УДК 342.922: 004.043
DOI 10.52452/19931778_2024_3_90

КАДРОВАЯ ПОЛИТИКА В СИСТЕМЕ ГОСУДАРСТВЕННОЙ СЛУЖБЫ НА СТРАЖЕ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ ОТ ИНФОРМАЦИОННЫХ УГРОЗ В ЦИФРОВОЙ СРЕДЕ

О.В. Гречкина

Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации, Москва

grechkina74@rambler.ru

Поступила в редакцию 01.04.2024

Представлены результаты исследования, посвященного выявлению проблем формирования кадровой политики в сфере государственной службы в эпоху цифровой трансформации государственного аппарата. В данной сфере государственные служащие, являясь фактически первичным звеном государственного управления, наиболее подвержены угрозам цифровой безопасности. Обоснован вывод о том, что кадровая политика имеет решающее значение в обеспечении информационной безопасности личности государственного служащего; действующее правовое регулирование обработки персональных данных государственных служащих имеет ряд недостатков и несоответствий.

Ключевые слова: государственная служба, государственный служащий, кадровая политика, персональные данные, информационная безопасность личности, угрозы цифровой безопасности.

Успешная организация государственной службы является главным условием обеспечения высокого уровня качества реализации функций и задач государства, в том числе и через оказание государственных услуг. Повышение качества и доступность государственных услуг, оказываемых в электронной форме, в соответствии с Указом Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», является приоритетной целью государства на предстоящий период. Помимо организации взаимодействия органов государственной власти и местного самоуправления с гражданами, концепция цифрового государства предполагает решение вопросов интеграции цифровых и информационных технологий во внутреннюю организационную деятельность органов государственной власти и организацию государственной службы.

Важно учитывать, что специфика организации государственной службы предполагает реализацию беспрерывного вертикального и горизонтального взаимодействия. Цифровизация внутренней работы призвана ускорить такое взаимодействие [1, с. 271]. Кроме того, информационные технологии позволяют минимизировать затраты различных материальных ресурсов, которые необходимы для осуществления того же объема работы в условиях бумажного документооборота. В общей своей массе такие преимущества можно охарактеризовать как увеличение производственных показателей государственного аппарата при уменьшении затрат ресурсов и средств на достижение поставленных перед ним задач. При этом особенно значимым аспектом является организация кадровой работы государственных служащих, в том числе борьба с угрозами, которые возникают в связи с цифровизацией государственного аппарата. К ним можно отнести, к примеру, защиту персональных данных государственного служащего, цифровых прав государственных служащих, а также защиту государственного служащего от проявлений информационного терроризма, повышение уровня цифровой грамотности и пр.

Одной из таких угроз является ненадлежащая обработка и утечка персональных данных государственных служащих. Нормами действующего законодательства персональные данные государственного служащего в определенной степени наделены особыми правовыми мерами защиты. Правовое регулирование правоотношений в сфере персональных данных госслужащего, в первую очередь, основывается на понимании того, что относится к таким данным и какое значение эта информация имеет для безопасности самого государственного служащего.

В соответствии с пунктом 2 Положения «О персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», утвержденного Указом Президента Российской Федерации от 30 мая 2005 года № 609 (далее – Положение о персональных данных), к персональным данным относятся сведения о фактах, событиях и

обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность. Вместе с тем легальное определение персональных данных в широком понимании данного термина, которое предложено в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в значительной степени отличается, поскольку в данном случае под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

С правовой точки зрения эти два понятия соотносятся как частное и общее соответственно. Специальный правовой статус персональных данных связан, на наш взгляд, с публично-правовой значимостью занимаемой должности. Однако ненадлежащая защита персональных данных и, как результат, их компрометация могут поставить под угрозу как саму фактическую безопасность государственного служащего, так и непосредственно государственные интересы.

Пунктом 11 Положения о персональных данных определено, что персональные данные государственного служащего являются конфиденциальной информацией. Из указанной нормы следует логический вывод, что правовое регулирование обработки и передачи третьим лицам такой информации не должно содержать каких-либо неоднозначных положений, позволяющих каким-либо образом нарушить режим конфиденциальности персональных данных государственного служащего.

Вместе с тем правовые меры, применяемые к защите персональных данных государственного служащего, в определенной степени кажутся противоречивыми. Так, к примеру, в соответствии с пунктом 13 указанного Положения о персональных данных по вопросу об обработке персональных данных государственных служащих указано, что по обращению средств массовой информации могут предоставляться сведения в том числе об объектах недвижимости, находящихся в собственности у государственного служащего. В то же время пунктом 15 того же Положения о персональных данных установлен запрет на предоставление информации, позволяющей определить место жительства служащего, равно как и информации, позволяющей определить местонахождение объектов недвижимости, принадлежащих гражданскому служащему на праве собственности. Указанные положения в определенной степени противоречат друг другу, поскольку создают правовую неопределенность в объеме информации, который может или не может быть представлен, например, при наличии у служащего единственного объекта недвижимости, пригодного для проживания, или объема информации о нахождении объекта недвижимости.

Также важно отметить, что действующее Положение о персональных данных не содержит системного подхода к цифровому обороту персональных данных в системе правового регулирования и к перечню персональных данных как таковых. Так, к примеру, Положением о персональных данных не предусмотрен закрытый перечень персональных данных, подлежащих внесению в Единую информационную систему управления кадровым составом государственной гражданской службы, или персональных данных, подлежащих обработке. Поэтому правовой статус персональных данных государственного служащего и меры по защите этих данных, помимо технической обеспеченности кадровой работы органа, должны исходить из необходимости полного нормативного обеспечения процесса получения и обработки персональных данных государственного служащего.

В системе действующего нормативного регулирования правового положения гражданского служащего основные права закреплены статьей 14 Закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее – закон 79-ФЗ) и важно, что в перечне указанных прав существуют положения пункта 5 части 1 о праве на доступ к материалам, необходимым для исполнения должностных обязанностей, а также пункта 9 части 1 о праве на защиту сведений о гражданском служащем. Их природа отличается от природы цифровых и информационных прав, принадлежащих обычным гражданам, поскольку элементы правового статуса гражданского служащего основаны на публично-правовом значении занимаемой должности. Реализация указанных прав связана с осуществлением гражданским служащим профессиональных обязанностей и направлена на обеспечение служащего достаточным уровнем цифровой и информационной свободы, необходимой для реализации своих полномочий. Вместе с тем в условиях современного правового регулирования остается открытым вопрос о праве на свободный сбор и распространение информации и свободный доступ к информационным ресурсам.

Положения закона 79-ФЗ содержат нормы, которые в определенной степени затрагивают данное право. Так, нормой статьи 20.2 указанного закона установлена обязанность гражданина, претендующего на замещение должности гражданской службы, при поступлении на службу, а также гражданского служащего ежегодно предоставлять информацию об общедо-

ступной информации и сведениях, об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети Интернет», позволяющих идентифицировать его. Непредставление таких сведений представителю нанимателя влечет за собой невозможность пребывания гражданина на гражданской службе, а в отношении гражданина является ограничением для поступления на гражданскую службу.

При анализе данных положений возникает справедливый вопрос о сути подобного ограничения в части его значения для интересов государственной службы и государства в целом, а также о соотношении такого ограничения с правом на равный и свободный доступ к информационным ресурсам. Представляется, что целесообразность установления соответствующего ограничения, в определенной степени, продиктована интересами профессиональной этики [2, с. 161]. В научной среде существует мнение о том, что подобное ограничение носит антикоррупционный характер, направлено на купирование коррупционных рисков [3, с. 306]. Однако к такому доводу необходимо отнестись скептически, поскольку, на наш взгляд, наличие у представителя нанимателя сведений об общедоступных сведениях о гражданском служащем в ИТС Интернет не ограничивает гражданского служащего в коррупционном поведении.

С другой стороны, возникает вопрос о том, является ли само по себе данное требование ограничением или к такой категории можно отнести требования к информации, размещаемой гражданским служащим непосредственно на страницах сайтов. Частью 3 статьи 20.2 закона 79-ФЗ установлено, что уполномоченными лицами осуществляется обработка информации и сведений, размещенных на таких сайтах. Вместе с тем законодательного регулирования целей такой обработки, требований к размещаемой информации и результатов ее обработки недостаточно для того, чтобы сделать вывод о том, какое правовое значение имеет данное законоположение для совокупности цифровых и информационных прав гражданского служащего. Если рассматривать норму статьи 20.2 закона 79-ФЗ с точки зрения защиты интересов этики, то в действующей системе правового регулирования отсутствуют четко сформулированные требования к информации, размещаемой гражданским служащим в открытом доступе в ИТС Интернет, или иные этические нормы о «публичном информационном поведении» служащего.

Как результат, в системе правового регулирования сформировался пробел, связанный с недостаточной регламентацией цифровых и информационных прав гражданского служащего, а также ограничений, связанных с прохождением службы. Существующих норм общего правового регулирования на уровне федерального законодательства, очевидно, недостаточно для того, чтобы сделать вывод о надлежащей реализации права гражданских служащих на свободный сбор и распространение информации и свободный доступ к информационным ресурсам.

Для разрешения сложившейся правовой проблемы, очевидно, необходима доработка действующего законодательства в той части, что федеральное законодательство будет дополнено нормой, определяющей четкие требования к публичному поведению государственного гражданского служащего в том числе с использованием ИТС Интернет, нарушение которых будет определяться в зависимости от обстоятельств, предусмотренных законом, дисциплинарным проступком, административным или уголовным правонарушением. Именно при изменении действующего законодательства можно будет говорить о достижении высокого уровня реализации информационных и цифровых прав государственных гражданских служащих.

Также важным элементом обеспечения информационной безопасности личности при осуществлении кадровой работы в сфере государственной службы является повышение цифровой грамотности государственных гражданских служащих. Когда мы говорим о «цифровой зрелости» аппарата государственного управления, то, в первую очередь, мы подразумеваем «цифровую зрелость» ее первичных элементов – государственных служащих. Наличие у гражданского служащего определённого объема знаний и навыков в сфере информационных и цифровых технологий является острой необходимостью в условиях стремительной цифровизации государственного аппарата. При этом для уяснения развития кадровой работы по повышению профессиональных навыков в сфере новых технологий необходима четкая определенность в вопросе о том, что понимается под цифровой грамотностью и какой уровень цифровой грамотности является достаточным для гражданского служащего.

Рассуждая в данном контексте о цифровой грамотности, в первую очередь мы говорим о совокупности знаний и навыков гражданского служащего, предполагающих не только способность гражданского служащего ориентироваться в цифровом пространстве и использовать программное обеспечение, необходимое для реализации профессиональной функции, но и умение купировать и противостоять угрозам в сфере информационной безопасности как в интересах личности, так и в интересах службы и

государства. Дополнительным аспектом является наличие так называемого «цифрового неравенства» – явления, которое предполагает изначально разный уровень цифровой осведомленности разных людей в зависимости от различных обстоятельств (возраст, место жительства, индивидуальные особенности и т.д.).

В связи с этим одной из задач кадровой работы на государственной службе, в контексте профессионального развития гражданских служащих, является в том числе и нивелирование такого явления, как «цифровое неравенство». Также важно определить, что именно является критериями достаточной цифровой осведомленности гражданского служащего. С нашей точки зрения, это совокупность в первую очередь профессиональных компетенций, которые в должной мере обеспечивают исполнение профессиональной функции гражданским служащим в объеме собственной компетенции.

В правовой литературе цифровая грамотность представлена совокупностью пяти элементов, к которым относится информационная грамотность (способность искать и использовать информацию), цифровая информационная грамотность (предполагает навыки управления и передачи информации, обеспечения ее безопасности), медийная работа (навык понимания и восприятия средств массовой коммуникации), компьютерная грамотность (эффективное использование компьютера), коммуникативная грамотность (навык телекоммуникационного этикета) [4, с. 45]. Однако такой подход является применимым в том случае, если мы говорим о цифровой грамотности в целом, а не о тех навыках цифровой грамотности, которые необходимы для успешного осуществления трудовых функций лицом, на которое возложены публично-правовые обязанности и от чьей информационной грамотности зависят безопасность и интересы государства и общества.

Таким образом, классификацию компонентов цифровой грамотности необходимо устанавливать исходя из тех задач, которые в профессиональной среде ставятся перед гражданскими служащими. Условно данную категорию можно разделить на несколько компонентов, которые на практике соответствуют уровням цифровой грамотности:

1. Алгоритмические навыки – способность гражданского служащего исполнять свои профессиональные обязанности посредством цифровых технологий исключительно в рамках заранее определенной и прописанной последовательности действий;

2. Практико-технические навыки – способность гражданского служащего применять в своей профессиональной деятельности компьютерные и цифровые технологии без заранее заданного алгоритма, используя ограниченный спектр функций или программ;

3. Теоретико-технические навыки – способность гражданского служащего свободно ориентироваться в работе компьютерных и цифровых технологий, информационных систем и программном обеспечении, необходимых и достаточных не только для осуществления профессиональной деятельности, с пониманием теоретических основ и принципов работы таких технологий, систем и программного обеспечения, но и для превенции возможных угроз информационной безопасности личности и государства.

При этом важно отметить, что с учетом профессиональных функций гражданского служащего, а также интересов информационной безопасности личности и государства не является достаточным уровнем цифровой грамотности освоение исключительно одного или двух компонентов, таких как алгоритмические навыки и практико-технические навыки. При таких обстоятельствах гражданский служащий при осуществлении им профессиональной деятельности не может в полной мере гарантировать ни собственную безопасность в цифровой и информационной среде, ни безопасность государственных интересов.

Незнание теоретико-технических основ работы тех технологий, систем, программных обеспечений, которые используются служащим в своей работе, говорит о том, что наличие той или иной стандартной ситуации, не обеспеченной алгоритмом решения или ранее не встречавшейся гражданскому служащему на практике, фактически поставит его в положение, при котором, во-первых, невозможно выполнить поставленную задачу, а во-вторых, не представляется возможным обеспечить должную степень безопасности информации и сведений, с которыми гражданский служащий работает.

Иным аспектом являются навыки государственного служащего по обеспечению личной информационной безопасности и информационной безопасности государства. Очевидно, что при росте цифровой грамотности государственных служащих уровень угроз информационной безопасности соразмерно снижается, поскольку снижаются риски допущения непреднамеренной ошибки при работе с данными или технологиями. Вместе с тем при проведении кадровой работы необходимо учитывать важность разъяснительной работы о существующих информационных угрозах и способах их избежать. Дополнительным средством обеспечения информационной безопасности личности при кадровой работе являются меры по противодей-

ствию информационному терроризму, а точнее – реализация мероприятий по развитию навыков и профессиональных компетенций государственного гражданского служащего по распознаванию угроз информационного террора и борьбе с его проявлениями.

Государственный гражданский служащий в силу исполнения им должностных обязанностей, наличия компетенций по принятию тех или иных решений, административно-властных полномочий, а также доступа к конфиденциальной информации или государственной тайне в наибольшей степени подвержен угрозам информационного терроризма, который может проявляться в различных формах. Например, таких как шантаж, запугивание, угрозы, похищение персональных и иных данных с целью манипуляций, непосредственное или косвенное психологическое воздействие и т.д. При таких условиях особое значение имеет совершенствование кадровой работы в сфере государственной службы, которая должна предполагать действия, направленные на повышение соответствующих профессиональных навыков и общей осведомленности служащих о противодействии информационному терроризму. В рамках просветительской деятельности, проводимой под эгидой кадровой работы, необходимо аккумулировать и обработать существующие источники угроз, возможные сферы проявления актов информационного терроризма. Кроме того, в рамках кадровой работы, на наш взгляд, надлежит осуществлять работу по оценке рисков быть подвергнутым воздействию информационного терроризма (виктимность в сфере киберпреступности) в отношении каждого кадра государственной гражданской службы в том или ином государственном органе.

Понятно, что такая деятельность подразумевает значительный объем работы и информации, которую надлежит обработать и оценить по тем или иным критериям. Соответственно, на наш взгляд, для организации такой работы в тех государственных органах, где виктимность служащих в сфере киберпреступности наиболее высока, необходимо создание специального отдела кадровой службы или как минимум подготовка ряда специалистов, уполномоченных на сбор, обработку информации, которая содержится в личных делах или подлежит включению в личные дела государственных служащих. В данном случае вновь возникает вопрос о реализации информационных, а также личных прав государственных служащих, в отношении которых в рамках данной процедуры будет оцениваться уровень виктимности в сфере информационного терроризма. Заметим, что большая часть информации, необходимой для оценки данного показателя, не относится к тем сведениям, которые находятся в личных делах или подлежат внесению в личные дела государственных гражданских служащих.

Так или иначе, необходимость получения таких сведений и оценки таких угроз зависит от должности, которую занимает государственный служащий, и от потенциальных рисков в сфере информационной безопасности, которые связываются с занимаемой государственным служащим должностью. Такие критерии целесообразности, на наш взгляд, надлежит оценивать в каждом органе отдельно. В любом случае угрозу акта информационного терроризма, осуществленного в отношении государственного служащего, можно в определенной степени нивелировать и способами, не затрагивающими частную жизнь государственного служащего. К таким средствам относится создание и внедрение технологий, не позволяющих государственному служащему использовать на рабочем месте и при осуществлении профессиональных функций те информационные ресурсы, сети и устройства, которые в определенной степени несут риск информационного воздействия и проявления актов информационного терроризма.

Иностранный опыт кадровой работы по повышению цифровой грамотности и противодействия информационным угрозам, в том числе угрозам информационного терроризма, богат примерами успешного подхода, основанного на принципе превентивного действия. Зарубежная практика показывает нам, что обучение кадрового состава высоким навыкам использования цифровых и информационных технологий должно начинаться еще на ранних этапах подготовки молодых кадров и иметь масштабы общегосударственной программы. Действующие в иностранных государствах программы, как показывает практика, в основном ориентированы на формирование конкретных навыков в зависимости от сферы. Основное направление программ занимает обеспечение информационной безопасности. В большинстве стран эта задача поставлена во главу. Вместе с тем широко развиты образовательные программы, которые позволяют будущим кадрам осваивать коммуникативные навыки и основы безопасности такой коммуникации на различных площадках: социальные сети, государственные информационные системы и т.д.

Интересным является опыт Великобритании, где в значительной степени сделан упор на повышение навыков работы со средствами массовой информации и социальными сетями. Очевидно, что такой упор сделан ввиду того, что

именно такие навыки формируют публичный характер государственной службы, а также позволяют купировать риски, связанные с нежелательными утечками конфиденциальной или иной информации через социальные сети и СМИ. Весьма актуальным является такой навык и в Российской Федерации, в контексте темы о публичной активности гражданских служащих в социальных сетях и требованиях к их публичному цифровому поведению. Также важно, что повышение цифровой грамотности кадров государственной службы в зарубежных странах, таких как, например, Сингапур, США, Великобритания, осуществляется вне зависимости от направления и сферы профессиональной деятельности служащего [5, с. 226].

Подводя итог, можно сформулировать ряд логических выводов, которые имеют решающее значение для успешного формирования кадровой политики в сфере государственной службы в эпоху цифровой трансформации государственного аппарата с тем, чтобы в должной мере обеспечить информационную безопасность личности и государства.

Цифровизация государственного аппарата на сегодняшний день является одной из качественных характеристик достижения глобальной цели цифровой трансформации государства и общества.

Очевидно, что новые технологические веяния в сфере организации государственного управления необратимо порождают угрозы цифровой безопасности личности и государства.

Государственные служащие, являясь фактически первичным звеном государственного управления, занимая должности, имеющие публично-правовое значение, наиболее подвержены таким угрозам.

Кадровая политика, как совокупность целей, принципов, мер и инструментов, направленных на наиболее успешную реализацию человеческого ресурса в интересах задач государственного управления, имеет решающее значение в обеспечении информационной безопасности личности государственного служащего.

Действующее правовое регулирование обработки персональных данных государственных служащих имеет ряд недостатков и несоответствий. К таким недостаткам, в первую очередь, необходимо отнести недостаточное правовое регулирование вопроса о понятии персональных данных государственного служащего и об исчерпывающем перечне предоставляемых государственным служащим персональных данных, сведениях, о порядке их передаче третьим лицам, в том числе в средства массовой информации.

Статья подготовлена в рамках научно-исследовательской работы на основании государственного задания Российской академией народного хозяйства и государственной службы при Президенте Российской Федерации № 5.5-2023-1 «Совершенствование законодательства в области защищенности личности от информационных угроз в цифровой среде».

Список литературы

1. Рыбакова М.В., Иванова Н.А. Цифровые технологии в современной системе государственной службы // Социология. 2022. № 2. С. 271–280.

2. Куценко Е.С. Некоторые особенности реализации в прокуратурах нормы закона о представлении сведений об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет» // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2021. № 4. С. 159–164.

3. Гудулова Г.О. Контроль поведения госслужащих в Интернете как средство повышения доверия органам государственной власти // АНИ: экономика и управление. 2018. № 1 (22). С. 305–307.

4. Овчинников С.С. Оценка цифровой грамотности государственных служащих // Политика и общество. 2022. № 4. С. 42–50.

5. Кайсарова В.П., Винокурова М.Ю. Профессиональное развитие цифровых компетенций современных государственных служащих: российский и зарубежный опыт // Государственное управление. Электронный вестник. 2021. № 88. С. 216–232.

PERSONNEL POLICY IN THE PUBLIC SERVICE SYSTEM IS ON GUARD TO ENSURE THE PROTECTION OF THE INDIVIDUAL FROM INFORMATION THREATS IN THE DIGITAL ENVIRONMENT

O.V. Grechkina

The results of a study devoted to identifying the problems of personnel policy formation in the field of public service in the era of digital transformation of the state apparatus are given. In this area, civil servants, being in fact the primary link of public administration, are most vulnerable to threats to digital security. The conclusion is substantiated that personnel policy is crucial in ensuring the information security of a civil servant's personality; The current legal regulation of the processing of personal data of civil servants has a number of shortcomings and inconsistencies.

Keywords: civil service, civil servant, personnel policy, personal data, personal information security, threats to digital security.

References

1. Rybakova M.V., Ivanova N.A. Digital technologies in the modern system of public service // Sociology. 2022. № 2. P. 271–280.

2. Kutsenko E.S. Some features of the implementation in prosecutor's offices of the law on the provision of information about the addresses of sites and (or) pages of sites in the information and telecommunications network «Internet» // Scientific notes of the V.I. Vernadsky Crimean Federal University. Legal sciences. 2021. № 4. P. 159–164.

3. Gudulova G.O. Control of the behavior of civil servants on the Internet as a means of increasing trust in public authorities // ANI: economics and management. 2018. № 1 (22). P. 305–307.

4. Ovchinnikov S.S. Assessment of digital literacy of civil servants // Politics and society. 2022. № 4. P. 42–50.

5. Kaisarova V.P., Vinokurova M.Yu. Professional development of digital competencies of modern civil servants: Russian and foreign experience // Public administration. Electronic bulletin. 2021. № 88. P. 216–232.