УДК 338.2(470):[004.056:316.776]

Л.В. Астахова

Проблемы культуры информационной безопасности в условиях цифровой экономики*

Выявлено противоречие между мировыми тенденциями развития компетенций человека (сотрудника организации в области информационной безопасности и гражданина), отраженными в международном праве и в зарубежной социальной науке и практике, и содержанием задач федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (2018). Показана ограниченность реализации системы повышения грамотности в области кибербезопасности как планируемого результата этой программы. Обоснована активная субъектная роль пользователя цифровых ресурсов в обеспечении информационной безопасности в условиях культуры цифрового общества и цифровой экономики. Изложены требования культурологического подхода к этой роли. Выявлены содержание понятия культуры информационной безопасности, факторы, влияющие на её уровень, а также проблема её развития в новых условиях.

Ключевые слова: *культура информационной безопасности, осведомленность, грамотность, сотрудник, организация, цифровая экономика, цифровая культура, цифровая безопасность, информационный центр, библиотека, машинное обучение*

DOI: 10.36535/0548-0019-2020-02-3

Цифровая трансформация общества актуализировала проблемы информационной безопасности личности, социума и государства в глобальном масштабе. Её технологии стремительно развиваются вслед за новыми угрозами, среди которых особую опасность занимают угрозы со стороны человека. Понимание их критичности пришло не сразу, долгое время доминировали технократические представления об этой сфере. Человек как главный источник угроз информационной безопасности изучается много лет, но по-прежнему остается критически важной областью теоретических и эмпирических исследований. Согласно отчету *PriceWaterhouseCoopers*, в 2018 г. основными источниками угроз безопасности были люди: сотрудники (30%), бывшие сотрудники (27%) и неизвестные хакеры (23%). Основные воздействия заключаются в компрометирующих записях о клиентах и сотрудниках, и в потере или повреждении личных данных [1]. Парадоксально, но при доминирующем числе инцидентов по вине человека только у 34% участников исследования внедрена программа повышения осведомленности сотрудников о различных аспектах безопасности. При этом обязательное обучение политике защиты данных и ее применение на практике организовано всего лишь у 31% респондентов [2].

В процессе решения проблемы снижения рисков информационной безопасности из-за человека используются разные термины: повышение осведомленности, грамотности, культуры информационной безопасности (ИБ), культуры кибербезопасности, культуры цифровой безопасности и др. Правда, последние два термина (культура кибербезопасности и культура цифровой безопасности) еще не вошли в число широкораспространенных.

В международных стандартах по обеспечению информационной безопасности широко используется понятие осведомленности – *Security Awareness*. Самое раннее упоминание «осведомленности» встречается в документе американского Национального института стандартов и технологий (*The National Institute of Standards and Technology – NIST*) NIST 800-16-1998 Information Technology Security Training Requirements: A Role- and Performance-Based Model (Требования к обучению безопасности информационных технологий: модель на основе ролей и производительности). В 2003 г. в NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program (Создание программы повышения осведомленности в области безопасности информационных технологий) появляется понятие *Security Awareness* [3].

Международные стандарты серии ISO/IEC 27000 (и их российские национальные аналоги ГОСТ Р ИСО/МЭК 27000) по управлению информационной безопасностью содержат как требования, так и реко-

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г., соглашение № 02.A03.21.0011).

мендации для организаций по обучению персонала вопросам информационной безопасности с целью повышения их осведомленности.

Согласно стандарту ISO/IEC 27000:2012 Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary (Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общий обзор и терминология), на реализацию и успешное внедрение системы менеджмента информационной безопасности (СМИБ), позволяющей организации достигать своих бизнес-целей, влияет большое количество факторов. Один из них – эффективная программа повышения осведомленности, обучения и подготовки по ИБ, доводящая до сведения всех сотрудников их обязанности по обеспечению ИБ, сформулированные в политиках и стандартах ИБ, и побуждающая их к соответствующим действиям [4].

Вопросам осведомленности по ИБ в стандарте ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements («Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента ИБ – Требования») посвящен подраздел 7.3. *Awareness* (Осведомленность). В нем приведены **требования** к лицам, осуществляющим работу под контролем организации: они должны быть осведомлены о политике ИБ; о своем вкладе в обеспечение эффективности системы менеджмента ИБ, включая выгоды от улучшения функционирования ИБ; о последствиях несоблюдения требований системы менеджмента ИБ [5].

Стандарт ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls (Информационная технология – Методы и средства обеспечения безопасности – Свод правил по мерам и средствам контроля и управления информационной безопасностью) содержит **рекомендации** по осведомленности, обучению и тренингам в области информационной безопасности. В разделе 8.2. «В период занятости» этого стандарта отмечается, что в организации необходимо обеспечить уверенность в том, что сотрудники и сторонние пользователи осведомлены о своих обязанностях в отношении ИБ и выполняют их. В пункте 8.2.2 *Information Security Awareness, Education and Training* (Осведомленность, обучение и подготовка в области ИБ) указано, что все сотрудники организации и при необходимости пользователи сторонних организаций должны проходить соответствующую программу информирования, обучение и подготовку и получать на регулярной основе обновленные варианты политик и процедур организации, необходимых для выполнения их рабочих функций. В этом же стандарте приведены конкретные рекомендации по разработке программы осведомленности и обучения в области ИБ [6].

Рекомендации по разработке программы информирования и обучения информационной безопасности представлены в п. 9.4.2 стандарта ISO/IEC 27003:2010 Information technology – Security techniques – Information security management systems implementation guidance (Информационная технология – Методы и средства обеспечения безопасности – Руководство по реализации системы менеджмента информационной безопасности) [7]. В новой версии этого стандарта приведенные рекомендации отражены в п.7.3. *Awareness* [8].

Повышение осведомленности сотрудников организации по вопросам ИБ – это также предмет различных рекомендаций и руководств. В 2008 г. силами агентства Европейского Союза по сетевой и информационной безопасности (ENISA) разработан документ «Information Security Awareness in Financial Organisations» («Осведомленность об информационной безопасности в финансовых организациях»), в котором приведены конкретные рекомендации для финансовых организаций [9]. В 2010 г. разработаны новые рекомендации, которые распространяются на все сферы деятельности и содержат подробное описание действий по организации процесса осведомленности в компании, а также советы и инструкции по созданию собственной программы по осведомленности [10].

Исследованиями и практикой в области *Security Awareness* активно занимается европейская научно-образовательная организация The SANS Institute, деятельность которой связана с исследованиями и образовательными программами в области ИБ, системного администрирования, аудита. В 2011 г. она разработала «Модель зрелости осведомленности по вопросам безопасности» (*Security Awareness Maturity Model*), которая позволяет организациям определить, на каком этапе находится их программа повышения осведомленности о безопасности в настоящее время и в каком направлении в дальнейшем организация должна продвигаться в данном направлении [11].

Сегодня активно развивается рынок сервисов повышения осведомленности по ИБ. Самыми крупными мировыми провайдерами платформ *Security Awareness* являются: PhishMe Knowbe4 Wombat Security MediaPro Inspired eLearning и др. [12].

Для повышения осведомленности широких масс в области ИБ проводятся специальные мероприятия. Так, в США ежегодно, начиная с 2004 г., проводится месячник под эгидой Департамента внутренней безопасности США совместно с Альянсом национальной кибербезопасности (National Cyber Security Alliance (NCSA)), куда входят такие компании, как Google, Cisco, Microsoft, Intel, SANS, Symantec, Facebook, Raytheon. Мероприятие называется National Cyber Security Awareness Month (NCSAM – Национальный месяц осведомленности о кибербезопасности). В его рамках рассматриваются такие темы, как: простые шаги к онлайн-безопасности; кибербезопасность на рабочем месте — дело каждого; сегодняшние прогнозы для завтрашнего Интернета; защита критической инфраструктуры от киберугроз и др. [13]. Целевой аудиторией месячника в США являются: дети (от 3-х до 7-ми лет); школьники; родители и учителя; молодые работники; пожилые американцы; сотрудники государственных органов, различных бизнес-структур, малого бизнеса, правоохранительных органов [14].

В Европе с 2012 г. ежегодно под эгидой ENISA тоже проходят подобные мероприятия под названием

European Cyber Security Month (ECSM). ECSM — это компания по повышению осведомленности по ИБ в ЕС, которая содействует кибербезопасности граждан и организаций и подчеркивает простые шаги, которые могут быть предприняты для защиты личных, финансовых или профессиональных данных. Основная цель этого мероприятия – повышение осведомленности, изменение поведения и предоставление ресурсов для всех о том, как защитить себя в Интернете. Действия по пропаганде осведомленности в области кибербезопасности регулируются правительством и распространяются на всех граждан, начиная от госорганов и корпораций и заканчивая простыми гражданами [15].

Наряду с понятием осведомленности (*Awareness*) в начале XXI в. в обиход вошло понятие культуры информационной безопасности (Information Security Culture – ISC). Ключевым стал 2002 г., когда Генеральная Ассамблея ООН в Резолюции «Создание глобальной культуры кибербезопасности» предложила государствам – членам развивать культуру кибербезопасности при применении и использовании информационных технологий [16]. Большая работа была проведена также Организацией по экономическому сотрудничеству и развитию (OECD), которая в 2002 г. опубликовала Рекомендации Совета по созданию глобальной культуры информационной безопасности «Безопасность информационных систем и сетей – на пути к культуре безопасности» [17].

В последние годы активно разрабатывается концепция цифровой среды как киберпространства, а также концепции культуры кибербезопасности (Cyber Security Culture –CSC) и цифровой безопасности (*digital security*) как частей культуры информационной безопасности. В 2015 г. OECD мотивирует создание культуры цифровой безопасности, в которой заинтересованные стороны должны учитывать риск своей собственной деятельности в цифровой среде [18]. Под эгидой ENISA, которое является центром экспертизы сетевой и информационной безопасности ЕС, в 2017 г. выходит документ «Cyber Security Culture in organisations», в котором представлены рекомендации по созданию и запуску программы повышения культуры кибербезопасности, а также описывается передовой опыт, выявленный в тех организациях, которые уже внедрили зрелые программы CSC, и которые специально распределены по категориям и адаптированы к разным аудиториям внутри организации, от высшего руководства до команды по информационной безопасности. Для облегчения разработки и реализации программы по культуре кибербезопасности в этом документе представлено восемь этапов реализации, а также дано подробное руководство по каждому из этих этапов. Кроме того, в нем обоснованы методы создания CSC для организации, показатели для измерения воздействия деятельности CSC, а также стратегии для создания надежного экономического обоснования для распределения внутренних ресурсов на будущие мероприятия по культуре кибербезопасности. В этом исследовании определены методологические инструменты и пошаговые инструкции для тех, кто хочет начать или усовершенствовать собственную программу культуры кибербезопасности в своих организациях, включая ресурсы для разработки бизнес-обоснования обеспечения финансирования такой программы [19].

Повышенный интерес к проблеме культуры информационной безопасности на организационном уровне привел к росту ее теоретических и эмпирических исследований. В настоящее время количество зарубежных публикаций по теме исчисляется сотнями. Ученые работают над определением термина «культура информационной безопасности» [20, 21 и др.], методами ее оценки [22 и др.] и др. Уже появились зарубежные исследования в виде обзоров. Так, европейские ученые выполнили исследование культуры информационной безопасности в период с 2000 по 2013 гг. [23]. Обзор определений и структур культуры информационной безопасности за период с 2003 по 2016 гг. был проведен малазийскими экспертами [24]. Члены еще одного научного коллектива [25] провели систематический обзор 405 публикаций, изданных с 2000 по 2017 гг., с использованием метода Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Все исследователи делают выводы об отсутствии единого подхода к определению культуры информационной безопасности, о несогласованности в определении обусловливающих ее факторов и т.д.

В научных публикациях нашли отражение и проблемы соотношения культуры информационной безопасности и кибербезопасности [26]. Культура кибербезопасности связана с тем, как люди воспринимают кибербезопасность и каково их поведение в киберпространстве, что влияет на защиту цифровой информации, систем и людей [27]. Сделана попытка определения культуры информационной безопасности, включающей в себя культуру кибербезопасности [28]. Иными словами, не только практика, но и наука о культуре ИБ находятся сегодня на пике своего развития.

В России гораздо позже стали уделять внимание вопросам человеческих (кадровых) рисков для информационной безопасности организации. Это связано с тем, что чрезвычайно «живучим» в нашей стране оказался стереотип об информационной безопасности как сугубо технической сфере деятельности, далекой от гуманитарных проблем. Опираясь на зарубежный опыт, в России обратили внимание на осведомленность в области информационной безопасности лишь в начале XXI в., когда началась гармонизация вышеупомянутых стандартов ИСО/МЭК по управлению информационной безопасностью. Затем требования по осведомленности в области информационной безопасности были приведены в Федеральном законе Российской Федерации № 152-ФЗ от 27 июля 2006 г. «О персональных данных». Статья 18.1 пункт 1 подпункт 6 «Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников»[1] относит обучение и ознакомление работников опера-

[1] Федеральный закон Российской Федерации № 152-ФЗ от 27 июля 2006 года «О персональных данных». – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 02.10.2019)

тора персональных данных с требованиями о защите персональных данных к возможной, но все же частной мере. На практике это ознакомление и обучение заканчиваются росписью в акте ознакомления с документами в организации.

Требования к повышению осведомленности работников в области информационной безопасности содержатся в приказе Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по защите информации в автоматизированных системах управления производственными и технологическими процессами (от 14 марта 2014 г. № 31)[2], в котором требования к мерам повышения осведомленности сформулированы в виде класса мер «XVIII. Информирование и обучение персонала (ИПО)». Этот блок включает требования к разработке правил и процедур (политик) информирования и обучения персонала, а также требования к обучению и информированию персонала по вопросам защиты информации. К сожалению, требования этого приказа выполняются только на основе решения владельца автоматизированной системы.

В приказе «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (от 25 декабря 2017 г. № 239) приводится блок требований «XVII. Информирование и обучение персонала (ИПО)», как и в Приказе №31. Отличием является лишь включение нового требования к контролю осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы[3].

Эти вопросы отражены и в отраслевых стандартах России. Так, в п. 8.9 СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» изложены требования к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности [29]. Весьма оптимистичны в настоящее время планы ЦБ РФ преобразовать рекомендательный статус этого стандарта в разряд обязательного для всех финансовых организаций РФ.

В Доктрине информационной безопасности Российской Федерации (2016) «низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности» названа одной из угроз ИБ, указана необходимость поддержки образовательных программ и организаций, работающих в данной области [30]. Таким образом, в содержании концептуальных и нормативных документов России требование наличия программы повышения осведомленности не является обязательным, способы и пути ее решения не конкретизируются.

Несмотря на недостаток нормативного регулирования, в России развивается практика в этой области. Например, как и на Западе, ежегодно с 2008 г. проводится «Неделя безопасного Рунета». Эта серия мероприятий, приуроченных к Международному Дню безопасного Интернета, проводится по инициативе Региональной общественной организации «Центр интернет-технологий» (РОЦИТ) и российского офиса Microsoft. Однако, в отличие от западных мероприятий, «Неделя безопасного Рунета» ориентирована только на детей и их родителей [15]. Начал развиваться российский рынок сервисов повышения осведомленности по ИБ среди вендоров – «Лаборатория Касперского», Phishman, «Антифишинг», UBS, «Системный софт», DeteAct, «Ростелеком» и др. [12].

Параллельно с проблемами осведомленности в России концептуализируется культурологический подход к решению проблемы человеческих рисков – с помощью повышения культуры информационной безопасности. Отрадно, что мероприятия федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утверждена президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. N 16) направлены на реализацию 4-х ключевых направлений: повышение уровня защищенности личности, информационной безопасности и устойчивости сетей связи общего пользования; создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных; профилактика и выявление правонарушений с использованием информационных технологий против общества и бизнеса; разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности. Наряду с прочими мероприятиями, в рамках этих направлений планируется осуществить «развитие подходов к повышению грамотности и практико-ориентированной подготовке в области кибербезопасности для представителей бизнеса и государства на базе опыта ведущих компаний цифровой экономики». До 31 декабря 2021 г. планируется «**разработать предложения** по популяризации добровольного страхования рисков информационной безопасности и **повышению киберкультуры»** (п.1.35)[4].

[2] Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868- (дата обращения 02.10.2019)

[3] Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. n 60)». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения – 02.10.2019

[4] Паспорт национальной программы "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. N 16). – URL: https://base.garant.ru/72190282/ (дата обращения: 24.09.2019).

К сожалению, в Паспорте этого проекта термин «киберкультура» заменен на **«систему повышения грамотности в области информационной безопасности»** (п.1.55)[5].

В рамках этой системы планируется разработать «не менее 10 учебных курсов по 4 направлениям, связанным с ИБ; ввести в эксплуатацию платформу управления обучением, включающую разработанные учебные курсы по ИБ; подготовить не менее 10 специальных практических комплексов для проведения семинаров и практикумов; провести не менее 100 образовательных мероприятий (лекций, семинаров, вебинаров и пр.) для слушателей, включая представителей МВД России, Следственного комитета, Генпрокуратуры и бизнес-структур; для организации обучения привлечь не менее 3 ведущих отечественных компаний в сфере информационной безопасности».

С сожалением можно констатировать, что массовый характер мероприятий по повышению осведомленности в области ИБ в этом документе не планируется. Да и неожиданный отказ от понятия «киберкультура» – это шаг назад. Невольно вспоминается, как недопустимо долго в нашей стране происходило переформатирование установки с информационной грамотности на информационную культуру, их отождествление. От первого упоминания термина «информационная культура» [31] до сегодняшнего дня прошло почти полвека, однако многочисленные исследования показывают, что и до сих пор уровень этой культуры низок. Российские ученые справедливо называют концепцию информационной грамотности рациональной, ибо она выросла из американских стандартов информационной грамотности и традиций американской системы образования с присущими ей утилитаризмом и практицизмом. Однако, в связи с тем, что невозможно формировать информационную грамотность без мотивирования человека, не обращаясь к его духовной сфере, в России появилась концепция информационной культуры личности как «грань общей культуры человека, которая включает в себя в качестве неотъемлемого компонента информационную грамотность» [32]. Информационную культуру личности невозможно рассматривать вне информационного мировоззрения и ценностных аспектов, вне норм информационного поведения человека в сети и др. [33]. Поэтому «информационная культура личности» – более широкое понятие, чем «информационная грамотность». Оно, в отличие от информационной грамотности, включает в свой состав информационное мировоззрение и характеризуется интегрированностью в сферу культуры. Это позволяет обеспечить синтез и целостность традиционной книжной (библиотечной) и новой (компьютерной) информационной культуры, дает возможность избежать в информационном обществе конфронтации двух полярных культур – технократической и гуманитарной [34].

Ценностная составляющая поведения человека в цифровом пространстве – это ключевой компонент, который, тесно связывает информационную культуру и культуру ИБ. Именно наличие ценностей отличает культуру от грамотности (осведомленности) и в области информации, и в области ИБ. Осведомленный – сведущий, знающий, знакомый с чем-либо, компетентный, грамотный, информированный, наслышанный о чем-либо и др. [35, с. 258]. Как видим, синонимом слова «осведомленность» является грамотность. А «грамотность», как известно, означает наличие элементарных навыков – умения читать и писать, знаний в какой-либо области [36, с. 337], поэтому грамотный – это осведомленный, умелый [35, с. 81]. Осведомленность, знание чего-либо, знакомство с чем-либо, компетентность, грамотность, информированность – однопорядковые понятия. Логично заключить, что осведомленность в области ИБ – это элементарный уровень грамотности, выражающийся в минимуме знаний об ИБ. Она не предполагает сложных знаний и умений, связанных с обеспечением безопасности информации, информационных систем и имеет семантическую окраску примитивности, самого простого, начального уровня знаний в этой области. Недостатком концепции осведомленности является и то, что в нее не входит необходимость формирования информационного мировоззрения, мотивации деятельности человека к обучению и использованию полученных знаний на практике. В ее рамках человеческий фактор не рассматривается в контексте новой культуры – культуры цифрового общества, основанного на знаниях, и вне ее социальных функций - образовательно-воспитательной, когнитивной, мировоззренческой, ценностной и др. Вот почему нам нужна культура информационной безопасности, а не грамотность или осведомленность в этой области. Учитывая высокий уровень опасности и критичность человеческих угроз информационной безопасности, концентрация на грамотности в этой области чревата отставанием России в развитии цифровой экономики.

В настоящей статье мы не ставим перед собой цели обоснования теории культуры информационной безопасности. Авторские исследования ее сущности, структуры, факторов влияния, методов измерения и др. представлены нами в статьях [21, 37-40 и др.]. По нашему мнению, *культура информационной безопасности организации – это способ целенаправленной созидательной совместной деятельности руководителей и сотрудников по обеспечению и повышению уровня ИБ организации, который выражен в ценностях, потребностях, знаниях и поведении этих руководителей и сотрудников: а) в формировании ценностных моделей их информационного взаимодействия как отправителей и получателей информации; б) в гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии); в) в непрерывном повышении их знаний, в том числе – осведомленности об ИБ; г) в способности работодателя и сотрудников реализовывать и развивать культурные ресурсы их информационного поведения в процессе совместной профессиональной деятельности.*

[5] Паспорт федерального проекта "Информационная безопасность" (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. N 9)). – URL: http://www.consultant.ru/document/ cons_doc_LAW_328932/ (дата обращения 02.10.2019)

В процессе формирования и развития культуры ИБ для предприятия важно учитывать все множество факторов и, по возможности, определять степень ее зависимости от каждого из них. Факторы, влияющие на культуру ИБ, можно классифицировать по разным признакам: по уровню влияния (микро- и макроуровень); по среде возникновения (внешние и внутренние); по направлению влияния (защищаемая информация, пользователь информационной системы); по степени важности (важные и менее важные); по степени распространения (факторы общего и локального действия) и др. Среди этих факторов особая роль в формировании и развитии культуры ИБ принадлежит группе факторов внешней и внутренней среды.

Факторы внешней среды (внешние факторы) объективны, от организации не зависят и влияют на культуру ИБ либо способствуя, либо тормозя ее развитие. К ним относятся национально-культурные, политические и правовые, экономические, социально-культурные и технико-технологические факторы.

Иное дело – факторы внутренней среды (внутриорганизационные факторы). Они формируют культуру ИБ внутри организации, поэтому требуют к себе активного деятельностного подхода со стороны организации и им присуща субъективность воздействия. Внутренние факторы – это общеорганизационные, управленческие, человеческие (связанные с персоналом) и факторы доверия между всеми участниками процесса.

К общеорганизационным факторам относятся: внутреннее состояние, стадия жизненного цикла организации, уровень общей организационной культуры, наличие действующей системы защиты конфиденциальной информации в организации. Управленческие факторы – это лидерство руководителя, политика ИБ и управление ИБ (управление рисками, инцидентами угрозы ИБ, изменениями, персоналом, осведомленностью, обучением и др.).

Большое влияние на уровень культуры информационной безопасности организации оказывают факторы, связанные с сотрудниками: их личностные качества и ценности; потребности и установки; эмоциональное состояние; знания об информационной безопасности; соблюдение правил ИБ-поведения. Огромное значение имеет степень взаимного доверия, лояльности (приверженности) сотрудников к организации, их вовлеченности в реализацию ИБ-стратегии предприятия. Степень гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии) существенно повышает шансы на успех развития КИБ. Высокий уровень лояльности сотрудника к организации предполагает, что он идентифицирует себя с ней, представляет себя и организацию как единое целое, отождествляет себя с ее культурой и способен реализовать все свои личностные характеристики в информационном поведении в процессе профессиональной деятельности. Полагаем, что культура информационной безопасности должна рассматриваться именно в данной, многофакторной интерпретации, иначе проблематично решать задачи по развитию цифровой экономики, в том числе поставленные в федеральном проекте «Информационная безопасность».

Одна из серьезных проблем повышения осведомленности, а значит, и культуры информационной безопасности – недостаток кадров, способных эту проблему решать [41]. Это актуально и на уровне организаций, и на массовом уровне.

В организациях эта функция закреплена за директором и специалистом по защите информации. Сегодня это уже не «технарь», как было раньше, а специалист широкого профиля – со знанием правовых аспектов, бизнеса, финансов, технологий, организационного управления, управления рисками, инцидентами, персоналом и в том числе – культурой ИБ. Поэтому он должен обладать педагогической компетенцией [42]. Как замечают эксперты, за рубежом термин *chief information security officer* (*CISO*) стал постепенно исчезать. Специалисты по ИБ все более становятся специалистами широкого профиля по защите бизнеса, даже буква "*I*" в аббревиатуре *CISO* постепенно исчезает. С сожалением следует констатировать, что пока таких специалистов российские вузы не готовят. Однако совершенно очевидно, что технологии развития культуры информационной безопасности в организациях должны быть обязательным предметом изучения в вузах, а также в системе переподготовки и повышения квалификации кадров.

А как же быть с массовой культурой информационной безопасности, кто будет формировать ее? Мы согласны с мнением экспертов о том, что это острая необходимость [43]. Если дети хоть как-то включены в орбиту внимания государства, то как же быть со всеми остальными гражданами? Может, решению этой проблемы будет способствовать «цифровой куратор»? Профессиональный стандарт, определяющий особенности этой новой специальности, появился в России в 2018 г.[6]

Если мы обратимся к содержанию этого стандарта, то найдем утвердительный ответ на этот вопрос. В рамках трудовой функции «Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий» в числе трудовых действий – «информирование о наиболее типичных угрозах при работе в сети, с использованием средств коммуникации», «информирование об основных методах противодействия информационным угрозам». В числе необходимых умений – «отбирать и применять инструменты обеспечения информационной безопасности», необходимых знаний – «требования информационной безопасности». Трудовая функция «Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий» предполагает умения «обрабатывать пер-

[6] Приказ Минтруда России от 31.10.2018 N 682н «Об утверждении профессионального стандарта "Консультант в области развития цифровой грамотности населения (цифровой куратор)"» (Зарегистрировано в Минюсте России 19.11.2018 N 52725). – URL: http://www.consultant.ru/document/Cons_doc_LAW_311506/ (дата обращения 02.10.2019)

сональные данные с соблюдением требований, установленных законодательством Российской Федерации», «оказывать консультативную помощь, связанную с оперированием персональными данными самими пользователями (и их защитой) при работе с интернет- сервисами».

Однако в остальном мы будем разочарованы: полное название специальности – "Консультант в области развития цифровой грамотности населения (цифровой куратор)" и, следовательно, будущий специалист ограничен элементарными уровнем грамотности, хоть и цифровой. Ценностные, мировоззренческие и другие гуманитарные аспекты ИБ в стандарте не упоминаются. Впрочем, это понятно: необходимо сначала ликвидировать «безграмотность» в этой области. Однако на подготовку кадров для решения даже этой, более простой задачи уйдет немало времени. А время, как известно, не ждет, и следует искать более оптимальные пути – там, где уже накоплен соответствующий опыт.

Может ли библиотека как главный субъект формирования и развития информационной культуры в нашей стране, справиться с этой задачей? Этим вопросом правомерно задались и библиотечно-информационные специалисты, ведь на данный момент, как это ни печально, библиотека не попала в проект ни как инициатор, ни как площадка для его реализации [44]. У библиотеки, безусловно, есть потенциал в реализации этих функций, есть инициативы, огромный опыт в использовании информационных ресурсов и технологий. Однако библиотечно-информационным специалистам срочно требуются новые компетенции в области ИБ. Эта проблема должна решаться в рамках вопроса о расширении миссии и функций современной библиотеки. Зарубежные эксперты все более склоняются к требованию активной интеллектуально-деятельностной позиции библиотечно-информационного специалиста. По словам экс-президента Американской библиотечной ассоциации С. Фельдмана [45, с. 5], будущая актуальность библиотек и библиотечных специалистов будет зависеть от того, *что они делают* для людей, а не от того, *что они имеют* для людей. Так, роль библиотеки как информационного центра неминуемо снижается из-за расширения возможностей удаленного доступа пользователей к информационным ресурсам, поэтому библиотека все более исследуется с позиций новой функции –учебного центра, в реализации которой она уже накопила большой и ценный опыт [46].

Для реализации своей образовательной функции библиотека, как и любой субъект, вынуждена будет использовать новейшие технологии, в том числе – технологии искусственного интеллекта. С их помощью уже сегодня можно выявлять скрытые закономерности в поведении потребителей, определять вероятность отклика на то или иное рекламное предложение, понимать, кому, когда, как и что лучше предложить, чтобы выстроить максимально персонифицированные коммуникации. Искусственный интеллект дает дополнительные навыки и помогает распознавать тексты, определять тип документа, извлекать значимые данные, чтобы затем передавать их в целевые информационные системы. По мнениям экспертов, искусственный интеллект в ближайшее время охватит все ИТ-сервисы. Наиболее перспективны персонификация предложений клиентам; создание релевантных рекомендательных сервисов нового поколения; автоматическая обработка пользовательского контента и действий: например, анализ отзывов, обращений, выявление ботов и т.д. [47]. Так, компания *Uber Technologies Inc*. использовала машинное обучение для прогнозирования спроса и предложения (алгоритм направляет водителя в ближайшие зоны с повышенным числом клиентов еще до того момента, как они появляются). Крупный финансовый холдинг *JPMorgan Chase* представил платформу *Contract Intelligence* (*COIN*), на которую были возложены задачи по обработке и анализу юридических документов, по извлечению из них ключевой информации, а также по сегментации клиентов на категории, в соответствии с которыми планировалось разрабатывать таргетированные предложения и оказывать услуги и др. [48]. И поскольку «успешность применения технологий искусственного интеллекта зависит главным образом от наличия достаточного объема данных» [47], логично предположить, что информационные центры и библиотеки, такими данными располагающие, могут использовать свой потенциал и опыт участников рынка программных решений по повышению осведомленности в области ИБ.

Но им следует пойти дальше осведомленности и грамотности – по направлению к культуре информационной безопасности, а потому – создавать свои инструментальные средства. Эти средства должны оценивать текущие угрозы ИБ со стороны пользователей; выявлять закономерности в их поведении; понимать, кому, когда, как и что предложить для обучения; создавать релевантные рекомендательные сервисы контента по информационной безопасности нового поколения; прогнозировать информационное поведение пользователей и их ИБ-уязвимости в будущем и др. Некоторые игроки рынка осведомленности уже начинают идти по этому пути. Так, программы повышения осведомленности «Лаборатории Касперского» не только дают знания, но и формируют правильное поведение; для разных категорий сотрудников они создают разные навыки; курс позволяет обучать пользователей в соответствии с ландшафтом угроз и их исходными навыками и т.д. [12].

Развитие культуры информационной безопасности должно стать предметом непрерывного образования в школах, вузах, по месту работы и досуга граждан, а значит – во всех видах и типах библиотек. Цифровые сервисы по повышению культуры ИБ должны размещаться на официальных и поисковых сайтах, в электронных библиотечных системах, в социальных сетях. Безусловно, это новые вызовы для российского информационного и библиотечного образования, и требуются не только государственные решения по этому вопросу, но и готовность специалистов-практиков к профессиональной переподготовке и непрерывному повышению квалификации.

Большим потенциалом для создания и внедрения цифровых сервисов повышения культуры ИБ обладает Всероссийский институт научной и технической

информации Российской академии наук (ВИНИТИ РАН). Согласно его Уставу, утвержденному приказом Министерства науки и высшего образования Российской Федерации № 5 от 06.07.2018, предметами деятельности Института являются, кроме научно-информационного и аналитического обеспечения научных исследований, «разработка научно-методологических основ информатизации общества и осуществление инновационной деятельности, направленной на обеспечение социально-экономического развития и национальной безопасности Российской Федерации; развитие информационных технологий; разработка концептуальных основ и методологических подходов к оценке эффективности процессов информатизации общества»[7]. Обращение к культурологическому методологическому подходу к осведомленности в области ИБ, разработка и внедрение высокотехнологичных инновационных инструментов по повышению культуры ИБ – все это, безусловно, позволит ускорить темпы и улучшить качество цифровизации общества, составляющей основу информационной и национальной безопасности страны.

Что касается кадровой готовности к решению столь нестандартных проблем, то руководство ВИНИТИ РАН так или иначе ставит перед собой задачу «усовершенствовать систему подготовки кадров информационных работников путем проведения соответствующих конференций и особенно семинаров для работников информационной сферы, активизации работы аспирантуры и докторантуры, привлечения студентов и аспирантов к информационной работе в сотрудничестве с вузами» [49, с. 4].

* * *

Предпринятый анализ зарубежной науки и практики показал, что до начала XXI в. доминировал подход к решению проблемы человеческих рисков информационной безопасности через повышение осведомленности о ней. Концепция осведомленности (грамотности) и разработанные на ее основе стандарты информационной безопасности отличаются сугубо прагматической направленностью, отсутствием мотивационно-рефлексивных, мировоззренческих аспектов, что неадекватно в условиях культурной цифровой трансформации. В последние годы в зарубежных странах осознается ограниченность столь прагматичного подхода, поэтому резко увеличился поток публикаций по культуре информационной безопасности, развивается её социальная практика в самых разных отраслях деятельности. Ограниченность науки и практики рамками осведомленности и грамотности в области информационной безопасности свидетельствует об отставании России от мировой тенденции. Нам необходимы широкомасштабные научные междисциплинарные исследования теории культуры информационной безопасности, перестройка системы подготовки кадров для выполнения её функций (специалистов по защите информации, информационных работников, библиотечно-информационных специалистов и др.), повсеместная практика ее развития под эгидой Совета безопасности Российской Федерации с участием образовательных и информационных организаций страны. Акцент на образовательную функцию информационных центров и библиотек согласуется с трансформацией их социальной миссии в цифровой культуре. Главным средством реализации этой функции должны стать многофункциональные цифровые сервисы по развитию культуры информационной безопасности, разработанные на основе машинного обучения.

[7] Устав Всероссийского института научной и технической информации Российской академии наук. Утв. приказом Министерства науки и высшего образования Российской Федерации № 5 от 06.07.2018. – URL: http://www.viniti.ru/viniti-about (дата обращения 02.10.2019).

СПИСОК ЛИТЕРАТУРЫ

1. PriceWaterhouseCoopers. The Global State of Information Security® Survey 2018. – URL: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (дата обращения 02.10.2019).
2. PriceWaterhouseCoopers. На пути к цифровому доверию. – URL: https://www.pwc.ru/ru/assets/pdf/digital_trust_insights_russian.pdf (дата обращения 02.10.2019).
3. NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf (дата обращения 02.10.2019).
4. ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary. – URL: https://www.iso.org/standard/56891.html (дата обращения 02.10.2019).
5. ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements. – URL: https://www.iso.org/standard/54534.html (дата обращения 02.10.2019).
6. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management. – URL: https://www.iso.org/standard/54533.html (дата обращения 02.10.2019).
7. ISO/IEC 27003:2010 Information technology – Security techniques – Information security management systems implementation guidance. – URL: https://www.iso.org/standard/ 42105.html (дата обращения 02.10.2019).
8. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance. – URL: https://www.iso.org/obp/ ui/#iso:std:iso-iec:27003:ed-2:v1:en (дата обращения 02.10.2019).
9. Information Security Awareness in Financial Organisations / ENISA. – URL: https://webcache.googleusercontent.com/search?q=cache:0Us-oaHURyQJ:https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport+&cd=1&hl= ru&ct=clnk&gl=ru (дата обращения 02.10.2019).
10. The new users guide: How to raise information security awareness [Электронный ресурс] / ENISA –

URL:https://www.enisa.europa.eu/publications/ archive/copy_of_new-users-guide (дата обращения 02.10.2019).
11. Spitzner L. Defining the Security Awareness Maturity Model. – URL: https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (дата обращения 02.10.2019).
12. Горюнов С.Е. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness). – URL:https://www.anti-malware.ru/analytics/Market_ Analysis/Security-Awareness#part3 (дата обращения 02.10.2019)
13. Bonderud D. National Cyber Security Awareness Month: What's New for 2018? – URL: https://securityintelligence.com/national-cyber-security-awareness-month-whats-new-for-2018/ (дата обращения 02.10.2019)
14. National Cybersecurity Awareness Month. – URL: https://www.dhs.gov/national-cyber-security-awareness-month (дата обращения 02.10.2019)
15. Пластунов В.А. Почему у задачи по повышению осведомленности в кибербезопасности нет альтернативы. – URL: https://www.itweek.ru/ security/ article/ detail.php?ID=195601 (дата обращения 02.10.2019)
16. Создание глобальной культуры кибербезопасности: Резолюция, принятая Генеральной Ассамблеей Организации Объединенных Наций [по докладу Второго комитета (A/57/529/Add.3)] 57/239. 31 January 2003. – URL: https://undocs.org/ ru/A/RES/57/239 (дата обращения 02.10.2019)
17. OECD. (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: Organisation for Economic Co-operation Development). – URL: https://www.oecd.org/sti/ ieconomy/15582260.pdf (дата обращения – 02.10.2019)
18. OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. – URL: https://www.oecd.org/sti/ieconomy/ digital-security-risk-management.pdf (дата обращения 02.10.2019)
19. ENISA. (2017). Cyber Security Culture in organisations / ENISA. – URL: https://doi.org/10.2824/10543 (дата обращения 02.10.2019)
20. AlHogail A., Mirza A. Information security culture: A definition and a literature review // 2014 World Congress on Computer Applications and Information Systems (WCCAIS). 17-19 Jan. 2014. – URL: https://ieeexplore.ieee.org/document/6916579 (дата обращения 01.10.2019)
21. Астахова Л.В. Понятие культуры информационной безопасности // Научно- техническая информация. Сер. 1. – 2014. – № 2. – С. 1-8; Astakhova L. The concept of the information-security culture // Scientific and Technical Information Processing. – 2014. – № 41, № 1. – P. 22-28.
22. Veiga A. d., Martins N. Information security culture and information protection culture: A validated assessment instrument // Computer Law & Security Review. – 2015. – № 312). – P. 243-256.
23. Karlsson F., Åström J., Karlsson M. Information security culture–state-of-the-art review between 2000 and 2013 // Information & Computer Security. – 2015. – № 23(3). – P. 246-285.
24. Mahfuth A., Yussof S., Baker A. A., Ali N. a. A systematic literature review: Information security culture // 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). – URL: https://ieeexplore.ieee.org/document/8002442 (дата обращения 02.10.2019)
25. Nasir A., Arshah R. A., Ab Hamid M. R., Fahmy S. An analysis on the dimensions of information security culture concept: A review // Journal of Information Security and Applications. – 2019. – № 44. – P. 12-22.
26. Solms B. von, Solms R. von. Cybersecurity and information security–what goes where? // Information & Computer Security. – 2018. – № 26(1). – P. 2-9.
27. Veiga A. d. Comparing the information security culture of employees who had read the information security policy and those who had not // Information and Computer Security. – 2016. – № 24(2). – P.139-151.
28. Veiga A. d., Martins N. Defining and identifying dominant information security cultures and subcultures // Computers & Security. – 2017. – № 70. – P. 72-94.
29. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». – URL: https://cbr.ru/ Content/Document/File/ 46921/st-10-14.pdf (дата обращения 02.10.2019)
30. Доктрина информационной безопасности Российской Федерации / Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения 02.10.2019)
31. Воробьев Г.Г. Информационная культура управленческого труда. – М.: Экономика, 1971. – 108 с.
32. Гендина Н.И. Можно ли измерить информационную грамотность (культуру)? // Образование в документах. – 2009. – № 20(213). – С. 58-62.
33. Астахова Л.В. Информационное мировоззрение: понятие и уровни // Вестник Челябинской государственной академии культуры и искусств. – 2014. – № 4 (40). – С. 9-16.
34. Гендина Н.И. Информационная грамотность и информационная культура личности: международный и российский подходы к решению проблемы // Открытое образование. – 2007. – № 5. – С. 58-69.
35. Словарь синонимов русского языка. – М.: Русский язык, 1993. – 495с.
36. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1990. – 1632 с.
37. Astakhova L.V. Information security culture and information destructiveness counterculture: essence and structure // Socio-cultural aspects of regional development. – Chelyabinsk, 2010. – P. 201-205.
38. Astakhova L.V. Information-psychological security in the region: culturological aspect // Bulletin of the Ural Federal District. Information security. – 2011. – №2. – P. 40-47.

39. Астахова Л.В. Информационная безопасность: риски, связанные с культурным капиталом персонала // Научно-техническая информация. Сер. 1. – 2015. – № 4. – С. 1-13; Astakhova L. V. Information security: risks related to the cultural capital of personnel (review) // Scientific and Technical Information Processing. – 2015. – № 42, № 2. – P. 41-52.
40. Astakhova L.V. From culture to cultural capital information security of the organization // Bulletin of Culture and Arts. – 2018. – №3(55). – P. 85-101.
41. 2018 SANS Security Awareness Report. Building Successful Security Awareness Programs. – URL: https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf (дата обращения – 02.10.2019)
42. Астахова Л.В. Педагогическая компетенция будущего специалиста по защите информации в вузе: проблема развития и понятие // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2014. – Т. 6, № 1. – С. 69-76.
43. Белов Е.Б., Лось В.П., Малюк А.А. Цифровая экономика и актуальные проблемы совершенствования системы подготовки кадров в области информационной безопасности // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 6-22.
44. Цифровой куратор. А при чём здесь библиотека? // Университетская книга. – 2019. – № 4. – С. 31-37.
45. Feldman S. The future of the MLIS: imparting enduring values with changing instruction models // American Libraries. – 2015. –- 46(11/12).
46. Kumar B. Academic Library in Transition from Library as a Place to Library as a Learning Centre: A Case Study of Indian Institutes of Management // Desidoc journal of library & information technology. – 2015. – Vol. 35, № 3. – P. 169-176.
47. Искусственный интеллект 2018. Российский рынок искусственного интеллекта: проблемы и перспективы: Обзор. – URL: http://www.tadviser.ru/index.php/_2018 (дата обращения 02.10.2019)
48. Андреянов Н. Подходит ли опыт западных стран в области машинного обучения для российского рынка? – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/foreign-machine-learning-experience (дата обращения 02.10.2019).
49. Щуко Ю.Н. Некоторые аспекты развития Всероссийского института научной и технической информации // Научно-техническая информация. Сер. 1. – 2018. – № 9. – С. 1-6.

Материал поступил в редакцию 03.10.19.

Сведения об авторе

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета (национального исследовательского университета), г. Челябинск
e-mail: astakhovalv@susu.ru