преимуществ (Халин, Чернова, 2018) связано также со значительными рисками для владельцев данных (Двинских, Талапина, 2019), а значит,

[3] См.: Доклад Центра стратегических разработок «Государство как платформа». 2019. URL: https://www.csr.ru/wp-content/uploads/2018/05/GOSUDARSTVO-KAK-PLATFORMA_internet.pdf (дата обращения: 20.09.2020).

требует постоянного внимания к уровню обеспечения информационной безопасности.

Ключевыми компонентами информационной безопасности в организации являются технологии, процессы деятельности и люди. При этом зарубежными и российскими экспертами подчеркивается важнейшая роль сотрудников в обеспечении информационной безопасности, значимость развития компетенций персонала в этой области. При соблюдении требований к используемым технологиям и при правильно выстроенных процессах работа по обеспечению информационной безопасности без оценки и развития компетенций сотрудников в данной области всегда будет сопряжена с рисками. Наиболее часто встречающиеся угрозы в области работы с информацией, так или иначе связанные с человеческим фактором, можно разделить на три группы:

1. Угрозы утечки конфиденциальной информации, в том числе: через компьютеры сотрудников по каналам связи (веб, e-mail, чаты, ftp, облачные сервисы и т.п.); с переносных носителей информации (USB-флешки, диски и т.п.); нарушение конфиденциальности данных, передаваемых по линиям связи вне контролируемой зоны, осуществляемое внешними нарушителями путем анализа трафика, проходящего по каналам связи (сюда же можно отнести считывание информации с оптических каналов связи интернет-провайдеров), перехват вводимой информации на компьютерах сотрудников с помощью как программных, так и технических средств (кейлогеры и т.п.); внедрение в ИТ-инфраструктуру фишинговых устройств (серверы, маршрутизаторы и т.п.) и программного обеспечения с целью перенаправления на них трафика и последующей кражи учетных данных сотрудников; печать или копирование конфиденциальной информации с последующим выносом ее за пределы организации.
2. Угрозы, связанные с внешними и внутренними злоумышленниками, в том числе: подбор паролей внутренними злоумышленниками к оборудованию и программному обеспечению во внутренней сети (BruteForce паролей); сканирование внутренней сети с целью получения различной технической информации (схемы сети, используемое ПО и т.п.); предоставление удаленного доступа к данным злоумышленнику (RDP, TeamViewer и т.п.); заражение компьютеров и серверов различным вредоносным кодом через подключаемые периферийные устройства (USB-флешки, телефоны, фотоаппараты и т.п.); заражение компьютеров и серверов различным вредоносным кодом через интернет (спам-письма, фишинговые сайты, взломанное ПО и т.п.) и др.
3. Угрозы нарушения целостности информации или ее недоступности, в том числе: нарушение целостности данных из-за ошибок пользователей, администраторов; несанкционированное изменение системной конфигурации, файлов, баз данных; плохо написанное программное обеспечение, скрипты и т.п.

В России тема использования и защиты данных нашла развитие в программе «Цифровая экономика» и призвана воплотиться в Национальной системе управления данными (НСУД). Трансформационные процессы по обе-

спечению информационной безопасности, как отмечают разработчики, в первую очередь должны быть направлены на изменение культуры, способа действий, появление новых ролей и компетенций, снижающих или исключающих риски в области информационной безопасности[4].

Проблемы информационного развития государственных органов власти в Российской Федерации также видятся во многом в слабой готовности персонала государственной службы к инновационным методам работы в информационной среде, в том числе при разработке и реализации новых инновационных практик (Barabashev, Zaytseva, 2020). По мнению специалистов (см., например: Куракин, Костенников, 2014), уровень подготовленности современных государственных служащих в этой области можно отнести к факторам, сдерживающим инновационное развитие государственной сферы.

Для ускорения цифровизации отмечается важность разработки учебных программ по информационной безопасности для обучения населения, сотрудников госучреждений и государственных служащих. В этом контексте существенно возрастает необходимость оценки уровня готовности служащих к обеспечению информационной безопасности.

Развивая идеи влияния человеческого фактора на успех цифровой трансформации и в целом на информационную безопасность, проведенное в статье исследование базируется на компетентностном подходе к определению состояния информационной безопасности в государственных органах и фокусируется на вопросах оценки государственных гражданских служащих в сфере информационной безопасности. При этом оценка рассматривается как отправная точка для разработки программ развития и обучения государственных (и муниципальных) служащих, важнейшая часть системных мер в органах власти для достижения требуемого уровня компетенций в области информационной безопасности.

## Исследуемая область

Регулирование вопросов оценки компетенций служащих по обеспечению информационной безопасности на государственной гражданской службе осуществляется Минтрудом России при взаимодействии с компетентными в данной области федеральными органами государственной власти (ФСТЭК, ФСБ, Минцифры России).

В 2017 г. Минтрудом России в качестве документа рекомендательного характера был разработан «Методический инструментарий по установлению квалификационных требований для замещения должностей государственной гражданской службы»[5]. Документ делит квалификационные требования

[4] См.: Доклад Центра стратегических разработок «Государство как платформа». 2019. URL: https://www.csr.ru/wp-content/uploads/2018/05/GOSUDARSTVO-KAK-PLATFORMA_internet.pdf (дата обращения: 20.09.2020).

[5] См.: Методический инструментарий по установлению квалификационных требований для замещения должностей государственной гражданской службы, версия 3.2 (утв. Министерством труда и социальной защиты РФ). 2020. URL: https://www.garant.ru/products/ipo/prime/doc/71755218/ (дата обращения: 06.06.2020).

на базовые и профессионально-функциональные требования к образованию, стажу, знаниям и умениям. Общие для всех базовые требования к знаниям и умениям включают список требований к знаниям в области обеспечения информационной безопасности и умениям по владению информационно-коммуникационными технологиями.

Основным способом проверки знаний соискателей на должности государственной гражданской службы (в том числе по нормативным правовым актам) является тестирование. Также у соискателей с помощью специальных заданий проверяется уровень владения пакетом офисных программ. Проверка компьютерных навыков никак не связана с вопросами обеспечения информационной безопасности.

«Методика всесторонней оценки профессиональной служебной деятельности государственного гражданского служащего»[6], также рекомендованная Минтрудом России, предусматривает оценку квалификации; профессиональных и личностных качеств (компетенций); эффективности и результативности профессиональной служебной деятельности гражданского служащего[7] по пяти уровням: Д (неудовлетворительный), Г (недостаточный), В (достаточный), Б (высокий), А (очень высокий). На момент написания статьи ни цифровые компетенции, ни компетенции по информационной безопасности в текущую (всестороннюю) оценку не включены.

Что касается законодательно закрепленных норм в рассматриваемой области, анализ документов показал отсутствие правового регулирования фондов оценочных средств для оценки при приеме на работу или в рамках аттестации. Это характерно как для бизнеса, так и для бюджетных организаций и органов государственной власти.

Следует констатировать, что системная работа в области оценки и развития компетенций государственных гражданских служащих по информационной безопасности еще не сложилась. Такое положение дел в условиях цифровизации и перевода части служащих в дистанционный режим работы повышает риски информационной безопасности в органах государственной власти РФ (Васильева, 2018).

Необходимость усиления государственных мер в направлении создания и внедрения методического инструментария оценки компетенций государственных гражданских служащих по обеспечению информационной безопасности подтверждена задачей федерального проекта «Информационная безопасность» как части национальной программы «Цифровая экономика»[8].

---

[6] Методика всесторонней оценки профессиональной служебной деятельности государственного гражданского служащего. 2020. URL: https://rosmintrud.ru/ministry/programms/gossluzhba/16/4/2 (дата обращения: 05.06.2020).

[7] В случае если в государственном органе могут быть разработаны количественно измеримые показатели, оценка эффективности и результативности осуществляется по показателям.

[8] См.: Паспорт национальной программы «Цифровая экономика Российской Федерации». 2020. URL: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (дата обращения: 4.06.2020).

Предмет нашего исследования – методический аппарат определения степени подготовленности государственных гражданских служащих в сфере информационной безопасности (далее – методический аппарат), включая оценочные средства/инструменты, методику и процедуру организации оценки компетенций по обеспечению информационной безопасности.

При разработке подходов к оценке по информационной безопасности служащих в органах государственной власти мы выделили три возможных направления по созданию оценочных средств: оценочные средства для самооценки, оценочные средства для проверки компетенций на уровне организации/органа власти, а также оценка независимыми экспертами/организациями вне деятельности организации/органа власти. Наша исследовательская работа была сфокусирована на разработке оценочных средств для проверки компетенций на уровне организации/органа власти.

Приступая к исследованию, мы ставили перед собой ряд вопросов, в том числе:

1. Каково состояние работы в органах государственной власти по оценке и развитию компетенций по обеспечению информационной безопасности госслужащих? Используются ли оценочные средства для оценки компетенций в области информационной безопасности в существующей практике органов государственной власти? Какие? Какое место занимает оценка компетенций по обеспечению информационной безопасности в органах власти: в течение «жизненного цикла» служащего?
2. Какие научно-практические подходы разработки оценочных средств и методик оценки навыков обеспечения информационной безопасности существуют в мировой практике в интересах граждан, предприятий и государственных органов?
3. Каков перечень требований к знаниям, умениям, навыкам, по которым проводится оценка по информационной безопасности на государственной службе, учитывают ли они задачи цифровизации?
4. Существуют ли различия в выборе инструментов и процедуры оценки компетенций государственных гражданских служащих на разных должностях?

Существующие пробелы в законодательстве, методическом обеспечении государственной службы и актуальность проблемы обусловили необходимость разработки *типового* оценочного инструментария и методики оценки компетенций государственных гражданских служащих по информационной безопасности.

В рамках исследования рассматривался опыт зарубежных стран и отечественные практики как в государственном, так и частном секторе экономики. Дополнительно мы опирались на возможности использования элементов итоговой оценки знаний, умений и навыков по окончании образовательных программ как аналога разрабатываемой оценки. Прорабатывались правовые нормы, регулирующие формы контроля образовательной деятельности, формы аттестации обучающихся, порядок оценки результатов обучения, а также порядок, формы и процедуры применения оценоч-

ных средств в рамках реализации образовательных программ. Учитывались положения Федерального закона «О независимой оценке квалификации» от 3 июля 2016 г. N 238-ФЗ, Положения о разработке оценочных средств для проведения независимой оценки квалификации (приказ Минтруда России от 01 ноября 2016 г. N 601н), Положения о разработке наименований квалификаций и требований к квалификации, на соответствие которым проводится независимая оценка квалификации (приказ Минтруда России от 12 декабря 2016 г. N 726н).

Несмотря на то, что 238-ФЗ не регулирует вопросы оценки на государственной гражданской службе, отдельные положения данных нормативных актов были использованы в качестве базы при формировании модели оценки компетенций и при разработке оценочных средств по информационной безопасности (далее – ИБ).

## Состояние работы в органах государственной власти по оценке и развитию компетенций по обеспечению информационной безопасности госслужащих

Для разработки и выбора оценочных средств было важно определить текущее состояние работы в органах государственной власти в области оценки компетенций по ИБ в отсутствие нормативно-методического обеспечения со стороны регуляторов. Для решения данной задачи в 2020 г. был проведен опорос специалистов кадровых служб, специалистов по информационной безопасности и специалистов по информационным технологиям в 66 ФОИВ, территориальных органов ФОИВ и ОИВ 83 субъектов РФ (всего более 700 ОИВ федерального и регионального уровня). В опросе участвовало 3673 служащих. Результаты опроса подтвердили гипотезу, что работа по оценке компетенций в области ИБ не является системной и регулярной и не может в полном объеме обеспечить определение требуемого перечня программ развития государственных гражданских служащих в области ИБ.

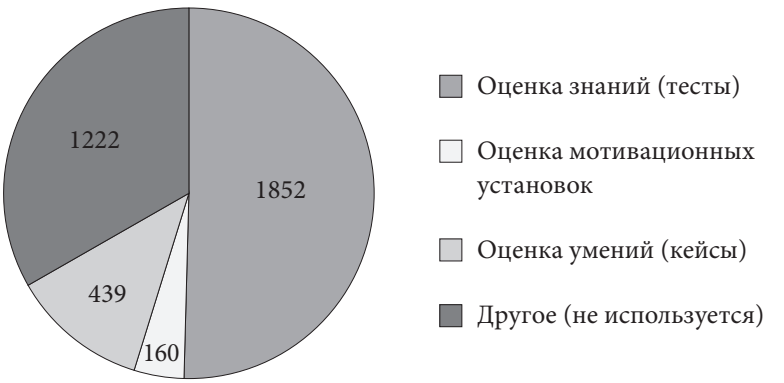
Несмотря на то, что 68% (2507) опрошенных подтвердили наличие оценки подготовленности государственных гражданских служащих к обеспечению ИБ в органах власти, отмечена низкая частота реализации такой оценки, разная глубина и охват компетенций по информационной безопасности.

Периодичность оценки один раз в три года в ходе аттестации отметили 31% (1123) респондентов. Проведение оценки в области обеспечения информационной безопасности в рамках конкурсных процедур на замещение должностей государственной гражданской службы зафиксировали только пять опрошенных (т. е. менее 1%).

В качестве оценочных средств для проверки знаний в ОГВ используются преимущественно тесты (50% ответов, 1852 респондента), кейсы как инструмент для проверки умений применяются значительно реже (12% ответов, 439 респондентов); использование заданий на оценку мотивационных установок отметили только 4% (160) опрошенных служащих (Рисунок 1).

*Рисунок 1*

**Используемые средства оценки компетенций по информационной безопасности в органах власти**




***Источник:*** Составлен авторами.

Низкие показатели наличия и использования оценочного комплекса по информационной безопасности, а также разброс данных по видам оценочных средств (от 50% до 4% ответов) демонстрируют, с одной стороны, разный уровень работы по информационной безопасности в органах власти, с другой стороны, отсутствие рекомендованного регулятором методического комплекса. Его внедрение могло бы обеспечить полноту, комплексность и единство подходов для проверки компетенций в данной области и создать основу для предупреждения рисков, связанных с человеческим фактором.

Заметно практически полное отсутствие оценки мотивации служащих на обеспечение информационной безопасности (4%). Как показывает мировая практика, недостаток данных у руководителей об уровне мотивации сотрудников/служащих на обеспечение информационной безопасности приводит к выбору неэффективных мероприятий по развитию компетенций в области информационной безопасности и значительно влияет на риски в этой сфере.

Полученные сведения по автоматизации данного вида оценки относились только к 68% всех участников опроса и продемонстрировали низкий уровень ее технического оснащения. Так, о полной автоматизации оценки говорили только 16% (584) респондентов, о проведении оценки в частично автоматизированном формате – 17% (628) респондентов, об отсутствии автоматизации, т.е. о проведении оценки полностью на бумажном носителе, – от 33% (1207) опрошенных.

Результаты опроса подтвердили необходимость и важность разработки, апробации и внедрения единого решения для всех государственных органов оценки готовности государственных гражданских служащих к обеспечению информационной безопасности; широкого тиражирования методического аппарата, включая рекомендации по оценке мотивационных установок, и встраивания оценки в конкурсные процедуры, периодическую всестороннюю оценку и аттестацию.

## Зарубежные практики оценки и развития компетенций по информационной безопасности

Важной задачей исследования был анализ существующей практики разработки и проведения оценки компетенций в области обеспечения информационной безопасности в странах с развитой экономикой, прежде всего ЕС и США.

В Европейском союзе усилия по развитию навыков по информационной безопасности носят системный характер (см. например: Соколова, 2020; Циренщиков, 2019) и реализуются последовательно: от определения модели компетенций, разработки программ обучения до создания инструментария оценки компетенций, включая самооценку. Еще в 2004 г. в ЕС создано Агентство по сетевой и информационной безопасности (ENISA – The European Union Agency for Network and Information Security, с июня 2019 г. – The European Union Agency for Cybersecurity). Одно из направлений его работы – повышение уровня подготовки граждан ЕС, поддержка просветительской и учебной деятельности в государствах – членах ЕС для безопасного использования информационно-коммуникационных технологий.

В 2010 г. агентство разработало документ «Руководство для новых пользователей: как повысить осведомленность об информационной безопасности»[9] – практическое руководство по планированию и реализации программы повышения осведомленности в области информационной безопасности.

Что касается необходимых знаний и навыков в данной сфере, в рекомендациях для граждан ЕС 2018 г.[10] делается акцент на угрозы кибербезопасности в отношении информации и связанных с нею рисков – ложных новостей, кибербуллинга и радикализации. В качестве критического риска отмечается нарушение информационной безопасности в системе государственного управления.

Оценка и одновременно обучение по информационной безопасности реализуются в рамках общеевропейских учений Cyber Europe. В учениях применяются технологии, предлагающие прохождение в онлайн-режиме захватывающих сценариев, которые разрабатываются европейскими экспертами по кибербезопасности и основаны на моделировании реальности[11].

Масштабность и системность работы ЕС по развитию цифровой грамотности отражается в количестве ее участников (18 национальных коалиций, свыше 300 разработчиков и более 7 млн граждан) и в числе мероприятий (11 видов), направленных на использование инструмента самоанализа SELFIE.

В США обязанности государственных организаций по проведению обучения всех сотрудников основам информационной безопасности закреплены на законодательном уровне. Федеральный закон об управлении ин-

[9] The new users' guide: How to raise information security awareness. URL: https://www.ifap.ru/library/book327.pdf (дата обращения: 15.05.2019).

[10] Цифровые навыки и компетенция, цифровое и онлайн обучение. Европейский фонд образования, Турин. 2019. URL: https://www.etf.europa.eu/sites/default/files/2019-08/dsc_and_dol_ru_0.pdf (дата обращения: 01.07.2019).

[11] Cyber Europe. 2020. URL: https://www.cyber-europe.eu/#previous-edition (дата обращения: 20.07.2020).

формационной безопасностью 2002 г. (FISMA)[12], являющийся Разделом III в Законе об электронном правительстве 2002 г. (публичный закон 107–347) (E-Government Act of 2002 (Public Law 107–347)), в параграфе 3544 «Обязанности федерального агентства» (Federal agency responsibilities) устанавливает обязательства по повышению осведомленности по вопросам информационной безопасности для всех сотрудников, работающих с информационными системами, включая персонал контрагентов. Для оценки и реализации программ развития компетенций по информационной безопасности сотрудники делятся на группы: «пользователи» и «специалисты в области информационных технологий». Периодическое тестирование знаний и проверка эффективности выполнения политик и процедур информационной безопасности являются регулярной практикой. Требования по повышению осведомленности в области ИБ и способы их проверки прописаны в специальном документе[13].

Отдельного внимания заслуживает документ «Создание программы обучения и ознакомления с безопасностью информационных технологий» от 2003 г.[14]. В нем детально прописана тематика по основам информационной безопасности, которая должна доводиться до всех сотрудников в процессе обучения. Документом охвачено более 25 аспектов поведения сотрудника, затрагивающих все грани его деятельности в информационной системе; даны рекомендации по применению целого ряда инструментов для проверки усвоения полученных знаний.

Очевидно, что в США периодическая оценка является неотъемлемой и крайне важной частью всей программы повышения осведомленности по ИБ. При этом основным инструментом проверки знаний, как следует из документов NIST, является тестирование по набору вопросов с выбором одного или нескольких правильных ответов. В качестве дополнительных инструментов рассматриваются внезапные проверки, использование специально подготовленных рассылок, наблюдение за совершаемыми нарушениями принятых политик и регламентов ИБ и их фиксация.

Несмотря на схожесть наборов инструментов проверки знаний, используемых в документах NIST (США) и ENISA (ЕС), следует отметить, что в США требования к квалификации в отношении сотрудников, непосредственно занимающихся планированием и обеспечением информационной безопасности в организации, прописаны более детально.

Разработанный в 2011 г. Управлением кадровой службы США документ «Модель компетенций для кибербезопасности»[15] определяет наборы компе-

[12] Federal Information Security Management Act of 2002. URL: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf (дата обращения: 15.06.2019).

[13] Office of Management and Budget (OMB) Circular A-130. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Forum/documents/aug-2016/wed945_a-130_cbales.pdf (дата обращения: 20.06.2019).

[14] NIST Special Publication 800-50 «Building an Information Technology Security Awareness and Training Program» (2003). URL: https://csrc.nist.gov/publications/detail/sp/800-50/final (дата обращения: 20.05.2019).

[15] Competency Model for Cybersecurity. 2011. URL: https://chcoc.gov/content/competency-model-cybersecurity (дата обращения: 16.06.2019).

тенций, необходимых специалистам по ИБ нескольких профилей, имеющих различные грейды.

Предложенный в данном документе подход используется многими государственными организациями США для стандартизации трудовых функций, выполняемых ИБ-специалистами, унификации требований к их начальной квалификации и определения потребностей в дополнительном обучении.

Документ «Национальная инициатива по образованию в области кибербезопасности (NICE): Структура кадровых ресурсов по кибербезопасности» от 2017 г.[16] вводит модель определения требуемой квалификации специалистов по информационной безопасности, выполняющих трудовые функции различных специальностей и ролей.

В документе выделены 52 функциональные роли (специализации) работников, занимающихся обеспечением информационной безопасности. Для каждой из 52 специализаций сформированы списки задач и соответствующие им знания, умения и навыки (KSA) (табл. 1).

*Таблица 1*

**Модель оценки по кибербезопасности (США)**

| **Параметры («Национальная инициатива по образованию в области кибербезопасности (NICE): Структура кадровых ресурсов по кибербезопасности» от 2017 г.)** | **Кол-во** | **Средства оценки** |
|---|---|---|
| Список трудовых задач | 1007 | *Основа для разработки компетенций* |
| Требуемые области знаний | 630 | Тесты на знания |
| Требуемые практические умения и навыки | 374 | Кейсы, симуляционные задания |
| Требуемые способности, установки | 176 | Психологические тесты |

***Источник:*** Составлена авторами на основе NIST Special Publication 800-181 «National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework», 2017.

Методы оценки выбираются в соответствии со спецификой области проверки. Для оценки знаний используются специальные тесты; для определения умений и навыков – кейсы и симуляционные задания; способности и мотивационные установки оцениваются с помощью психологического тестирования.

Независимую оценку компетенций специалистов по ИБ в США проводят сторонние организации, занимающиеся сертификацией таких специалистов. Допускается признание полученных сертификатов в качестве подтверждения компетенций для работодателя.

Перечень сертифицирующих организаций определяется нормативными актами, среди них меморандум от 13.08.2008 «Информационный бюллетень по сертификации и программам сертификации» (Fact Sheet on Certification

[16] National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework. 2017. URL: https://www.assuresign.com/blog/thinking-of-outsourcing-your-cybersecurity-strategy-read-this-first/ (дата обращения: 25.06.2019).

and Certificate Programs) для всех государственных организаций США, разработанный Управлением кадровой службы США, руководство от 19.12.2005 N 8570.01 «Программа повышения квалификации кадров по обеспечению информации» (Information Assurance Workforce Improvement Program) и директива от 11.08.2015 N 8140.01 «Управление персоналом в киберпространстве» (Cyberspace Workforce Management) для военных и гражданских ИБ-специалистов, привлекаемых на работу в U.S. Department of Defense.

Несмотря на особенности национального законодательства, различия в части подходов, в терминологии, тем не менее требования к компетенции «Информационная безопасность» в США и ЕС практически идентичны. Также во многом совпадают и используемые инструменты для оценки этой компетенции (табл. 2).

*Таблица 2*

**Инструменты оценки. Сравнение: США, ЕС**

| **Инструменты оценки по компетенции «Информационная безопасность»** | **США** | **ЕС** |
|---|---|---|
| Тесты | + | + |
| Кейсы | + | + |
| Самооценка | | + |
| Скрытые проверки | + | |

***Источник:*** Составлена авторами.

Обобщая результаты анализа опыта США и ЕС по оценке и развитию компетенций в области цифровой грамотности и информационной безопасности, можно отметить схожесть подходов к разработке и использованию инструментов оценки.

## Подходы к разработке оценочных средств и методики оценки компетенций государственных гражданских служащих по обеспечению информационной безопасности

Опираясь на требования российских нормативных актов, национального проекта «Цифровизация», с учетом успешного международного опыта, текущего состояния в российских органах власти, был сформирован ряд основных подходов для разработки методического аппарата:

1. При *определении квалификационных требований* к государственным гражданским служащим в области обеспечения ИБ как основы для создания оценочного инструментария необходимо учитывать особенности деятельности служащих и уровни ответственности на занимаемых должностях. Кроме того, в оцениваемых знаниях, умениях и навыках должны найти отражение современные тенденции цифровизации как перспективной области развития компетенций.

2. Выбор *оптимальных методов для оценки компетенций* должен основываться на принципе их соответствия оцениваемым областям. Общемировая практика свидетельствует: проверка знаний в области ИБ требует разработки тестов; оценка уровня умений и навыков возможна через применение кейсов и симуляционных заданий, демонстрационного экзамена[17]; для оценки мотивационных установок используются специализированные и проверенные на практике психологические инструменты.
3. Разработка *оценочных средств* должна вестись на основе требований к тестам, кейсам и другим проверочным методикам, в том числе для аттестационных процедур в образовательной деятельности. Должны предусматриваться меры защиты от утечки информации по правильным ответам на оценочные задания.
4. Процедура, методика использования оценочных средств должна быть увязана с нормативными правовыми актами РФ, регулирующими вопросы оценки и аттестации на государственной гражданской службе. Оценка компетенций по ИБ должна быть встроена в общие процедуры тестирования и проверки умений при проведении конкурсов на замещение должности государственной гражданской службы, текущей (всесторонней или комплексной) оценки, осуществляемой по решению органа государственной власти ежегодно или в рамках очередной аттестации.

Перечисленные подходы определили последовательность и содержание этапов разработки методического комплекса оценки готовности государственных гражданских служащих по обеспечению информационной безопасности.

## Систематизация требований по информационной безопасности

Для разработки оценочного инструментария прежде всего требовалось определить перечень квалификационных требований по информационной безопасности, учитывающий специфику различных должностей государственной гражданской службы[18]. Создание такого перечня является необходимым условием разработки и реализации программ цифровой трансформации государственных органов[19].

Итоговый перечень квалификационных требований был сформирован рабочей группой при участии экспертов Минтруда России, Минцифры России, Аналитического центра при Правительстве Российской Федера-

[17] На примере демонстрационного экзамена WorldSkills. URL: https://worldskills.ru/nashi-proektyi/demonstraczionnyij-ekzamen/obshhaya-informacziya.html (дата обращения: 03.05.2020).

[18] Включение области информационной безопасности в область информационных технологий закреплено в Приказе Минтруда России от 05 сентября 2013 г. N 450 «О внесении изменений в приложение к приказу Министерства труда и социальной защиты Российской Федерации от 08 мая 2013 г. N 200 «Об утверждении перечня проектов профессиональных стандартов, разработка которых предусмотрена в 2013 году за счет средств федерального бюджета».

[19] См., например, справку, размещенную на официальном сайте Минкомсвязи России «Минкомсвязь России», разъясняющую порядок формирования программ цифровой трансформации госорганов. URL: www.digital.gov.ru (дата обращения: 01.02.2021).

ции, Центра компетенций федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (ПАО Сбербанк), Межрегиональной общественной организации «Ассоциация защиты информации». Требования определены на основе анализа федеральных законов, затрагивающих вопросы информационной безопасности в органах государственной власти. Учтено более 30 нормативных актов, разработанных ФСТЭК России, ФСБ России и Национального координационного центра по компьютерным инцидентам (НКЦКИ), регламентирующих работу Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), Центральным Банком России и Минтрудом России, которые прямо или косвенно фиксируют требования к квалификации и уровню знаний в области ИБ. Кроме того, в требованиях отражены положения разработанного Минтрудом России[20] Справочника квалификационных требований к специальностям, направлениям подготовки, знаниям и умениям, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих.

Следует отметить, что требования к государственным служащим в области информационной безопасности сочетают знания нормативных правовых актов РФ и знания и умения в области информационно-коммуникационных технологий. Однако к моменту начала исследовательской работы все требования не были собраны в отдельный документ и не имели разграничения по должностям. Это, безусловно, затрудняло системный охват всех требований и разработку оценочного комплекса и методики оценки по ИБ. Требовалась систематизация выше обозначенных квалификационных требований. Основанием для их группировки стала модель цифровых компетенций, предложенная в рамках саммита «Группы двадцати» (G20) в апреле 2017 г.[21].

Квалификационные требования по ИБ к госслужащим были сгруппированы по пяти элементам модели цифровых компетенций:

1) информационная грамотность;
2) компьютерная грамотность;
3) медиа-грамотность;
4) коммуникативная грамотность;
5) грамотность внедрения технологических инноваций.

Требования в области обеспечения информационной безопасности были систематизированы с учетом элементов модели (табл. 3).

[20] О подготовке Справочника в соответствии с частью 8 статьи 12 Федерального закона от 27 июля 2004 г. N 79-ФЗ «О государственной гражданской службе Российской Федерации» было объявлено в письме Минтруда России от 26 апреля 2017 г. N 18-1/10/В-3260. Обновленная версия справочника подготовлена на основе предложений государственных органов, поступивших в Минтруд России в 2018 г. – I квартале 2019 г.

[21] Bridging the Digital Divide: Measuring Digital Literacy, G20 Insights. 2017. URL: https://www.g20-insights.org/policy_briefs/bridging-digital-divide-measuring-digital-literacy/ (дата обращения: 16.04.2020).

*Таблица 3*

**Систематизация требований к информационной безопасности с учетом цифровых компетенций и квалификационных требований, согласованных с Минтрудом России**

| 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 |
| | НПА: | |
| | – 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.<br>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.<br>Эксплуатация средств защиты |
| | – защита от вредоносного кода; | |
| | – сетевая безопасность; | |
| | – защита от атак; | |
| | – управление уязвимостями;<br>– криптографическая защита информации;<br>– резервное копирование; | |
| | – защита от утечек по техническим каналам | |

| Предметная область требований | Знания | Умения |
|---|---|---|
| ***Б. Компьютерная грамотность*** | Построение защищенных систем и сетей | Проектировка, внедрение, аттестация, аудит защищенных систем |
| | Управление информационной безопасностью | Эксплуатация защищенной информационной системы |
| | Контроль и аудит информационной безопасности | |
| ***В. Медиа-грамотность*** | Пользование поисковыми системами в информационной сети интернет | Поиск и получение информации (PRAVO.GOV.RU);<br>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;<br>со служебной электронной почтой и служебными ПК | Формирование правил по информационной безопасности, разработка положений, инструкций, регламентов для пользователей, в том числе по работе:<br>– с электронной подписью;<br>– в сети интернет;<br>– с персональными данными.<br>Проведение внутренних семинаров по коммуникативной грамотности для пользователей.<br>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 |

***Источник:*** Составлена авторами.

***Примечание:*** Как видим, в модели требований к информационной безопасности не представлен блок «мотивационные установки». Он не был учтен при систематизации требований, так как отсутствовал в исходных документах (квалификационных требованиях в области ИБ).

Для учета специфики деятельности и уровня ответственности в модели требований по ИБ был проведен анализ должностей. Были выделены две большие группы: «пользователи» и «специалисты в области информационных технологий». Однако проведенные в ходе исследования фокус-группы с участием государственных служащих, специалистов кадровых служб и ИТ-технологий позволили уточнить структуру целевых групп.

Группа А была разделена на А1 и А2: руководителей разного уровня и «рядовых» сотрудников, имеющих разный уровень ответственности и доступа

к информации. Требования к направлению подготовки (специальности) профессионального образования служащих группы А определены требованиями по замещению должности. От пользователей требуются знания нормативных правовых актов в области ИБ (соответственно должности), инструкций по ИБ, умения владеть правилами использования ИТ-технологий, инструментов и т.п.

В отличие от пользователей, для группы «специалисты» (группа Б) обеспечение информационной безопасности является основным функционалом должности, что предусматривает оценку их квалификации как специалистов в обозначенной области.

Группа специалистов (Б), в свою очередь, была поделена на группы Б1 и Б2 с учетом специфики и предмета деятельности.

Группа Б1: ИТ-специалисты с квалификацией по информационным технологиям, которым требуется специализированная подготовка по укрупненным группам специальностей и направлений подготовки (УГСНП) – «Компьютерные и информационные науки», «Информатика и вычислительная техника», «Электроника, радиотехника и системы связи», предусмотренная соответствующими образовательными стандартами.

Группа Б2: специалисты по информационной безопасности; к данным служащим предъявляются требования по обязательной специализированной подготовке по УГСНП «Информационная безопасность».

## Выбор оптимальных методов оценки компетенций и разработка оценочных средств и методики оценки

Для выбора оценочных средств в области информационной безопасности и методики их использования в различных целевых группах государственных служащих мы исходили из следующих положений:

1. Методические подходы к выбору оценочных средств, процедуре и подведению результатов оценки по информационной безопасности должны быть реализованы по аналогии с уже сложившимися практиками оценки общепрофессиональных компетенций служащих ОГВ.
2. По своему содержанию оценочное средство должно соответствовать проверяемому при оценке требованию.
3. Оценочные средства должны быть доступными для использования непрофильными специалистами в области ИТ-технологий, к которым относятся специалисты кадровой службы.
4. Оценочное средство должно быть:
   a) индикативным (проверка ключевых и типовых рисков), не избыточным, коротким, не затратным по времени для оценки госслужащих-пользователей;
   b) достаточно полным и объемным для госслужащих-специалистов по ИТ и ИБ.
5. Оценочное средство должно полностью соответствовать целевому назначению:
   a) знания проверять специально разработанными тестами;
   b) умения проверять решением кейсов;

с) навыки (а в идеале и умения) проверять либо посредством симуляционных инструментов, моделирующих реальную ситуацию с помощью специальных технических условий, либо через независимую оценку квалификации и аудит документов, процессов, показателей информационной сферы.

6. База оценочных средств должна быть сформирована как конструктор, инструменты из которого выбираются кадровой службой для подготовки оценочного задания (совместно с руководителем ИТ-подразделения и лица, ответственного в органе государственной власти за соблюдение информационной безопасности).
7. Оценочные средства кадровой службой должны выбираться при проведении конкурсных процедур или аттестации.

Перечисленные положения позволили определить виды оценочных средств, наиболее корректных для использования в практике работы кадровых служб органов власти (см. табл. 4).

*Таблица 4*

**Оценочные средства по информационной безопасности для разных целевых групп**

| **Характеристика** | **Целевые группы оцениваемых** | | | |
|---|---|---|---|---|
| | **Группа А «пользователи»** | | **Группа Б «специалисты»** | |
| | **Руководители** | **Все служащие** | **Специалисты по ИТ** | **Специалисты по ИБ** |
| **Что проверяется** | Знания и умения ИБ общие | Знания и умения ИБ общие | Знания специальные | Знания и умения по ИБ специальные |
| **Оценочное средство** | Тесты | Кейсы | Тесты | 1. Кейсы.<br>2. Чек-листы.<br>3. Гайд-интервью.<br>4. Симуляции |
| **Что является основой для разработки оценочных средств** | Квалификационные требования, модель цифровых компетенций | Квалификационные требования, модель цифровых компетенций | Квалификационные требования к специалистам (образовательный и профессиональный стандарт) | 1. Квалификационные требования к специалистам (образовательный и профессиональный стандарт).<br>2. Анализ процессов ИБ органа власти |
| **Использование** | 1. Конкурс на замещение.<br>2.Аттестация | 1. Конкурс на замещение.<br>2. Аттестация | 1. Конкурс на замещение.<br>2. Аттестация | 1. Независимая оценка квалификации до конкурса на замещение вакантной должности.<br>2. Внутренний аудит (при аттестации) |

***Источник:*** Составлена авторами.

С учетом данного подхода была разработана база оценочных инструментов, содержащая:

1. Базовый комплект тестов/кейсов, который имеет разное количественное наполнение для разных групп (от 10 до 20 вопросов и кейсы).

При этом для госслужащих группы Б допускается не проводить тестирование при проведении конкурса на замещение вакантной должности в случае наличия у них сертификата по независимой оценке.

2. Дополнительный комплект тестов и кейсов для выбора по принципу конструктора, который может использоваться в зависимости от приоритетных целей органа в отношении цифровизации, от уровня развития ИТ-технологий в ОГВ, от уровня развития компетенций в области ИТ и ИБ. Дополнительный комплект содержит для разных целевых групп оценки от 60 до 140 тестовых вопросов (всего 751 тестовый вопрос), по 15 кейсов и симуляционные задачи.

Для специалистов кадровых служб была разработана методика оценки, включая содержание и последовательность действий по проведению процедур оценки и использованию оценочных средств.

В частности, предложено, чтобы тесты, кейсы и другие задания кадровая служба получала в двух комплектах – с ключами оценки и без ключей, на случай использования оценочных средств в офлайн-формате, для сохранения конфиденциальности.

Оценку по информационной безопасности рекомендовано предварять размещением инструкций и перечня нормативных актов, регулирующих данную область, в открытом доступе для подготовки кандидатов и служащих к оценочным процедурам.

Предлагаются пошаговые алгоритмы проведения оценки и подсчета результатов.

В методике также представлены типовые кадровые решения, направленные на обеспечение требуемого уровня информационной безопасности, профилактические и развивающие. Часть из них должна быть реализована в сотрудничестве с подразделением по информационной безопасности органа власти.

В качестве профилактических мер отмечена важность регулярной информационно-разъяснительной работы с госслужащими органа власти для минимизации рисков, связанных с ИБ, в частности:

– при расширении базы НПА по информационной безопасности;
– при внедрении/актуализации локальных регламентов по информационной безопасности в ОГВ;
– при выявлении типовых проблемных ситуаций в ОГВ, связанных с нарушением ИБ.

Все вышеперечисленные события рекомендуется сопровождать проведением инструктажа в очном или онлайн-формате с разбором проблемных ситуаций, в том числе типичных для данного органа власти. Должны быть разработаны и размещены в общем доступе инструкции и наглядные материалы, предупреждающие критические ситуации, связанные с информационной безопасностью. Для контроля усвоения материала рекомендуется

разрабатывать тесты. Проблемные ситуации, оформленные в виде кейсов, и разработанные тесты должны быть включены в базу оценочных средств органа власти.

Развивающие меры, предлагаемые методикой, рекомендуется реализовывать с учетом факторов:

– целевые группы (все служащие, руководители, специалисты по ИТ, специалисты по ИБ);
– вид оценки компетенции (оценка при поступлении на государственную службу, текущая оценка), по результатам которой принимаются кадровые решения;
– достигнутый по результатам оценки уровень развития компетенции по информационной безопасности (низкий результат, удовлетворительный результат, высокий результат).

Безусловно, инструментарий оценки компетенции «Информационная безопасность» государственных гражданских служащих требует постоянной актуализации и наращивания, а методика применения этого инструментария – совершенствования с учетом мнения и запроса органов государственной власти.

## Апробация оценочных средств по информационной безопасности

Для проверки методического аппарата на предмет объективности, воспроизводимости, доказательности и точности результатов оценки в 2019–2020 гг. проводилась апробация с использованием разных методов: независимая экспертиза, публичное обсуждение в экспертном сообществе, публикации, пилотное внедрение.

В 2019 г. подтвердили практическую значимость и готовность методического аппарата к использованию независимые эксперты Межрегиональной общественной организации «Ассоциация защиты информации» (АЗИ), Федерального учебно-методического объединения в системе высшего образования по УГСНП «Информационная безопасность» (ФУМО ИБ), а также ряда ведущих образовательных организаций в системе ДПО по информационной безопасности.

Пилотное внедрение инструментов оценки было реализовано в апреле–июле 2020 г. в четырех органах государственной власти с участием 4855 служащих всех целевых групп оцениваемых служащих (группы А – пользователи, Б – специалисты, а также кадровой службы как организатора и администратора оценки).

Проект по пилотному внедрению был направлен на экспертизу методического аппарата по трехбалльной шкале:

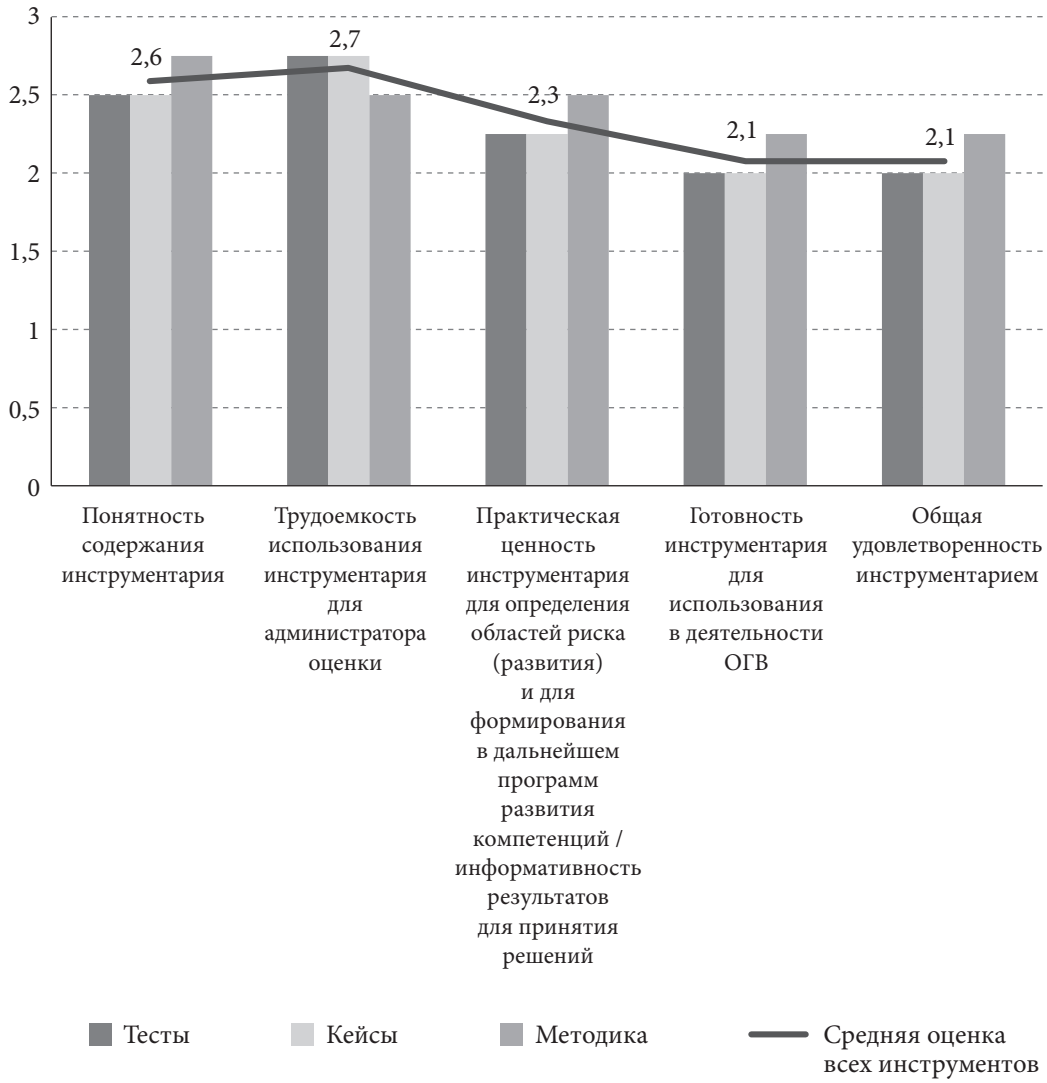
1 – есть существенные замечания;

2 – удобно, полезно, в целом соответствует ожиданиям, но есть несущественные замечания;

3 – полностью соответствует ожиданиям по критериям: понятность, трудоемкость, практическая значимость, готовность к использованию и общая удовлетворенность.

*Рисунок 3*

**Средняя оценка всех инструментов методического аппарата по всем пилотным площадкам органов власти**




***Источник:*** Составлено авторами.

Итоговая средняя оценка всех инструментов методического аппарата составила 2,4 балла, что свидетельствует о качестве апробируемого материала. Наиболее высокая оценка получена по критериям: понятность содержания инструментария (2,6), трудоемкость использования инструментария для администратора оценки (2,7). Участники отметили практическую ценность инструментария для определения областей риска (развития) и для формирования в дальнейшем программ развития компетенций – информативность результатов для принятия решений (2,3). Средняя оценка в разрезе инструментов показала их примерную сопоставимость по обозначенным

критериям, чуть более высокую оценку получила методика (2,45), оценка тестов и кейсов составила 2,3 балла.

Пилотное внедрение продемонстрировало соответствие фактического времени, затраченного на проведение оценки, расчетному и предложенному в методике. Среднее время на прохождение тестирования составило от 10 до 20 мин, на решение кейсов – 10–15 мин. На самостоятельную подготовку варианта оценочных средств организаторами апробации в среднем затрачивалось 30 мин. Высокая оценка по критерию трудоемкости в анкетах обратной связи свидетельствует об оптимальном уровне трудозатрат на подготовку и прохождение оценочных процедур.

В целом оценка результатов апробации 2019–2020 гг. показала востребованность и практическую применимость подходов, заложенных в методику оценки, доступность инструментария для применения в практике государственных органов по решению следующих задач:

– подготовки и организации процедуры оценки;
– для предварительной подготовки целевых групп к оценочным процедурам;
– оценки кандидатов на замещение должностей государственной гражданской службы в рамках проведения конкурсных процедур;
– оценки в ходе очередной аттестации;
– принятия решений по развитию компетенций в области информационной безопасности.

Инструментарий может быть рекомендован для формирования и пополнения единой российской базы оценочных средств госслужащих в области информационной безопасности, мониторинга уровня компетенций целевых групп; разработки программ дополнительного профессионального образования для служащих; в аттестационных мероприятиях выпускников вузов (РАНХиГС, МГУ, Финансового университета и других, занимающихся подготовкой государственных гражданских служащих).

Перспектива развития предмета исследования видится в следующем:

1. Автоматизация методического комплекса. Применение разработанных оценочных средств в практике органов государственной власти с использованием информационно-коммуникационных технологий, в том числе единой информационной системы управления кадровым составом государственной гражданской службы РФ (ЕИСУ КС).
2. Регулярное пополнение/актуализация оценочной базы новыми тестами, кейсами, упражнениями, симуляциями.
3. Разработка образовательных, в том числе модульных, программ дополнительного профессионального образования в части информационной безопасности для государственных гражданских служащих с учетом модели квалификационных требований.
4. Формирование предложений/инициатив по правовому регулированию фондов оценочных средств, разработке НПА в отношении обязательности использования оценки компетенций государственных гражданских служащих по информационной безопасности для снижения рисков, связанных с человеческим фактором.

## Заключение

Разработанный в ходе исследования методический аппарат дает основу для системного подхода к определению областей развития компетенций государственных гражданских служащих в сфере информационной безопасности.

Предлагаемые оценочные средства и методика оценки позволяют с высокой степенью достоверности определять готовность государственных служащих по обеспечению информационной безопасности в соответствии с квалификационными требованиям в области ИБ, учитывающими уровень ответственности и специфику должностей.

Востребованность в государственных органах, целесообразность и практическая значимость применения оценочных средств и процедуры оценки подтверждена апробацией 2019–2020 гг.

Оценка компетенций по информационной безопасности обеспечит обоснованность выбора методов и форм профессионального развития государственных гражданских служащих в области информационной безопасности, что может быть востребованным как в органах власти, так и в образовательных организациях, занимающихся подготовкой государственных гражданских служащих в данной сфере.

Актуальность результатов, полученных в ходе исследования, повышается в условиях интенсивной цифровизации органов государственной власти РФ.

## ЛИТЕРАТУРА

1. Алексеева Л.Н. Система информационной безопасности органов государственной власти как основа современного государственного управления // Вестник университета. – 2015. – № 13. – С. 5–9.

2. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. – 2015. – № 13. – С. 96–99.

3. Бураева Л.А. Террористические объединения в глобальном информационном пространстве // Пробелы в российском законодательстве. – 2014. – № 3. – С. 274–276.

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

5. Двинских Д.Ю., Талапина Э.В. Риски развития оборота данных в государственном управлении // Вопросы государственного и муниципального управления. – 2019. – № 3. – С. 7–30.

6. Куракин А.В., Костенников М.В. Государственная служба и информационная безопасность // Вопросы безопасности. – 2014. – № 6. – С. 18–67.

7. Маркин В.В., Осташков А.В. Мониторинг в системе оказания государственных и муниципальных услуг как инструмент реализации стратегии повышения качества государственного и муниципального управления: опыт, проблемы, рекомендации // Учебное пособие. Авторы: Неделько С. И., Осташков А. В., Матюкин С. В., Ретинская В. Н., Мурзина И. А., Кревский И. Г., Луканин А. В., Кошевой О. С. – М.: Экслибрис Пресс, 2008.

8. Мартынова С.Э. Концепция «сервисного» государства в контексте постиндустриальной парадигмы социального управления // Вестник Тюменского государственного университета. – 2013. – № 8. – С. 165–173.

9. Потехин В.А. Совершенствование властных отношений как условие модернизации управленческой деятельности // Власть. – 2010. – № 6 – С. 18–22.

10. Сидоренко Э.Л., Барциц И.Н., Хисамова З.И. Эффективность цифрового государственного управления: теоретические и прикладные аспекты // Вопросы государственного и муниципального управления. – 2019. – № 2. – С. 93–114.

11. Соколова Е.И. Цифровые компетенции и новые технологии в образовании: по материалам документов европейской комиссии // Непрерывное образование: XXI век. – 2020. – № 2. – Т. 30. – С. 121–133.

12. Халин В.Г., Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Власть и экономика. Управленческое консультирование. – 2018. – № 10. – С. 46–63.

13. Циренщиков В.С. Цифровизация экономики Европы // Современная Европа. – 2019. – № 3. – С. 104–112.

14. Barabashev A., Zaytseva T. The Innovative HR Practices of Regional Administrations: Is it a New Round of Civil Service Reform in Russia? // NISPAcee Journal of Public Administration and Policy. 2020. Vol. 13. N 2. P. 229–248.

15. ENISA. Cyber Europe 2020. EU, ENISA 2019. URL: https://www.cyber-europe.eu/img/CE2020_presentation.pdf (дата обращения: 05.11.2020).

16. Rman M., Brezovšek M., Stare J. The Measurement Model of Professional Operation of State Administration // Central European Public Administration Review. 2020. Vol. 18. N 2. P. 29–52.

17. Shkarlet S., Oliychenko I., Dubyna M., Ditkovska, Zhovtok V. Comparative Analysis of Best Practices in E-Government Implementation and Use of This Experience by Developing Countries // Administratie Si Management Public. 2020. No. 34. P. 118–136.

18. World Population Review. Internet Users by Country 2021. World Population Review, USA. 2021. URL: https://worldpopulationreview.com/country-rankings/internet-users-by-country (дата обращения: 11.01.2021).

# FEATURES OF THE ASSESSMENT OF INFORMATION SECURITY COMPETENCIES OF STATE AND MUNICIPAL EMPLOYEES

**Nadezhda M. Sladkova**
Ph.D. (in Pedagogical Sciences), Director for Development
of the FSBI «All-Russian Research Institute of Labor»
Ministry of Labor of Russia.
Address: 29, 4th Parkovaya Str., 105043 Moscow, Russian Federation.
E-mail: n.sladkova@vcot.info

**Olga A. Ilchenko**
Project Manager of FSBI VNII Labor of the
Ministry of Labor of Russia, Moscow, Russia.
Address: 29, 4th Parkovaya Str., 105043 Moscow, Russian Federation.
E-mail: o.ilchenko@vcot.info

**Andrei A. Stepanenko**
Senior Analyst, FSBI VNII Truda, Ministry of Labor of Russia,
Address: 29, 4th Parkovaya Str., 105043 Moscow, Russian Federation.
E-mail: andrew.a.stepanenko@gmail.com

**Vitaly A. Shaposhnikov**
Ph.D. (Physical and Mathematical Sciences), Senior analyst
of the FSBI «All-Russian Research Institute of Labor»
of the Ministry of Labor of Russia, Deputy head of the educational
and methodological department of the ANO DPO Central Research Center AIS.
Address: 29, 4th Parkovaya Str., 105043 Moscow, Russian Federation.
E-mail: Shaposhnikov.Vitalij@yandex.ru

## Abstract

The lack of systematic work to determine the level of development of the competencies of state civil servants in the field of information security in the context of digitalization increases the risks of the Russian state authorities in this area. The existing gaps in legislation, in methodological support from regulators, in the practice adopted in the civil service, and the relevance of the problem, confirmed by the federal project «Information Security», led to the need to develop a standard assessment tools and methods for assessing the competencies of state civil servants in information security. The article describes the scientific and practical approaches to the development of the methodological apparatus of assessment and the results of its pilot implementation in 2019–2020. The article describes the scientific and practical approaches to the development of the methodological apparatus for assessing competencies in information security and the results of its pilot implementation in 2019–2020. The subject of the research is methodological tools, including evaluation tools (tests, cases), methods and procedures for organizing the assessment of information security competencies for evaluating candidates and employees. The results of the analysis of foreign practices, the survey of the demand for methodological tools in government bodies, the analysis of the regulatory and methodological support for the assessment of informa-

tion security competencies are presented. This conceptual approaches to the development of competency models, assessment tools and assessment procedures taking into account the requirements of normative acts in the field of information security, the characteristics of the target groups of employees estimated and evaluation purpose. The approbation of the methodological apparatus confirmed its practical value for the authorities. It is assumed that the use of methodological tools will make it possible to obtain the necessary analytical information to determine the tasks and select programs for the development of competencies, which may also be in demand in educational organizations engaged in the training of state civil servants.

**Keywords:** information security; public service; information security assessment; assessment of public servants; evaluation methodology.

**Citation:** Sladkova, N.M., Il'chenko, O.A., Stepanenko, A.A. & Shaposhnikov, V.A. (2021). Osobennosti otsenki kompetentsii po informatsionnoi bezopasnosti gosudarstvennykh i munitsipal'nykh sluzhashchikh [Features of the Assessment of Information Security Competencies of State and Municipal Employees]. *Public Administration Issues*, no 1, pp. 122–149 (in Russian).

## REFERENCES

1. Alekseeva, L.N. (2015). Sistema informacionnoy bezopasnosti organov gosudarstvennoy vlasti kak osnova sovremennogo gosudarstvennogo upravleniya [Information Security System of Public Authorities as the Basis of Modern Public Administration]. *Vestnik universiteta*, no 13, pp. 5–9.

2. Barabashev, A. & Zaytseva, T. (2020). The Innovative HR Practices of Regional Administrations: Is it a New Round of Civil Service Reform in Russia? *NISPAcee Journal of Public Administration and Policy,* vol. 13, no 2, pp. 229–248.

3. Buraeva, L.A. (2014). Terroristicheskie ob"edineniya v global'nom informatsionnom prostranstve [Terrorist Associations in the Global Information Space]. *Probely v rossiyskom zakonodatel'stve*, no 3, pp. 274–276.

4. Buraeva, L.A. (2015). O nekotorykh voprosakh obespecheniya kiberbezopasnosti v sovremennykh usloviyakh [On Some Issues of Ensuring Cybersecurity in Modern Conditions]. *Teoriya i praktika obshchestvennogo razvitiya,* no 13, pp. 96–99.

5. ENISA (2019). Cyber Europe 2020. EU, ENISA 2019. Available at: https://www.cyber-europe.eu/img/CE2020_presentation.pdf (accessed: 05 November 2021).

6. Dvinskikh, D.Yu. & Talapina, E.V. (2019). Riski razvitiya oborota dannykh v gosudarstvennom upravlenii [Risks of Data Turnover Development in Public Administration]. *Public Administration Issues*, no 3, pp. 7–30.

7. Halin, V.G. & Chernova, G.V. (2018). Tsifrovizatsiya i ee vliyanie na rossiyskuyu ekonomiku i obshchestvo: preimushchestva, vyzovy, ugrozy i riski [Digitalization and its Impact on the Russian Economy and Society: Advantages, Challenges, Threats and Risks]. *Vlast' i ekonomika. Upravlencheskoe konsul'tirovanie*, no 10, vol. 118, pp. 46–63.

8. Kurakin, A.V. & Kostennikov, M.V. (2014). Gosudarstvennaya sluzhba i informatsionnaya bezopasnost' [Public Service and Information Security. Security Questions]. *Voprosy bezopasnosti*, no 6, pp. 18–67.

9. Markin, V.V. & Ostashkov, A.V. (Eds) (2008). *Monitoring v sisteme okazaniya gosudarstvennykh i munitsipal'nykh uslug kak instrument realizatsii strategii povysheniya kachestva gosudarstvennogo i munitsipal'nogo upravleniya: opyt, problemy, rekomendatsii.* Textbook [Monitoring in the System of Rendering State and Municipal Services as a Tool for Implementing a Strategy for Improving the Quality of State and Municipal Administration: Experience, Problems, Recommendations]. Moscow: Eksklibris Press.

10. Martynova, S.E. (2013). Kontseptsiya «servisnogo» gosudarstva v kontekste postindustrial'noy paradigmy sotsial'nogo upravleniya [The Concept of the «Service» State in the Context of the Post-Industrial Paradigm of Social Management]. *Vestnik Tumenskogo gosudarstvennogo universiteta*, no 8, pp. 165–173.

11. Potekhin, V.A. (2010). Sovershenstvovanie vlastnykh otnosheniy kak uslovie modernizatsii upravlencheskoy deyatel'nosti [Improvement of Power Relations as a Condition for the Modernization of Management Activities]. *Vlast'*, no 6, pp. 18–22.

12. Rman, M., Brezovšek, M. & Stare, J. (2020). The Measurement Model of Professional Operation of State Administration. *Central European Public Administration Review*, vol. 18, no 2, pp. 29–52.

13. Shkarlet, S., Oliychenko, I., Dubyna, M., Ditkovska & Zhovtok, V. (2020). Comparative Analysis of Best Practices in E-Government Implementation and Use of This Experience by Developing Countries. *Administratie Si Management Public*, no 34, pp. 118–136.

14. Sidorenko, E.L., Bartsits, I.N. & Khisamova Z.I. (2019). Otsenka effektivnosti tsifrovogo gosudarstvennogo upravleniya: Teoreticheskie i prikladnye aspekty [The Efficiency of Digital Public Administration Assessing: Theoretical and Applied Aspects]. *Public Administration Issues*, no 2, pp. 93–114.

15. Sokolova, E.I. (2020). Tsifrovye kompetentsii i novye tekhnologii v obrazovanii: po materialam dokumentov evropeyskoy komissii [Digital Competencies and New Technologies in Education: Based on the Materials of Documents of the European Commission]. *Neprerыvnoe obrazovanie: XXI vek*, no 2, vol. 30, pp. 121–133.

16. Tsirenshchikov, V.S. (2019). Tsifrovizatsiya ekonomiki Evropy [Digitalization of the European Economy]. *Sovremennaya Evropa*, no 3, pp. 104–112.

17. Vasil'eva, E.V., Pulyaeva, V.N. & Yudina, V.A. (2018). Razvitie tsifrovykh kompetentsiy gosudarstvennyhh grazhdanskihh sluzhashchihh Rossiyskoy Federatsii [Development of Digital Competencies of State Civil Servants of the Russian Federation]. *Biznes-informatika*, no 4, vol. 46, pp. 28–42.

18. World Population Review (2021). World Population Review, USA. 2021. Available at: https://worldpopulationreview.com/country-rankings/internet-users-by-country (accessed: 11 January 2021).