Культура и искусство
Правильная ссылка на статью:
Былевский П.Г. — Культурологические аспекты профессиональной культуры информационной безопасности // Культура и искусство. – 2023. – № 8. DOI: 10.7256/2454-0625.2023.8.43846 EDN: VPJECJ URL: https://nbpublish.com/library_read_article.php?id=43846

Культурологические аспекты профессиональной культуры информационной безопасности

Былевский Павел Геннадиевич

ORCID: 0000-0002-0453-526X

кандидат философских наук

доцент, кафедра информационной культуры цифровой трансформации; кафедра международной информационной безопасности, Московский государственный лингвистический университет

119034, Россия, Москва, г. 119034 Москва, ул. Остоженка, 36, оф. 106

pr-911@yandex.ru

Статья из рубрики "Теоретическая культурология и теория культуры"

DOI:

10.7256/2454-0625.2023.8.43846

EDN:

VPJECJ

Дата направления статьи в редакцию:

20-08-2023

Аннотация: Цель исследования – изучение потенциала культурологического подхода к профессиональной культуре информационной безопасности в современных условиях. Предметом исследования являются социально-культурные аспекты профессиональных компетенций в контексте формирования и развития общегражданской культуры информационной безопасности. Объектом исследования выступает предшествующая и продолжающаяся эволюция профессиональной культуры информационной безопасности в России. В качестве материалов использованы научные, исследовательские и научно-практические публикации по теме исследования в российских журналах перечня ВАК и в международной базе Scopus (категорий Q1 и Q2) за 2021-2023 гг. Применены эволюционный и структурно-функциональный методы, предмет исследования рассматривается с точки зрения культурологической парадигмы – динамической системной модели. Новизна исследования заключается в применении понятийного аппарата и методов культурологии для исследования профессиональной культуры информационной безопасности. Ранее формирование и развитие культуры информационной безопасности рассматривалось в рамках технических научных

дисциплин, а затем юриспруденции, менеджмента, педагогики, психологии и лингвистики. Результат исследования – выявление социально-культурных факторов как компонентов, неотъемлемо присущих профессиональной культуре информационной безопасности на современном этапе. К ним относятся традиционные ценности, идентичность, противодействие манипуляциям сознанием, а также психолого-педагогические компетенции обучения не профессионалов в информационной безопасности сотрудников организаций и граждан, клиентов и пользователей сервисов. Сделан вывод: культурологический подход высоко востребован в информационной безопасности, что обусловлено превращением её в общегражданскую культуру, необходимо включающую всё более значимые социально-культурные аспекты.

Ключевые слова:

информационная безопасность, профессиональная культура кибербезопасности, общегражданская культура кибербезопасности, социально-культурные угрозы, традиционные ценности, культурная идентичность, социальная инженерия, дезинформация, цифровой суверенитет, технологическая импортонезависимость

Введение

Формирование и развитие национальной системы развития культуры информационной безопасности — необходимость, вызванная повсеместным разнообразным применением компьютерно-телекоммуникационных технологий и проявлением новых социально-культурных угроз высокого уровня. Содержание информационной безопасности, включая угрозы и средства противодействия, прежде носившее преимущественно технический характер, всё более наполняется социально-культурными и общегражданскими аспектами, требуя профильного научного осмысления. Изначально, в 1990-е годы, информационная безопасность формировалась как техническая дисциплина, постепенно включая организационно-правовые, педагогические [1], психологические [2] и социально-культурные направления [3], но культурологи рассматривали лишь отдельные её аспекты.

Настоящее исследование должно восполнить указанный пробел: использование культурологической парадигмы, динамической системной модели информационной безопасности является профильным для развития и повышения соответствующей культуры граждан России. Применение эволюционного и структурно-функционального подходов позволяет определить специфику, место и роль профессиональных компетенций информационной безопасности в общегражданской культуре информационной безопасности. Такое методологическое сопровождение позволяет профессионально разрабатывать и применять методики усиления противодействия угрозам информационной безопасности, адаптированные для разных категорий граждан в соответствии с их социально-культурными особенностями, интересами, привычками и поведением.

1. Эволюционное развитие профессиональной культуры информационной безопасности

Применение компьютерно-телекоммуникационных технологий, интернет-коммуникаций распространилось на все отрасли профессиональной деятельности и практически на всех граждан России. Культура информационной безопасности, формировавшаяся в 1990-е

годы как узкопрофессиональная, в дальнейшем разрастается вначале до профессиональных специализаций в различных отраслях, а затем и до массового, общегражданского масштаба. Значимым подтверждением эволюционной зрелости этой тенденции является принятие «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» (Распоряжение Правительства России от 22 декабря 2022 г. № 4088-р).

Профессиональная культура информационной безопасности остаётся исходным элементом, базисом и основным детерминантом для других отраслей, профессий и общегражданской сферы [4]. Вместе с тем профессиональная культура не остаётся неизменной, функционально и структурно эволюционируя как элемент расширяющейся системы всё большего многообразия профессий и общегражданских применений, требующих обеспечения информационной безопасности. В этой области проявляется соотношение между профессиональной и массовой культурой, существующее в других профессиях, видах социально-культурной деятельности. Просматривается аналогия с взаимодействием профессионального искусства и художественной самодеятельности: трансляция высокой артистической культуры любителям дополняется обратным аккумулированием, синтезом профессионалами лучших достижений народного творчества.

Эволюционно культура специалистов информационной безопасности перестаёт в 2000-е годы быть узкопрофессиональной, функционально распространяясь практически на все отрасли, где начинают применяться компьютерно-телекоммуникационные технологии, интернет-коммуникации; соответственно возникает необходимость в обеспечении их безопасности применительно к содержательным особенностям профессии. Отличительной чертой этого периода является распространение корпоративных компьютерных сетевых систем, электронного делопроизводства и документооборота. Обеспечение информационной безопасности на этом этапе чаще всего не выделено в отдельное организационное подразделение, а относится к обязанностям системных администраторов. Профессиональная культура информационной безопасности, прежде узкопрофессиональная и закрытая, приобретает публичный характер, расширяется до специализированной деятельности применительно к особенностям разных отраслей.

Технические аспекты структурно пополняются нормативно-правовыми и организационными, а также психолого-педагогическими вопросами: специалистам по информационной безопасности приходится формулировать её правила, обучать сотрудников выполнению, контролировать результаты. Чтобы не превратиться в уязвимость, критически повышающую риски ущерба, сотрудники организаций, не профессионалы в информационной безопасности, должны знать и уметь выполнять её правила применительно к своим служебным обязанностям. Кадровая подготовка таких специалистов по информационной безопасности для различных отраслей была обеспечена введением соответствующих профессиональных и образовательных стандартов, созданием системы специализированного обучения, открытием направлений подготовки десятками организаций высшего и среднего специального образования. Дисциплины, связанные с формированием профессиональной культуры информационной безопасности, учитывая отраслевые особенности, всё шире внедряются в подготовку специалистов самых разных профилей.

Следующий период эволюции профессиональной культуры информационной безопасности, с 2010-х годов по настоящее время, совершается в условиях универсального распространения, повсеместного и всё более разнообразного

применения компьютерно-телекоммуникационные технологий, автоматизации анализа больших данных и «искусственного интеллекта» I «цифровой трансформации». Основной социально-культурной особенностью этого периода следует признать появление, развитие и распространение до общегражданских масштабов массовых клиентских (пользовательских) сервисов, осуществляемых посредством компьютерно-телекоммуникационных технологий. Успех цифровой трансформации невозможен не только без массовых, общегражданских пользовательских умений и навыков, но и без доверия к новым сервисам, обусловленного культурой безопасности их применения. Актуализировался вопрос «всеобуча» граждан не только правильному, но и безопасному пользованию цифровым оборудованием и сервисами: пониманию сопутствующих актуальных угроз, умению их распознавать и правильно реагировать.

2. Корпоративно-отраслевая специализированная культура информационной безопасности сотрудников

По мере проявления в ходе цифровой трансформации необходимости в массовой культуре информационной безопасности потребовалось решить: кто, как и за счёт каких ресурсов должен обеспечить её эффективное формирование и развитие, выполнение функциональных предназначений. В 2000-х годах государством уделялось должное внимание профессиональной подготовке специалистов по информационной безопасности для государственного управления [5] и разных отраслей (энергетики [6], транспорта [7], финансов [8], медицины, социального обеспечения, культуры и т.п.). Учитывалась необходимость развития специализированной профессиональной культуры информационной безопасности у сотрудников организаций, не являющихся специалистами в данной области [9] в объёмах и с содержанием, определяемыми корпоративно-отраслевой спецификой и должностными обязанностями.

Культура безопасности интернет-сервисов выступала в роли «командной субкультуры» [10], обеспечивалась «по корпоративному принципу»: лишь внутри организации, не распространяясь на пользователей сервисов [11]. Профессионалы информационной безопасности организаций должны были заботиться о сохранности корпоративных ценностей [12], их не обязывали отвечать за повышение культуры безопасности клиентов, несущих ущерб от инцидентов по собственной вине. Обеспечение безопасности интернет-сервисов со стороны клиента оставалось собственным делом граждан; гражданская культура личной и общественной информационной безопасности формировалась в основном стихийно.

До конца 2000-х годов основным пользовательским оборудованием служили настольные персональные компьютеры с сетевым электропитанием и проводным доступом в интернет. Главной ценностью, привлекавшей компьютерную преступность, были безналичные электронные денежные средства клиентов в дистанционных банковских и платёжных сервисах. Атаки и хищения совершались в основном при помощи технических средств — специального вредоносного программного обеспечения («банковских вирусов») и оборудования (например, для «скимминга», скрытого незаконного копирования банковских карт). Профессиональная культура информационной безопасности, в том числе сотрудников сервисных служб, сводилась к умению применять технические средства защиты, а также смежным нормативно-правовым и организационным вопросам. Ограничение профессиональной культуры информационной безопасности корпоративными рамками и техническими аспектами, защищаемым «периметром» организации, включая сервисы, оставалось оправданным и достаточно эффективным,

пока сохранялся комплекс вышеперечисленных условий [13].

С 2010-х годов происходят значительные качественные организационно-технологические и масштабные социально-культурные изменения, потребовавшие существенного структурно-функционального и содержательного обновления профессиональной культуры информационной безопасности [14]. Краткой формулировкой сущности перемен может служить понятие универсализации, повсеместного всё более разнообразного, значимого и непрерывного использования каждым гражданином компьютерно-телекоммуникационных решений и интернет-сервисов. Настольные персональные компьютеры были дополнены массово доступными мобильными устройствами с автономным аккумуляторным электропитанием, зависимыми от постоянного беспроводного доступа в интернет. Планшеты, смартфоны, носимые гаджеты, «умная» бытовая техника и системы видеонаблюдения в общественных местах превратились в круглосуточную «цифровую среду» для каждого гражданина, обеспеченную покрытием населённых территорий России беспроводным широкополосным доступом в интернет.

Параллельным взаимозависимым процессом было создание «нового поколения» интернет-сервисов и коммуникаций, с интерактивными возможностями (оценок, комментариев и создания собственных публикаций): прессы, социальных сетей и блоггерских платформ, мессенджеров. Эти возможности сделали жизнь каждого гражданина разносторонне «цифровой», увеличив время пользования интернет-сервисами, а также перечень и значимость сопряженных ценностей. Технологии анализа «больших данных» позволили автоматизировать анализ разнообразных данных о гражданах, непрерывно собираемых в режиме реального времени. На основе автоматизированного анализа «больших пользовательских данных» интернет-сервисы позволяют манипулировать сознанием [15], поступками, поведением и привычками больших социальных групп, модифицировать личности жертв. Продолжительность пользования сервисом, степень внимания к контенту, показатели вовлечённости и активности пользователя превратились в товар для целевой «рекомендательной» рекламы и агрессивного маркетинга [16]. Не только деньги, многие другие ценности пользователя, персональные данные (яркий пример — медицинские сведения [17]) стали привлекательными целями для злоумышленников.

3. Профессиональные компетенции в формировании общегражданской культуры информационной безопасности

Реальность, формирующаяся в ходе цифровой трансформации, в том числе всплеск распространения дистанционных сервисов во время массового карантина 2020 года, обновила ландшафт угроз. Произошло переформатирование интернет-преступности, её целей и арсенала инструментов, содержательно влияя на функции и структуру профессиональной культуры информационной безопасности. Целями злоумышленников стали не только денежные, но и другие значимые ценности пользователей, включая социально-культурные. Атаки стали перенаправляться с технических средств защиты компьютерного оборудования и программного обеспечения на сознание пользователей. На прежнем этапе, в 2000-е годы, компьютерные преступления соотносились преимущественно с кражами со взломом, включая применение технических средств. Теперь же приоритетными стали интернет-мошенничества («телефонные» и др.) в отношении частных лиц и организаций [18], названные «социальной инженерией», а также шантаж, клевета, нанесение ущерба репутации, вовлечение в деструктивную, запрещённую деятельность.

Социально-культурные угрозы проявились даже в самой среде профессионалов информационной безопасности: были разработаны модели, включающие «внутреннего нарушителя» («инсайдера») (см. «Методику оценки угроз безопасности информации», утверждённую ФСТЭК России 5 февраля 2021 г.), автоматизированные системы для предотвращения утечек вовне (DLP — Data Leak Prevention) и выявления потенциального злоумышленника среди сотрудников организации. Профессионалам информационной безопасности отныне приходится нормировать и обучать сотрудников не только организационно-техническим, но социально-культурным аспектам противодействия угрозам, самим становиться специалистами в этих вопросах. Прежняя «корпоративно-отраслевая» модель безопасности массовых интернет-сервисов исчерпала себя: с 2018 года был зафиксирован резкий рост ущерба клиентам не от технических атак, а от «социальной инженерии» [19]. Функции корпоративной профессиональной культуры информационной безопасности финансовых организаций были расширены подготовкой и доведением до клиентов правил, развитием их знаний и умений безопасного пользования интернет-сервисами.

Причиной появления нового комплекса угроз информационной безопасности стал кризис однополярного глобализма, начало переформатирования международных отношений, триггерами которых послужили государственный переворот на Украине в 2014 году и начало там в феврале 2022 года специальной военной операции. Сложившийся ландшафт информационной безопасности включал новые технологические и социально-культурные угрозы, вызвавшие расширение функций и структурные изменения профильной профессиональной культуры (в особенности военного дела [20] и подготовки офицеров [21]). Перечень потенциальных нарушителей расширился с международной киберпреступности до государственных организаций и корпораций недружественных стран (в том числе глобальных цифровых платформ, базирующихся в США).

Для противодействия антироссийским санкциям недружественных государств, прекращению высокотехнологичного импорта, отключению от интернет-сервисов (S.W.I.F.T — банковских международных денежных расчётов и др.) и т.п. были созданы новые направления деятельности: обеспечение цифрового суверенитета России и независимости от импорта, защита российской критической инфраструктуры от трансграничных кибердиверсий. Новыми социально-культурными функциями профессиональной культуры информационной безопасности стали противодействие дискриминации российских граждан и официальной прессы со стороны глобальных цифровых платформ, массовым телефонным мошенничествам, автоматизированным фейк-новостям и дезинформации. Ранжирование важности этих социально-культурных функций повысилось до приоритетного уровня, что отразилось соответствующими структурными изменениями в организациях и профильных подразделениях информационной безопасности. Прежде формирование и развитие профессиональной культуры информационной безопасности совершалось преимущественно в рамках технических научных дисциплин; в настоящее время всё более заметную долю и значение приобретают юриспруденция, менеджмент, педагогика, психология, лингвистика [22], а теперь и культурология.

Формирование и развитие массовой, общегражданской культуры информационной безопасности превращается в общественную необходимость и новое актуально важное направление государственной политики. За счёт новых социально-культурных аспектов существенно модернизируется профессиональная культура специалистов, отныне обеспечивающих не только информационную безопасность государственных

организаций, но и развитие соответствующей общегражданской культуры. Эти обновления касаются обучения в организациях высшего и среднего специального образования [23], профессиональной переподготовки и повышения квалификации преподавателей, сотрудников официальной прессы, социальной рекламы.

Заключение

Результатом исследования является выявление высокого потенциала понятийного аппарата и методов культурологии как профильной науки для осмысления проблематики и разработки методик развития профессиональной культуры информационной безопасности в современных условиях. Эволюционный и структурно-функциональный анализ позволили установить важнейшие факторы эволюции профессиональной культуры информационной безопасности: универсальное применение компьютерно-телекоммуникационных технологий (цифровая трансформация) и углубление кризиса однополярного глобализма, актуализировавшего новые трансграничные технологические и социально-культурные угрозы со стороны недружественных стран и корпораций, включая глобальные цифровые платформы, базирующиеся в США.

Показано, что новые реалии и угрозы обусловливают необходимость содержательных и структурно-функциональных изменений профессиональной культуры информационной безопасности, включающих как организационно-технические (обеспечение цифрового суверенитета, независимости от технологического импорта), так и социально-культурные аспекты (противодействия трансграничным мошенничествам и дезинформации, направленной на разрушение традиционных ценностей, подмену идентичности и вовлечение в экстремистскую антигосударственную и антиобщественную деятельность).

Сделан вывод: новые социально-культурные (психолого-педагогические и др.) функции профессиональных компетенций приобретают приоритетное значение, становятся стержнем формирования и развития общегражданской культуры информационной безопасности, включая обучение сотрудников государственных, коммерческих и общественных организаций, клиентов и пользователей интернет-сервисов. Полученные результаты могут быть использованы для дальнейших исследований и разработок методических материалов в областях культурологии и развития культуры информационной безопасности в России.

Библиография

1. Астахова Л.В., Уторов О.Р. Будущий специалист по защите информации как субъект образовательной деятельности // Вестник УрФО. Безопасность в информационной сфере. 2022. № 1 (43). С. 84-89. DOI: 10.14529/secur220110
2. Голушко Т.К. Информационный иммунитет как ключевое понятие информационно-психологической безопасности личности // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2022. Т. 27. № 6. С. 1483-1495. DOI: 10.20310/1810-0201-2022-27-6-1483-1495
3. Alowais S., Armeen I., Sharma P., Johnston A. Cyber Hygiene Practices Across Cultures: A Cross Cultural Study of the US and Saudi Arabia based Information Systems Users // Procedia Computer Science. 2023. Vol.219. Pp.744-750. DOI: 10.1016/j.procs.2023.01.347
4. Богданов Д.А. Профессиональная культура специалиста в области защиты информации // Известия Воронежского государственного педагогического университета. 2021. № 4 (293). С. 27-31. DOI: 10.47438/2309-7078_2021_4_27
5. Воскресенская О.А., Сладкова Н.М., Горковенко Ю.Л. Оценка ценностно-

мотивационных установок сотрудника в области обеспечения информационной безопасности // Социально-трудовые исследования. 2022. № 1 (46). С. 142-153. DOI: 10.34022/2658-3712-2022-46-1-142-153

6. Georgiadou A., Michalitsi-Psarrou A., Askounis D. A security awareness and competency evaluation in the energy sector // Computers & Security. 2023. Vol.129. DOI: 10.1016/j.cose.2023.103199
7. Yerzhanov A., Nurzhanova G., Annenskaya N., Butova T., Balova S., Anzorova S., Aimakova G., Bissenbayev B. Building information security skills among young transport professionals // Transportation Research Procedia. 2022. Vol. 63. Pp. 1481-1488. DOI: 10.1016/j.trpro.2022.06.159
8. Паньшин Б.Н., Карачун И.А. Интеграция профессиональных и культурных знаний при подготовке специалистов банковской сферы // Креативная экономика. 2021. Т. 15. № 12. С. 4625-4642. DOI: 10.18334/ce.15.12.113893
9. Ющик Е.В. Развитие навыков информационной безопасности при формировании информационно-коммуникационных компетенций будущих специалистов рыбной отрасли // Педагогический журнал. 2022. Т. 12. № 5-1. С. 477-485. DOI: 10.34670/AR.2022.68.62.063
10. Sharma Sh., Aparicio E. Organizational and team culture as antecedents of protection motivation among IT employees // Computers & Security. 2022. Vol.120. DOI: 10.1016/j.cose.2022.102774
11. Ma X. IS professionals' information security behaviors in Chinese IT organizations for information security protection // Information Processing & Management. 2022. Vol.59, Iss.1. DOI: 10.1016/j.ipm.2021.102744
12. Ogbanufe O., Crossler R., Biros D. The valued coexistence of protection motivation and stewardship in information security behaviors // Computers & Security. 2023. Vol.124. DOI: 10.1016/j.cose.2022.102960
13. Patterson C., Nurse J., Franqueira V. Learning from cyber security incidents: A systematic review and future research agenda // Computers & Security. 2023. Vol.132. DOI: 10.1016/j.cose.2023.103309
14. Жестовский А.Г., Околот Д.Я., Рудинский И.Д. Культура информационной безопасности морского специалиста и условия ее формирования // Педагогика. Вопросы теории и практики. 2022. Т. 7. № 1. С. 100-107. DOI: 10.30853/ped20220010
15. Бердюгин А.А. Обеспечение безопасности естественного интеллекта в условиях развития киберпространства // Защита информации. Инсайд. 2022. № 5 (107). С. 75-81. EDN: DGFLML
16. Былевский П.Г. Пользовательские и персональные данные – анализ рисков извлечения знаний // Вопросы защиты информации. 2023. № 1 (140). С. 35-40. DOI: 10.52190/20732600_2023_1_35
17. Демаков В.И., Рерке В.И., Портная Я.А., Ракитский В.В. Об обеспечении информационной безопасности в сфере медицины и актуальности ее изучения в ведомственных вузах // Человеческий капитал. 2021. № 4 (148). С. 83-89. DOI: 10.25629/HC.2021.04.07
18. Борисов В.Р. Информационные технологии и цифровизация как среда деятельности кибермошенников // Инновационное развитие экономики. 2021. № 6 (66). С. 69-79. DOI: 10.51832/2223-79842021669
19. Grassegger T., Nedbal D. The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering // Procedia Computer Science. 2021. Vol.181.

Pp.59-66. DOI: 10.1016/j.procs.2021.01.103

20. Казимирович А.М. Практика реализации направлений развития профессиональной направленности на информационную безопасность у курсантов военных институтов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 3: Экономические, гуманитарные и общественные науки. 2022. № 1. С. 140-145. DOI: 10.46418/2079-8210_2022_1_25
21. Самедова Ю.А., Дорохов А.Н., Григоров С.Ю. Педагогические аспекты формирования критического мышления как средства информационной безопасности будущих офицеров в условиях военного вуза // Современные наукоемкие технологии. 2021. № 2. С. 209-213. DOI: 10.17513/snt.38520
22. Краснянская Т.М., Тылец В.Г., Иохвидов В.В. Репрезентация лингвистической и психолингвистической безопасности в языковом сознании // Язык и культура. 2022. № 57. С. 60-79. DOI: 10.17223/19996195/57/3
23. Нархов Д.Ю., Нархова Е.Н., Ярутина С.А., Шкурин Д.В. Социокультурный потенциал студенчества в аспекте информационной безопасности и профессиональной подготовки // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2021. № 2. С. 20-34. DOI: 10.17513/srps.244

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

В журнал «Культура и искусство» автор представил свою статью «Культурологические аспекты профессиональной культуры информационной безопасности», в которой проведено исследование социокультурного потенциала системы защиты виртуального пространства.
Автор исходит в изучении данного вопроса из того, что применение компьютерно-телекоммуникационных технологий, интернет-коммуникаций распространилось на все отрасли профессиональной деятельности и практически на всех граждан России. Культура информационной безопасности, формировавшаяся в 1990-е годы как узкопрофессиональная, эволюционировала вначале до профессиональных специализаций в различных отраслях, а затем и до массового, общегражданского масштаба.
Актуальность исследования обусловлена тем, что формирование и развитие национальной системы развития культуры информационной безопасности в современном мире является необходимостью, вызванной повсеместным разнообразным применением компьютерно-телекоммуникационных технологий и проявлением новых социально-культурных угроз высокого уровня. Содержание информационной безопасности, включая угрозы и средства противодействия, прежде носившее преимущественно технический характер, всё более наполняется социально-культурными и общегражданскими аспектами, требуя профильного научного осмысления. Практическая значимость исследования заключается в том, что полученные результаты могут быть использованы для дальнейших исследований и разработок методических материалов в областях культурологии и развития культуры информационной безопасности в России.
Проведя анализ научной обоснованности проблематики, автор приходит к заключению, что изначально, в 1990-е годы, информационная безопасность формировалась как техническая дисциплина, постепенно включая организационно-правовые,

педагогические, психологические и социально-культурные направления, однако не рассматривалась культурологией комплексно. Следовательно, научная новизна исследования заключается в применении эволюционного и структурно-функционального подходов, что позволяет определить специфику, место и роль профессиональных компетенций информационной безопасности в общегражданской культуре информационной безопасности, адаптировать ее для разных категорий граждан в соответствии с их социально-культурными особенностями, интересами, привычками и поведением.

Цель данного исследования заключается в анализе социокультурного аспекта информационной безопасности. Методологическую базу составил комплексный подход, включающий общенаучные методы анализа и синтеза, эволюционный и структурно-функциональный анализ.

Автором выявлен высокий потенциал понятийного аппарата и методов культурологии как профильной науки для осмысления проблематики и разработки методик развития профессиональной культуры информационной безопасности в современных условиях.

Эволюционный и структурно-функциональный анализ позволили автору установить важнейшие факторы эволюции профессиональной культуры информационной безопасности: универсальное применение компьютерно-телекоммуникационных технологий (цифровая трансформация) и углубление кризиса однополярного глобализма, актуализировавшего новые трансграничные технологические и социально-культурные угрозы со стороны недружественных стран и корпораций, включая глобальные цифровые платформы, базирующиеся в США.

Автором показано, что новые реалии и угрозы обусловливают необходимость содержательных и структурно-функциональных изменений профессиональной культуры информационной безопасности, включающих как организационно-технические, так и социально-культурные аспекты, а именно противодействия трансграничным мошенничествам и дезинформации, направленной на разрушение традиционных ценностей, подмену идентичности и вовлечение в экстремистскую антигосударственную и антиобщественную деятельность.

Автором исследованы новые социально-культурные (психолого-педагогические и др.) функции профессиональных компетенций, которые в современной социокультурной ситуации приобретают приоритетное значение, становятся стержнем формирования и развития общегражданской культуры информационной безопасности, включая обучение сотрудников государственных, коммерческих и общественных организаций, клиентов и пользователей интернет-сервисов.

В заключении автором представлен вывод по проведенному исследованию, в котором приведены все ключевые положения изложенного материала.

Представляется, что автор в своем материале затронул актуальные и интересные для современного социогуманитарного знания вопросы, избрав для анализа тему, рассмотрение которой в научно-исследовательском дискурсе повлечет определенные изменения в сложившихся подходах и направлениях анализа проблемы, затрагиваемой в представленной статье.

Полученные результаты позволяют утверждать, что изучение социокультурных аспектов различных направлений деятельности и путей повышения их эффективности представляет несомненный научный и практический культурологический интерес и заслуживает дальнейшей проработки.

Следует заметить, автор достиг поставленной цели. Представленный в работе материал имеет четкую, логически выстроенную структуру, способствующую более полноценному усвоению материала. Библиографический список исследования состоит из 23 источников, в том числе и иностранных, что представляется достаточным для обобщения

и анализа научного дискурса по исследуемой проблематике.

Следует констатировать: статья может представлять интерес для читателей и заслуживает того, чтобы претендовать на опубликование в авторитетном научном издании.