УДК 336.1+351
JEL: H83
DOI 10.24147/1812-3988.2023.21(2).89-98

БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ В ПУБЛИЧНОМ УПРАВЛЕНИИ: ТРЕБОВАНИЯ К ЧИНОВНИКАМ

С.В. Анисимова, М.А. Зырева

Тверской государственный университет (Тверь, Россия)

Информация о статье
Дата поступления
10 февраля 2023 г.

Дата принятия в печать
22 марта 2023 г.

Тип статьи
Обзорная статья

Ключевые слова
Государственная гражданская служба, сервисное государство, требования, компетенции, кибербезопасность, профиль должности государственного гражданского служащего

Аннотация. В статье раскрыты тенденции изменения вопросов работы в цифровой среде и кибербезопасности сервисов вообще и публичного сектора в частности. Данные тенденции способствуют изменениям в требованиях к государственным гражданским служащим в части изменения требований к их цифровым знаниям, умениям, компетенциям. Раскрыто содержание понятия «кибербезопасность», выделены цифровые компетенции чиновников для безопасной работы в публичном цифровом пространстве. Обоснована необходимость рассмотрения блока безопасного поведения и пользования Интернета в рамках понятия «культура безопасности». Высказано предложение о внесении изменений в раздел П.16 «Управление в сфере цифрового развития, информационных технологий, связи, массовых коммуникаций и средств массовой информации» Справочника квалификационных требований, а именно: требований к профессиональным знаниям и знаний в сфере российского законодательства в части *IT*-безопасности, даны конкретные формулировки. Даны направления дальнейших исследований по теме.

CYBERSPACE SECURITY IN PUBLIC ADMINISTRATION: REQUIREMENTS FOR OFFICIALS

S.V. Anisimova, M.A. Zyreva

Tver State University (Tver, Russia)

Article info
Received
February 10, 2023

Accepted
March 22, 2023

Type paper
Review

Keywords
State civil service, service state, requirements, competencies, cybersecurity, profile of the position of a state civil servant

Abstract. The article reveals trends in the issues of work in the digital environment and cybersecurity of services in general, and in particular, the public sector, which contribute to changes in the requirements for public civil servants in terms of changing the requirements for their digital knowledge, skills, and competencies. The authors revealed the content of the concept of "cybersecurity", highlighted the digital competencies of officials for safe work in the public digital space. The article substantiates the need to consider the block of safe behavior and use of the Internet within the concept of "safety culture". The authors proposed amendments in the section of P.16 "Management in the field of digital development, information technology, communications, mass communications and mass media" of the Handbook of qualification requirements: requirements for professional knowledge and knowledge in the field of legislation of the Russian Federation in terms of IT security, specific formulations are given. The authors give directions for further research on the topic.

1. Введение. Взаимодействие в цифровой среде использует разные способы, несёт определённые угрозы, а значит требует формирования навыков выживания и правил поведения. Эксперты отмечают, что количество кибератак на госсектор России выросло в 2022 г. в несколько раз (по другим оценка на 80 %) (https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире#). Это подтверждает значимость проведения исследований требуемых знаний и умений (компетенций) чиновников и органов власти в области кибербезопасности при осуществлении функций публичного управления.

Истоки киберпреступности уходят корнями в телекоммуникации, а «хакерская» культура происходит от «телефонного фрикинга», который достиг пика в 1970-х гг. [2]. Появление проблем с цифровой безопасностью возникло с появлением первых серьёзных угроз корпоративным и государственным системам данных. Одним из самых известных хакеров, с появлением которого и связывают эти проблемы стал Кевин Митник. Его известное высказывание – «взломать человека гораздо проще, чем компьютер» в настоящее время раскрывается в новом свете и смысле. Особенно на фоне закона о ЕБиС (Федеральный закон от 29.12.2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты РФ и признании утратившими силу отдельных положений законодательных актов РФ»), когда государство должно определить правила работы с персональными данными и биометрией, обеспечить безопасное их использование. Сегодня К. Митник – консультант по безопасности, что символизирует изменения к понятию и подходам к *IT*-безопасности. *IT*-безопасность перестала быть «системой сохранения тайны», безопасность стала культурой и общекорпоративной ценностью. Это составная часть «культуры безопасности» – комплексного термина, появившегося после Чернобыльской аварии [3]. В условиях активного вовлечения в киберпространство трудовых ресурсов страны, вопросы безопасного взаимодействия в нем усиливаются, что обуславливает необходимость включения блока «безопасность в киберпространстве» в понятие «культура безопасности».

На государственном уровне многие страны имеют собственный взгляд на вопросы кибербезопасности, что отражено в их концептуальных стратегических документах. Среди них:

– «Стратегия национальной безопасности» США;

– Закон о кибербезопасности КНР;

– Правила Евросоюза по безопасности сетевых и информационных систем»;

– Доктрина информационной безопасности РФ;

– Национальная программа «Цифровая экономика» обозначила не только цифровые цели и векторы развития национальной экономики;

– Концепция формирования и развития культуры информационной безопасности граждан РФ (далее – Концепция).

Стратегические ориентиры развития института государственной службы, построения сервисного государства отражают мировой запрос на развитие государства и его сервисов. Это в свою очередь усиливает важность и скорость изменений в требованиях к квалификации государственных гражданских служащих (далее – ГГС), в частности к их цифровым знаниям и умениям. Так, вопросы безопасного и компетентного управления в публичном секторе актуальны по причинам: обширного нахождения в киберпространстве граждан страны, органов власти; наличием и активным ростом киберпреступности; расширением понятия «культура безопасности»; построением сервисного государства, принятием доктрины информационной безопасности страны.

2. Обзор литературы. В условиях наращивания цифрового потенциала РФ обозначены новые национальные цели и направления развития, в частности – в области кибербезопасности. Концепция обозначила направления мероприятий и активности государственных органов власти в области формирования компетенций граждан и ГГС в области кибербезопасности.

В российской практике используется концепция цифровых компетенций, сформулированная в Европейской рамке квалификаций (проект Еврокомиссии DigComp 2.0), она изложена в [4]. А.М. Ташбаевым, А.А. Маликовым, К.Г. Жакшылык дана классификация цифровых навыков и компетенций [5]. В российской практике локализованная версия сервиса DigComp 2.0 получила название «Независимая

оценка компетенций цифровой экономики» на портале «Готов к цифре», успешное применение сервиса позволило сформировать и диагностировать базовые цифровые компетенции, но в отношении специальных цифровых компетенций локализованные сервисы отсутствуют, а национальные методики оценки специальных навыков далеки от систематичности изложения, принятой для каркасных моделей.

Более детальное раскрытие цифровых компетенций в области кибербезопасности, можно найти в источнике [6], но оно сформировано для руководящего состава предприятий, нуждается в существенной детализации навыков и связанных с ними компетенций, адаптации для государственной службы.

Вопрос разрозненного состояния знаний и требований в области безопасного использования интернета волнует учёных всего мира [7; 8]. Вопросы, которые затрагиваются в научных исследованиях касаются, в том числе, и геостратегической ориентации в регулировании этих вопросов (ориентация на опыт Запада или Востока?) [9].

В большей части исследование компетенций в области кибербезопасности сосредоточено на формировании кадрового обеспечения кибербезопасности России [10]. Проблематика необходимости трансформации компетенций чиновников находит отражение в научной среде и формирует новое поле исследований [11].

В практике Евросоюза, ориентированной на использование общепринятых каркасных моделей и максимального раскрытия информации, в том числе машиночитаемых форматах, можно найти эффективную практику исследования цифровых компетенций в разных отраслях экономики, а также ГГС в государственном секторе (https://www.cedefop.europa.eu/en/tools/skills-intelligence/sectors?sector=06.14#5).

В статье [12] делают акцент на развитии региональных моделей профессиональных компетенций для цифровой экономики.

Анализ зарубежных источников позволяет говорить о поддержке тренда построения сервисного государства. Так в статье [14] затронуты вопросы оцифровки внутренних операций государственного управления. Растущее число мобильных и беспроводных устройств является ключевой причиной растущего значения и интереса к мобильному правительству [13]. В статье [15] приводится описание опыта использования открытых публичных источников (форумов) в рамках реализации государственных программ, показано как в политику можно встроить социальные технологии, но при этом быть нейтральными политически и полезными гражданам. В рамках проводимого авторами исследования основной интерес к материалам источника состоит в описании элементов компетенций ГГС в публичном представлении интересов в сети.

Таким образом, обзор научной литературы позволяет сделать выводы об обращении исследователей к вопросам кибербезопасности, цифровым компетенциям и цифровым компетенциям, включающим блок кибербезопасности. Отдельно стоит вопрос о построении сервисного государства и работе чиновников в новых условиях. Мало работ, посвященных цифровым компетенциям чиновников. Это может объясняется спецификой регулирования рынка труда, а также недавним принятием стратегии и концепции в этой сфере (декабрь 2022 г.). Это лишь подчёркивает значимость поставленных авторами статьи задач в анализе и разработке рекомендаций по вопросу компетентного управления безопасность в рамках публичного управления при работе в киберпространстве.

3. Гипотезы и методы исследования. Гипотеза исследования заключается в том, что на фоне роста значимости цифровых сервисов в России и зарубежом, реализуемых как элемент клиентоцентричности государства, меняются требования к компетенциям ГГС в вопросах обеспечения безопасности результатов их ежедневной деятельности, а также безопасного взаимодействия с населением.

Эти требования касаются и вопросов безопасной деятельности сервисов передачи служебной информации, и подходов ГГС к их использованию, и их готовности к работе в цифровой среде, которая может подвергаться киберугрозам. Это значит, что каждый сотрудник органов государственной власти (и государственный гражданский служащий, и прочие сотрудники, не занятые на должностях государственной гражданской службы) должен обладать новыми цифровыми компетенциями, в том числе – в сфере безопасности. И это требование должно быть отражено в профиле компетенций по должности, квалификационных требованиях Минтруда.

Среди методов исследования стоит отметить общие: анализ, классификация, аналогия;

частные: сравнение, описание, моделирование. Авторами был проведён теоретический анализ экономической, управленческой и нормативно-правовой литературы по теме исследования, учтён отечественный и зарубежный опыт.

4. Результаты исследования. Обеспечение информационной безопасности РФ – крайне важная задача, подразумевающая создание соответствующих спецподразделений внутри госструктур [16]. Важно исследовать и действующие требования к чиновникам, их компетенциям в цифровой среде, в частности тех, что заняты вопросами кибербезопасности с целью их трансформации к требованиям меняющихся сервисов государств и прочим факторам.

В свою очередь, классификация цифровых навыков и компетенции формируется по 5 основным направлениям: информационная грамотность, коммуникация и сотрудничество, создание цифрового контента, безопасность, решение проблем и профессиональные компетенции [18]. Опыт применения оценки компетенций в такой классификации представлен проектом «Еврокомиссии» DigComp 2.0.

В международной практике взаимосвязи профессиональных сводов знаний и международных стандартов куррикулумов и их влияние на модели профессиональных навыков достаточно тесно переплетены между собой [19].

Авторы статьи [12] предлагают региональную модель профессиональных компетенций для цифровой экономики, в основе которой цифровые компетенции: итерация, аналитика, безопасность, работа с биг-дата. После этого по значимости идут навыки проектного управления, аналитические способности, знания иностранных языков, проактивность, способность к образованию, эмоциональный интеллект и прочее. Уточним, что эта модель предлагается вообще для экономики, без привязки к конкретной деятельности или сфере.

Для формирования модели цифровых компетенций в области кибербезопасности ГГС и граждан РФ можно воспользоваться приведённой выше каркасной моделью. Однако в РФ есть нормативно-правовые особенности для органов власти при приеме работников: квалификационные требования для замещения должностей государственной гражданской службы разработаны Минтрудом России (https://mintrud.gov.ru/ministry/programms/gossluzhba/16/1) (далее – Справочник). В них в области информационно-коммуникативных технологий (далее – ИКТ) выделены пять направлений требований:

«– знания основ компьютерной безопасности и защиты информации;

– знания основных положений законодательства о персональных данных;

– знания общих принципов функционирования системы электронного документооборота;

– знания основных положений законодательства об электронной подписи;

– основные знания и умения по применению персонального компьютера».

Изложенные в методических материалах Минтруда подходы активно используются при поступлении на должности ГГС, процедурах аттестации и формировании кадрового резерва. Однако, как показывает анализ, этих компетенций недостаточно для эффективной работы в современном и строящемся сервисном государстве.

В настоящее время есть чёткое понимание возможности и способности к самостоятельной разработке в России безопасной модели поведения в отношении многих инструментов цифрового мира:

• навыки работы с текстовыми и табличными редакторами, графическими пакетами;

• использование принтеров и периферийных устройств,

• использование модемов, передача данных;

• применение резервного копирования и инструментов восстановления данных;

• навыки работы в браузерах;

• понимание работы интернет-провайдеров и широкополосного доступа в Интернет;

• хранение своего музыкального и медийного контента;

• поведение в социальных сетях, сообществах;

• поиск новостных блоков, использование блогов;

• правила формирования паролей и первично безопасного поведения.

Концепция не формирует списка направлений безопасного поведения гражданина, но явно обязывает органы государственной власти обеспечить «реализацию мероприятий по повышению грамотности по вопросам информационной безопасности». Важно понимать, что для формирования прочного цифрового фундамента необходимо формирование уве-

ренных навыков и безопасной модели поведения чиновника и гражданина в сервисном государстве по направлениям:

• использования и организации работы мобильных приложений, в том числе применения геопозиции;

• модели использования услуг через социальные сети;

• навыков работы с видео, подкастами, применения цифровых камер;

• использование цифровых форматов сотрудничества через API, IFTTT;

• навыков работы с данными (в том числе личные данные), цифровой аналитикой;

• принципов организации и применения биометрических данных, цифровой аутентификации;

• применение виртуализации, расширений приложений, виртуальной и дополненной реальностью;

• навыков использования агентов, ботов, аватаров и мн. др.

Эти направления рекомендовано учитывать при разработке мероприятий повышения грамотности граждан. Изменения цифровой среды постоянны и нарастают в геометрической прогрессии, что требует регулярных изменений в глобальной и страновой повестки кибербезопасности. Подготовка к следующему поколению киберпреступности, требует нескольких вещей от интернет-пользователей. Это и защита устройств с помощью антивирусного программного обеспечения, и осведомлённость о текущих тенденциях угроз для предотвращения просмотра ваших данных внешними субъектами, и сопряжение антивирусного программного обеспечения с доверенным VPN, заворачивающим веб-трафик пользователя в туннель шифрования. Эти меры способны остановить большинство киберпреступлений, но это не спасают от атак опытных киберпреступников [2].

Для усиления основ грамотности по вопросам информационной безопасности авторы считают уместным введение дополнительных требований к цифровым компетенциям специалистов в области *IT*-безопасности. Они формируются сочетанием навыков, знаний и умений в областях (доменах компетенций). Опираясь на Справочник, авторами разработан прототип онтологии рекомендованных цифровых компетенций специалистов в области *IT*-безопасности для ГГС, приведенный ниже.

Отметим, что данные рекомендации относятся к П.16 «Управление в сфере цифрового развития, информационных технологий, связи, массовых коммуникаций и средств массовой информации» Справочника, в части требований к профессиональным знаниям и профессиональным умениям.

Таблица 1. **Цифровые компетенции специалистов в области *IT*-безопасности для ведения профессиональной служебной деятельности ГГС**

Table 1. **Digital competencies of specialists in the field of IT security for conducting professional official activities of state civil servants**

Д.1) Домен «Понимание» – дополнение к п. 16, блок «Иные профессиональные знания»
1.1.4. Российские и международные стандарты и методологии, регулирующие жизненный цикл информационных систем, включая системы хранения и обработки данных, принципы интеграции информационных систем;
1.1.5. российские и международные стандарты, регулирующие жизненный цикл и требования к цифровым продуктам (государственным и муниципальным услугам, предоставляемым в электронном виде гражданам и организациям, информационным системам и цифровым платформам);
1.1.6. технологии формирования и развития организационной культуры цифровой трансформации;
1.1.7. основные нормативные акты регулирующие процессы проектирования и строительства в области информационных технологий, связи (ГОСТы, СниПы, РД)
Д.2) Домен «Безопасность данных и конфиденциальность» – дополнение к п. 16.7, блок «Иные профессиональные знания»
7.22. Комплекс мер по повышению надежности и обеспечению непрерывности оказания услуг, предоставляемых государственным органом в электронном виде с учетом методов и инструментов обеспечения безопасности данных;
7.23. принципы, требования и порядок предоставления государственных услуг исполнения государственных функций;
7.24. область защиты персональных данных;
7.25. общие вопросы в области обеспечения информационной безопасности;

Окончание табл. 1
The end of Table 1

7.26. понятие аппаратного и программного обеспечения, форм и методов работы с применением автоматизированных средств управления; 7.27. возможности и особенности применения современных информационно-коммуникационных технологий в государственных органах, включая использование возможностей межведомственного документооборота; 7.28. понятие несанкционированного доступа к информации; 7.29. порядок определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; 7.30. основные меры и способы защиты информации от несанкционированного доступа; 7.31. основные средства защиты информации и контроля защищенности информации; 7.32. основные способы оценки эффективности мер защиты информации от несанкционированного доступа
Д.3) Домен «Цифровая идентификация» – дополнение к п. 16, блок «Иные профессиональные знания» 1.1.8. Понимание и применение «Единой системы авторизации и идентификации»; 1.1.9. понимание и применение идентификационного номера налогоплательщика; 1.1.10. применение инструментов и методов идентификации, оценки, реагирования, мониторинга и контроля рисков и возможностей проекта; 1.1.11. понимание и применение идентификационной экспертизы товаров и технологий; 1.1.12. понимание и применение электронной цифровой подписи и машиночитаемых доверенностей
Д.4) Домен «Правовые основы» – дополнение блоков п. 16.1 и 16.2 «Иные профессиональные знания» 2.13. В П.16.1 знание нормативных правовых актов Российской Федерации и методических документов ФСТЭК России в области защиты информации; 2.19. в П.16.2. знание национальных, межгосударственных и международных стандартов в области защиты информации, в том числе ГОСТ Р ИСО/МЭК 15408 (1-3), ГОСТ Р ИСО/МЭК 27001, 27002, 27004, 27005, 27033, 56545, 53109, 34.10, 34.13, 28147
Д.5) Домен «Архитектура и технологии» – дополнение в п. 16.7, блок «Иные профессиональные знания» 7.33. Принципы создания хранилищ данных; 7.34. методы и технологии работы с данными; 7.35. методы математического моделирования, системного анализа, статистического анализа; 7.36. требования к работе с неструктурированными данными; 7.37. методы и инструменты обеспечения безопасности данных; 7.38. технологии обработки больших данных: создание прогностических моделей, поиск шаблонов данных; 7.39. системы распределенного реестра (блокчейн); 7.40. основы работы инженерных систем, каналов связи и сетей (беспроводные, проводные, оптические); серверного оборудования; инфраструктурного программного обеспечения; принципов построения систем управления базами данных и объектно-ориентированного программирования; систем резервного копирования данных (ленточные библиотеки); построения систем виртуализации; 7.41. облачные решения и особенности их использования; 7.42. основные технологические стеки для разработки современных цифровых решений, в том числе на основании облачных технологий; 7.43. особенности проектирования и построения отказоустойчивых решений; 7.44. особенности создания, внедрения и развития цифрового продукта

На основании рекомендуемых дополнений в части цифровых компетенций в сфере *IT*-безопасности ГГС, авторами составлен рекомендуемый для применения профиль цифровых компетенций в сфере *IT*-безопасности ГГС региона (на примере Тверской области) (табл. 2).

Стоит подчеркнуть, что для чиновников профильных министерств, управлений и отделов или просто должностей профиль должен быть разработан дополнительно, в более глубоко проработанном варианте с чётким указанием необходимых для использования методов, приемов, инструментов, программ.

Таблица 2. **Профиль цифровых компетенций в сфере *IT*-безопасности ГГС региона (на примере Тверской области)**

Table 2. **Profile of digital competencies in the field of IT security of state civil servants of the region (on the example of the Tver region)**

Категории/группы должностей	*Требования на текущий момент для занятия должности*	*Дополнительные (рекомендуемые для включения) требования к цифровым компетенциям в области IT-безопасности*
«Руководители», «помощники (советники)», «специалисты» высшей и главной групп	Наличие высшего образования не ниже уровня специалитета, магистратуры. Дополнительные требования в зависимости от области и вида профессиональной служебной деятельности гражданского служащего	Д.1 Д.2 Д.3 Д.4 Д.5
«Руководители», «помощники (советники)» ведущей группы должностей гражданской службы, категории «специалисты» ведущей и старшей групп должностей гражданской службы, а также категории «обеспечивающие специалисты» главной и ведущей групп должностей гражданской службы	Наличие высшего образования	Д.1 Д.2 Д.3 Д.4
«Обеспечивающие специалисты» старшей и младшей групп должностей гражданской службы	Наличие профессионального образования	Д.1 Д.2 Д.3

5. Заключение. В результате проведённого исследования была подтверждена гипотеза о необходимости изменения требований к компетенциям ГГС в вопросах обеспечения безопасности результатов их ежедневной деятельности, а также безопасного взаимодействия с населением. А именно были:

1) обоснована необходимость включения в понятие «культура безопасности» вопроса безопасного поведения и пользования интернета, в частности, цифровыми сервисами государства;

2) дано определение понятию компетентность в сфере кибербезопасности;

3) выделены компетенции (как домены, включающие комплекс профессиональных знаний, умений) в сфере *IT*-безопасности для всех групп и категорий должностей ГГС;

4) доказана необходимость указания в Справочнике в разделе П.16. «Управление в сфере цифрового развития, информационных технологий, связи, массовых коммуникаций и средств массовой информации» требований к профессиональным знаниям и знаний в сфере законодательства РФ в части *IT*-безопасности (на момент написания статьи таковые отсутствуют).

5) предложены формулировки иных профессиональных знаний для внесения в указанный Справочник (табл. 1, 2).

Важностью предложенных авторами положений является их возможность применения в органах власти всех уровней (включая муниципальную службу, с корректировкой пунктов, исходя из требований в справочнике квалификационных требований для муниципальных служащих) при определении требований к поступающим на службу, а также в процессе прохождения аттестационных процедур.

Отдельного внимания и дополнительных решений требуют вопросы формирования модели компетенций для чиновников, непосредственно занятых вопросами *IT*-безопасности, и занятых остальными видами профессиональной служебной деятельности. Отдельного поиска решений требуют вопросы: изменения положений кодексов этики в части разработки и формирования положений цифровой этики.

Литература

1. *Gleick J.* The information: a history, a theory, a flood / J. Gleick. p. cm. Includes bibliographical references and index.

2. *Ляхнов М. В., Коршунова Е. Н.* Кибербезопасность: прошлое и будущее // Закон. Право. Государство. – 2022. – № 2 (34). – С. 66–69.

3. *Руденко В. А., Евдошкина Ю. А., Железнякова А. В., Жук А. В.* Культура безопасности как интегральный элемент в формировании профессиональных компетенций работников АЭС // Глобальная ядерная безопасность. – 2017. – № 2 (23). – С. 104–110.

4. *Сухомлин В. А., Белякова О. С., Климина А. С.* [и др.]. Модель цифровых навыков кибербезопасности. – М. : Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала «Лига интернет-медиа», 2021. – 294 с. – DOI: 10.25559/e3858-3795-1033-h.

5. *Ташбаев А. М., Маликов А. А., Жакшылык К. Г.* Цифровые навыки и компетенции для цифровой экономики: модели, структура и виды цифровых навыков // Финансовая экономика. – 2020. – № 2. – С. 430–435.

6. *Можаева Г. В., Александрова Л. Д., Пуляева В. Н.* Цифровые компетенции в модели актуальных компетенций управленческих кадров // Вестник Финансового университета. Гуманитарные науки. – 2020. – № 10 (6). – С. 49–55. – DOI: 10.26794/2226-7867-2020-10-6-49-55.

7. *Bernd W. Wirtz, Peter Daiser, Boris Binkowska.* E-participation: A Strategic Framework // International Journal of Public Administration. – 2018. – Vol. 41, iss. 1. – P. 1–12. – DOI: 10.1080/01900692.2016.1242620.

8. *Bernd W. Wirtz, Jan C. Weyerer.* Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats // International Journal of Public Administration. – 2017. – Vol. 40, no. 13. – P. 1085–1100. – DOI: 10.1080/01900692.2016.1242614.

9. *Tuba Eldem.* The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security // International Journal of Public Administration. – 2020. – Vol. 43:5. – P. 452–465. – DOI: 10.1080/01900692.2019.1680689.

10. *Нечай А. А.* Формирование профессиональной компетенции в области кибербезопасности у будущих учителей информатики // Вестник Ленинградского государственного университета им. А.С. Пушкина. – 2020. – № 4. – С. 114–124. – DOI: 10.35231/18186653_2020_4_114.

11. *Бритикова Е. А., Михайлова А. Д., Симонян Ж. С.* Трансформация модели компетенции государственных служащих в условиях цифровой экономики // Новая наука: новые перспективы: материалы IX Междунар. науч.-практ. конф. (Краснодар, 30 июня 2021 г.) / под общ. ред. А.С. Поповой, Е.А. Янпольской. – Краснодар : Автономная некоммерческая организация дополнительного профессионального образования «Институт стандартизации, сертификации и метрологии», 2021. – С. 84–88.

12. Developing personnel's new professional competencies in the context of the digital economy / E. Shcherbik, T. Patrakhina, A. Tagirova, T. Galynchik // Proceedings of the IX International Scientific and Practical Conference "Current problems of social and labour relations" (ISPC-CPSLR 2021) : Proceedings of the IX International Scientific and Practical Conference, Makhachkala, 16–17 December 2021. Vol. 646. – Amsterdam : Atlantis Press, 2022. – P. 374–381. – DOI: 10.2991/assehr.k.220208.066.

13. *Bernd W. Wirtz, Isabell Balzer, Daniel Schmitt.* Mobile Government: Research Development and Research Perspectives // International Journal of Public Administration. – 2021. – DOI: 10.1080/01900692.2021.1993910.

14. *Ongaro E.* The long and winding road towards the EU policy of support to Member States public administration reform: History (2000–2021) and prospects // Public Policy and Administration. – 2022. – DOI: 10.1177/09520767221117689.

15. Maggetti M., Papadopoulos Y. Happily unaccountable? Perceptions of accountability by public managers // Public Policy and Administration. – 2022. – DOI: 10.1177/09520767221074487.

16. *Борисенко А. В.* Понятие кибербезопасности. Кибербезопасность государственных органов // Актуальные проблемы развития экономических, финансовых и кредитных систем: сб. материалов X Междунар. науч.-практ. конф. (Белгород, 15 сентября 2022 г.). – Белгород : Белгородский государственный национальный исследовательский университет, 2022. – С. 297–299.

17. *Сухомлин В. А., Белякова О. С., Климина А. С.* [и др.]. Модель цифровых навыков кибербезопасности. – М. : Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала «Лига интернет-медиа», 2021. – 294 с. – DOI: 10.25559/e3858-3795-1033-h.

18. *Ташбаев А. М., Маликов А. А., Жакшылык К. Г.* Цифровые навыки и компетенции для цифровой экономики: модели, структура и виды цифровых навыков // Финансовая экономика. – 2020. – № 2. – С. 430–435.

19. *Сухомлин В. А., Белякова О. С., Климина А. С.* [и др.]. Модель цифровых навыков кибербезопасности. – М. : Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала «Лига интернет-медиа», 2021. – 294 с. – DOI: 10.25559/e3858-3795-1033-h; *Сухомлин В. А., Лебедь С. В., Белякова О. С.* [и др.]. Куррикулум дисциплины «Кибербезопасность». – М. : Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала «Лига интернет-медиа», 2022. – 402 с. – DOI: 10.25559/f6676-8117-2920-j.

References

1. Gleick, James. The information: a history, a theory, a flood / James Gleick. p. cm. Includes bibliographical references and index.

2. Lyaxnov M.V., Korshunova E.N. Kiberbezopasnost`: proshloe i budushhee // Zakon. Pravo. Gosudarstvo. 2022. № 2 (34). S. 66-69.

3. Rudenko V.A., Evdoshkina Yu.A., Zheleznyakova A.V., Zhuk A.V. Kul`tura bezopasnosti kak integral`nyi element v formirovanii professional`nykh kompetentsii rabotnikov AES // Global`naya yadernaya bezopasnost`. 2017. № 2 (23). S. 104-110.

4. Suxomlin V.A., Belyakova O.S., Klimina A.S. [i dr.]. Model` tsifrovykh navykov kiberbezopasnosti. Moscow, Fond sodeistviya razvitiyu internet-media, IT-obrazovaniya, chelovecheskogo potentsiala «Liga internet-media», 2021. 294 s. DOI: 10.25559/e3858-3795-1033-h.

5. Tashbaev A.M., Malikov A.A., Zhakshylyk K.G. Tsifrovye navyki i kompetentsii dlya tsifrovoi ekonomiki: modeli, struktura i vidy tsifrovykh navykov // Finansovaya ekonomika. 2020. № 2. S. 430-435.

6. Mozhaeva G.V., Aleksandrova L.D., Pulyaeva V.N. Tsifrovye kompetentsii v modeli aktual`nykh kompetentsii upravlencheskikh kadrov. Gumanitarnye nauki. Vestnik Finansovogo universiteta. 2020. 10(6). 49-55. DOI: 10.26794/2226-7867-2020-10-6-49-55.

7. Bernd W. Wirtz, Peter Daiser & Boris Binkowska (2018) E-participation: A Strategic Framework, International Journal of Public Administration, 41:1, 1-12, DOI: 10.1080/01900692.2016.1242620.

8. Bernd W. Wirtz, Jan C. Weyerer (2017) Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats, International Journal of Public Administration, 40:13, 1085-1100, DOI: 10.1080/01900692.2016.1242614.

9. Tuba Eldem (2020) The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security, International Journal of Public Administration, 43:5, 452-465, DOI: 10.1080/01900692.2019.1680689.

10. Nechai A.A. Formirovanie professional`noi kompetentsii v oblasti kiberbezopasnosti u budushhikh uchitelei informatiki // Vestnik Leningradskogo gosudarstvennogo universiteta im. A.S. Pushkina. 2020. № 4. S. 114-124. DOI: 10.35231/18186653_2020_4_114.

11. Britikova E.A., Mixailova A.D., Simonyan Zh.S. Transformatsiya modeli kompetentsii gosudarstvennyx sluzhashhikh v usloviyakh tsifrovoi ekonomiki // Novaya nauka: novye perspektivy: materialy IX Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Krasnodar, 30 iyunya 2021 goda / pod obshhei redaktsiei A.S. Popovoi, E.A. Yanpol`skoi. Krasnodar: Avtonomnaya nekommercheskaya organizatsiya dopolnitel`nogo professional`nogo obrazovaniya "Institut standartizatsii, sertifikatsii i metrologii", 2021. S. 84-88.

12. Developing personnel's new professional competencies in the context of the digital economy / E. Shcherbik, T. Patrakhina, A. Tagirova, T. Galynchik // Proceedings of the IX International Scientific and Practical Conference "Current problems of social and labour relations" (ISPC-CPSLR 2021): Proceedings of the IX International Scientific and Practical Conference, Makhachkala, 16–17 December 2021 . Vol. 646. Amsterdam: Atlantis Press, 2022. P. 374-381. DOI: 10.2991/assehr.k.220208.066.

13. Bernd W. Wirtz, Isabell Balzer, Daniel Schmitt (2021) Mobile Government: Research Development and Research Perspectives, International Journal of Public Administration. DOI: 10.1080/01900692.2021.1993910.

14. Ongaro E. (2022). The long and winding road towards the EU policy of support to Member States public administration reform: History (2000–2021) and prospects. Public Policy and Administration. DOI: 10.1177/09520767221117689.

15. Maggetti M., Papadopoulos Y. (2022). Happily unaccountable? Perceptions of accountability by public managers. Public Policy and Administration. DOI: 10.1177/09520767221074487.

16. Borisenko A.V. Ponyatie kiberbezopasnosti. Kiberbezopasnost` gosudarstvennyx organov // Aktual`nye problemy razvitiya ekonomicheskikh, finansovykh i kreditnykh sistem: sbornik materialov X Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Belgorod, 15 September 2022. Belgorod: Belgorodskii gosudarstvennyi nacional`nyi issledovatel`skii universitet, 2022. S. 297-299.

17. Suxomlin V.A., Belyakova O.S., Klimina A.S. [i dr.]. Model` tsifrovykh navykov kiberbezopasnosti. Moscow, Fond sodeistviya razvitiyu internet-media, IT-obrazovaniya, chelovecheskogo potentsiala «Liga internet-media», 2021. 294 p. DOI: 10.25559/e3858-3795-1033-h.

18. Tashbaev A.M., Malikov A.A., Zhakshylyk K.G. Tsifrovye navyki i kompetentsii dlya tsifrovoi ekonomiki: modeli, struktura i vidy tsifrovykh navykov // Finansovaya ekonomika. 2020. № 2. S. 430-435.

19. Suxomlin V.A., Belyakova O.S., Klimina A.S. [i dr.]. Model` tsifrovykh navykov kiberbezopasnosti. Moscow, Fond sodeistviya razvitiyu internet-media, IT-obrazovaniya, chelovecheskogo potentsiala «Liga internet-media», 2021. 294 p. DOI: 10.25559/e3858-3795-1033-h; Suxomlin V.A., Lebed` S.V., Belyakova O.S. [i dr.]. Kurrikulum distsipliny "Kiberbezopasnost`". Moscow, Fond sodeistviya razvitiyu internet-media, IT-obrazovaniya, chelovecheskogo potentsiala "Liga internet-media", 2022. 402 p. DOI: 10.25559/f6676-8117-2920-j.

Сведения об авторах

Анисимова Софья Викторовна – канд. экон. наук, доцент кафедры государственного управления
Адрес для корреспонденции: 170100, Россия, Тверь, пер. Студенческий, 12
E-mail: Anisimova.SV@tversu.ru; sophi2911@mail.ru
ORCID: 0000-0002-2201-8557
РИНЦ AuthorID: 1017901

Зырева Марина Александровна – старший преподаватель кафедры государственного управления
Адрес для корреспонденции: 170100, Россия, Тверь, пер. Студенческий, 12
E-mail: Zyreva.MA@tversu.ru; marinazyreva@gmail.com
ORCID: 0000-0001-8908-6899
РИНЦ AuthorID: 728654

About the authors

Sof'ia V. Anisimova – PhD in Economic Sciences, Associate Professor of the Department of Public Administration
Postal address: 12, Studencheskii per., Tver, 170100, Russia
E-mail: Anisimova.SV@tversu.ru; sophi2911@mail.ru
ORCID: 0000-0002-2201-8557
RSCI AuthorID: 1017901

Marina A. Zyreva – senior lecturer of the Department of Public Administration
Postal address: 12, Studencheskii per., Tver, 170100, Russia
E-mail: Zyreva.MA@tversu.ru; marinazyreva@gmail.com
ORCID: 0000-0001-8908-6899
RSCI AuthorID: 728654

Вклад авторов равнозначен

The contribution of the authors is equal

Для цитирования

Анисимова С. В., Зырева М. А. Безопасность в киберпространстве в публичном управлении: требования к чиновникам // Вестник Омского университета. Серия «Экономика». – 2023. – Т. 21, № 2. – С. 89–98. – DOI: 10.24147/1812-3988.2023.21(2).89-98.

For citations

Anisimova S.V., Zyreva M.A. Cyberspace security in public administration: requirements for officials. *Herald of Omsk University. Series “Economics”*, 2023, Vol. 21, no. 2, pp. 89-98. DOI: 10.24147/1812-3988.2023.21(2).89-98. (in Russian).