Мир науки. Социология, филология, культурология https://sfk-mn.ru
World of Science. Series: Sociology, Philology, Cultural Studies

2024, Том 15, № 1 / 2024, Vol. 15, Iss. 1 https://sfk-mn.ru/issue-1-2024.html

URL статьи: https://sfk-mn.ru/PDF/09KLSK124.pdf

DOI: 10.15862/09KLSK124 (https://doi.org/10.15862/09KLSK124)

5.10.1. Теория и история культуры, искусства (культурология)

Ссылка для цитирования этой статьи:
Былевский, П. Г. Нарратив информационной безопасности для культурологов, теоретиков и работников культуры / П. Г. Былевский // Мир науки. Социология, филология, культурология. — 2024. — Т. 15. — № 1. — URL: https://sfk-mn.ru/PDF/09KLSK124.pdf DOI: 10.15862/09KLSK124

For citation:
Bylevskiy P.G. Information security narrative for cultural scientists, theorists and cultural workers. *World of Science. Series: Sociology, Philology, Cultural Studies*. 2024; 15(1): 09KLSK124. Available at: https://sfk-mn.ru/PDF/09KLSK124.pdf. (In Russ., abstract in Eng.) DOI: 10.15862/09KLSK124

Исследование выполнено в рамках государственного задания ФГБОУ ВО МГЛУ по теме НИР «Культурная идентичность в современном мире: аналитические модели, способы конструирования и формы презентации» (номер государственного учёта АААА-А19-119072590048-4)

УДК 008 + 004.056

Былевский Павел Геннадиевич
ФГБОУ ВО «Московский государственный лингвистический университет», Москва, Россия
Доцент кафедры «Информационной культуры цифровой трансформации»
и кафедры «Международной информационной безопасности»
Кандидат философских наук
E-mail: pr-911@yandex.ru
ORCID: https://orcid.org/0000-0002-0453-526X
РИНЦ: https://elibrary.ru/author_profile.asp?id=283871

Нарратив информационной безопасности для культурологов, теоретиков и работников культуры

Аннотация. Цель исследования — определить роль, возможности и теоретические принципы участия культурологов, теоретиков и работников культуры в выработке и реализации мер противодействия угрозам, связанным с использованием компьютерных технологий и интернет-коммуникаций. Предметом исследования является культурологический нарратив научных публикаций об информационной безопасности за 2021–2023 годы. Объектом исследования являются современные угрозы традиционным ценностям и идентичности, вызванные универсальной цифровой трансформацией, началом специальной военной операции на Украине, обострением международных отношений с технологически лидирующими странами и глобальными интернет-сервисами, базирующимися в США.

Актуальность темы определяется, в частности, утверждением Правительства России 22 декабря 2022 г. «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации».

Методология исследования характеризуется применением культурологической парадигмы (подходу к культуре информационной безопасности как динамической системе человеческой деятельности), структурно-функционального и эволюционного методов. В качестве материалов использованы публикации в журналах ВАК К1, К2 и Scopus Q1, Q2.

Новизна статьи заключается в исследовании потенциала культурологического нарратива информационной безопасности в решении проблемы формирования общегражданской культуры информационной безопасности, профессиональной и массовой.

Результатом исследования является вывод о возрастании в информационной безопасности доли и значения социально-культурных факторов в сравнении с техническими. Теория культуры, культурология определены как профильные дисциплины для повышения как профессиональной, так и общегражданской культуры информационной безопасности. Культурологическая парадигма информационной безопасности включает систему взаимодействия профильной специализации профессиональной и общегражданской, массовой культуры информационной безопасности. Прогнозируется и доказывается эффективность создания специализированной подготовки культурологов, теоретиков и работников культуры в области профессиональной и массовой информационной культуры безопасности.

Ключевые слова: культура информационной безопасности; культурология; социально-культурные риски; интернет-коммуникации; дезинформация в социальных сетях; психологическая война; деструктивный контент; традиционные ценности; социокультурная идентичность; социальная инженерия

Введение: проблема, методы и материалы

Вопросы безопасности компьютерно-телекоммуникационных технологий, первоначально преимущественно организационно-технические, дополняются педагогическими, психологическими, социальными и, наконец, культурологическими аспектами. Знания, умения и навыки обеспечения информационной безопасности всё более формируются в особую культуру, распространяясь практически во все отрасли и сферы общественной жизни, на всех граждан России, при этом обогащаясь социально-культурным содержанием. Использование преимуществ новых технологий, охватывающих всех граждан, всё более оказывается сопряжённым с социально-культурными ценностями высокого уровня, с сопутствующими угрозами и критическими рисками ущерба традиционным ценностям и идентичности [1].

В расширении информационной безопасности, вначале узкопрофессиональной, до общегражданской культуры, как это отмечают и зарубежные исследователи [2], важную роль играют два фактора. Это универсальное разнообразное повсеместное распространение компьютерно-телекоммуникационных технологий, известное как цифровая трансформация, и обострение международных отношений с технологически лидирующими странами и глобальными интернет-сервисами, базирующимися в США, связанное с началом в 2022 году специальной военной операции на Украине. Реализация «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации», утвержденной Правительством России 22 декабря 2022 г., требует профильного культурологического подхода.

Инструменты культурологии способны эффективно определить потенциал культурологов, теоретиков и работников культуры в повышении как профессиональной, так и общегражданской культуры информационной безопасности. Трудности формирования и развития непрофессиональной культуры информационной безопасности связаны, в частности, с новизной для широкой целевой аудитории проблематики, необходимостью «популяризации» понятий и терминологии, разработанных и использовавшихся лишь специалистами по технической защите информации и государственной тайны. Поэтому при формировании нарратива информационной безопасности для культурологов, теоретиков и работников культуры приходится жертвовать наукообразностью, стремясь к понятности рисков, угроз и средств противодействия злоумышленникам для широкой аудитории российских граждан.

1. Ограниченность технических факторов профессиональной культуры информационной безопасности

Современная культура информационной безопасности эволюционно формировалась в связи с развитием и распространением массовых гражданских применений компьютерных технологий. Первоначально, в 1940–1950-е годы, разработка и применение электронно-вычислительной и радиоэлектронной техники относились к военной тайне, поскольку осуществлялись для нужд шифрования сведений, каналов связи и для баллистических расчётов доставки атомных зарядов авиацией, артиллерией и боевыми ракетами. В 1960–1980-х годах ЭВМ и компьютерные сети начали всё шире применяться в гражданских целях для государственного и промышленного управления, сопровождаясь профессиональной защитой государственной и коммерческой тайны, обеспечением техники безопасности. К социально-культурным аспектам информационной безопасности тогда можно было отнести разве что декларации о рисках создания гипотетического «сильного искусственного интеллекта».

Технологической основой появления и повышения роли социально-культурных факторов информационной безопасности в 1990-е годы стало начало массового производства и распространения не только в организациях, но и среди граждан настольных персональных компьютеров, локальных сетевых решений. Поначалу безопасность работы на них носила в основном технический характер и относилась к пользовательской культуре, централизованные массовые интернет-сервисы только начинали развиваться. Использование гражданами компьютерного оборудования не было связано с ценностями, интересующими злоумышленников. Первое гражданское вредоносное программное обеспечение («вирусы») создавалось «из любви к искусству» или в хулиганских целях, без расчёта на получение финансовой или имущественной выгоды.

Возможности незаконно извлекать непосредственную выгоду от несанкционированного компьютерного доступа к ценностям пользователей, первоначально главным образом денежным, появились в 2000-е годы по мере распространения дистанционных банковских услуг. Банковские карты, банкоматы и платёжные интернет-сервисы быстро распространялись благодаря неведомым прежде удобствам для клиентов и выгодности для банков. Новые банковские технологии стали привлекательной мишенью для потенциальных злоумышленников, питательной средой формирования и развития массовой киберпреступности.

На этом этапе хищения денег в системах дистанционного банковского обслуживания совершались в основном при помощи технических средств, «банковских» вредоносных программ («вирусов») и специального оборудования (например, для «скимминга» – скрытого незаконного копирования банковских карт). Противодействие хищениям осуществляли профессионалы информационной безопасности банков посредством в основном технических, а также смежных организационных и нормативно-правовых инструментов. К началу 2010-х годов специалистам отрасли информационной безопасности банков удалось закрыть большинство уязвимостей, понизив до приемлемого уровня риски хищений денег злоумышленниками, применявшими технические средства.

Цифровая трансформация превратила практически всех граждан, модифицировав их идентичности, в пользователей персональных мобильных устройств с повсеместным круглосуточным широкополосным беспроводным доступом к интернет-сервисам [3]. В то же время использование интернет-коммуникаций стало сопряжено с высокоуровневыми ценностями массового пользователя, потенциально представляющими интерес для злоумышленников [4].

09KLSK124
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Первой массовой мишенью такого рода, к тому же обладающей «высокой ликвидностью», оказались денежные средства в системах дистанционного банковского обслуживания. Профессионалы информационной безопасности научили достаточно хорошо защищать технические средства дистанционных сервисов. Однако, после того как были закрыты большинство критических брешей технического характера, цифровая трансформация породила уязвимости нового, социально-культурного типа, которые также связывают с «человеческим фактором» [5]. Отсутствие культуры информационной безопасности у большинства граждан, превратившихся в круглосуточных и повсеместных пользователей интернет-сервисов, включая банковские, привело к мутации киберпреступности. Ситуацию осложняло отсутствие элемента информационной безопасности в массовой пользовательской культуре: интернет, мобильные телекоммуникации, несмотря на полные возможности анонимности и «поддельных личностей» пользователей, представлялись доверенной, надёжно защищённой средой.

2. Усиление массовых социально-культурных угроз цифровой трансформации

Злоумышленники начали всё больше предпочитать не технический «взлом» программного обеспечения, а хищения посредством манипуляций сознанием и поведением жертвы [6], обмана, мошенничества, шантажа и вымогательства (телефонного, по электронной почте, в социальных сетях и интернет-мессенджерах и т. п.), создания поддельных интернет-сайтов финансовых организаций. Оказалось практически невозможным защитить граждан, пользующихся финансовыми интернет-сервисами, без их участия, от такого типа атак только усилиями со стороны банков. Формирование гражданской культуры информационной безопасности было начато банками в виде предупреждений об актуальных угрозах и правилах защиты от злоумышленников при использовании дистанционных финансовых услуг. Также оказалось, что сами профессионалы информационной безопасности, хорошо ориентировавшиеся в основном в организационно-технических, нормативно-правовых аспектах, оказались слабо защищёнными от новых угроз безответственного поведения [7] и утончённых (целевых) схем обмана, которые в своём стиле окрестили «социальной инженерией».

Дальнейшая эволюция интернет-преступности характеризовалась увеличением разнообразия и совершенствованием приёмов и схем обмана пользователей, «диверсификацией» атакуемых ценностей граждан. Манипуляции сознанием стали применяться для извлечения незаконной, криминальной выгоды за счёт деформации, подмены, фальсификации вкусов, предпочтений, поведения, жизненных ценностей и принципов, самой социокультурной идентичности пользователей интернета [8]. В 2010-е годы социальные сети стремительно набрали массовую аудиторию, и возникли «группы по интересам», вовлекавшие в деструктивные зависимости [9], такие как самоубийства, потребление наркотиков, интернет-травлю (cyberbullying), «школьные расстрелы» (schoolshooting), экстремальное поведение и экстремистские сообщества.

С запозданием на несколько лет начали создаваться и активно действовать общественные органы и организации («Лига безопасного интернета» и др.), был принят ряд федеральных законов, защищающих права граждан в интернете. Органы государственной исполнительной власти были наделены полномочиями вести мониторинг незаконного и запрещённого содержания в интернете, ограничивать к нему доступ, отзывать делегирование доменных имён, вести расследования и привлекать к ответственности виновных. Как и в случае с дистанционными банковскими сервисами, оказалось невозможным защитить граждан от социокультурных угроз в интернете только мерами со стороны государства и организаций отрасли информационной безопасности. Назревала необходимость выработки и реализации целенаправленной политики изживания массовых предрассудков о том, что Интернет является

09KLSK124
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

доверенной средой выработки осторожности, понимания угроз трансграничной передачи данных, анонимности и подделки личностей злоумышленниками.

В 2020–2022 годы проблематику информационной безопасности граждан России обострили жёсткие ограничительные меры, предпринятые в связи с распространением коронавируса: произошёл пороговый всплеск количества пользователей и объёмов использования дистанционных интернет-сервисов (финансовых, образовательных, деловых и т. п.), и, соответственно, интернет-преступности. Ещё более критическим драйвером стали антироссийские санкции недружественных государств и зарубежных высокотехнологичных компаний, начатые под предлогом начала специальной военной операции на Украине.

С рядом технологически лидирующих стран практически прекратилось сотрудничество в противодействии международной киберпреступности; напротив, начались зарубежные атаки на компьютерную инфраструктуру и граждан России в рамках необъявленной гибридной войны. Глобальные цифровые сервисы, базирующиеся в США, начали проводить дискриминационную политику, цензуру и кампании «культуры отмены» [10] в отношении официальной прессы и граждан России, потворствуя трансляции фейк-новостей, дезинформации и другого запрещённого российскими законами контента. Зарубежное влияние на традиционные ценности и социально-культурную идентичность россиян, прежде оказывавшееся в формате «мягкой силы», приобрело открытый агрессивный характер [11]. И снова, как в случае с безопасностью дистанционных финансовых сервисов и пользования социальными сетями, возникла необходимость формирования и повышения массовой, общегражданской культуры информационной безопасности.

3. Роль теоретиков и практиков культуры, культурологов в формировании общегражданской культуры информационной безопасности

Наряду с мерами по противодействию на территории России незаконному контенту в интернете, блокировке, расследованию инцидентов и привлечению к ответственности виновных, Правительством России была принята «Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации» (Распоряжение от 22 декабря 2022 г. № 4088-р). Профильной наукой для осмысления и решения проблематики, разработки методов и средств повышения общегражданской культуры информационной безопасности во взаимодействии с другими дисциплинами является культурология. Структурно-функциональный подход позволяет выделить следующие основные направления такой культуры: профессиональное (в том числе самих специалистов по информационной безопасности) и массовое гражданское, относящееся к «бытовым» пользователям компьютерного оборудования и интернет-сервисов.

Культурологический нарратив информационной безопасности, в отличие от философского, психологического, педагогического и др., можно определить как рассмотрение методами культурологии социально-культурных аспектов противодействия угрозам российским гражданам, связанных с развитием и применением компьютерно-телекоммуникационных технологий, интернет-коммуникаций, универсальной цифровой трансформации. Культурологическая парадигма представляет культуру информационной безопасности как динамичную развивающуюся систему направлений, видов и подвидов; которым присущи различные сочетания организационно-технических, нормативно-правовых и социально-культурных аспектов и элементов [12]. Задача культурологии как науки заключается в определении социально-культурных угроз, характера их содержания, соотношений с другими факторами, потенциального ущерба и средств его минимизации, предотвращения. Как профильные специалисты культурологи могут быть эффективны, участвуя в разработках

09KLSK124
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

социально-культурных разделов моделей угроз (от «социальной инженерии» до цифровой автоматизированной дезинформации, фальсификации идентичности) и нарушителей, а также в выработке средств противодействия, в том числе превентивного. Среди недавних примеров — анализ психосоциальных рисков игровой активности в виртуальной реальности [13], «социально-культурного искусственного интеллекта» [14], а также результаты культурологического исследования мнимых и действительных социально-культурных угроз российским гражданам со стороны автоматизированных моделей генерации текстов [15], включая ChatGPT — зарубежный (США) машинный генератор текстовых ответов, имитирующего диалог [16].

Противодействие санкциям и дискриминационным мерам недружественных государств и высокотехнологичных корпораций ставит перед специалистами по информационной безопасности задачу обеспечить цифровой суверенитет России и независимость от импорта. Актуализируется интерес к лучшим примерам отечественной истории и своей профессии, традиционным ценностям и социально-культурной идентичности; зарубежные исследователи обращают внимание на важность их «цифровых» представлений [17]. Динамика увеличения доли и значения социально-культурных аспектов информационной безопасности позволяет оценивать потребность в культурологах и работниках культуры как универсальную практически для всех отраслей и профессий, а также для развития профильной массовой «бытовой» культуры граждан [18]. В свою очередь, участие в научных исследованиях и разработках практических методик противодействия цифровым социально-культурным угрозам, повышения общегражданской культуры информационной безопасности потребует от культурологов овладения спецификой подобной проблематики, понятийным аппаратом и методами.

Новая культурологическая специализация – это социально-культурные аспекты, а также развитие профессиональной и массовой культуры информационной безопасности. Методы культурологии не проецируются механически на безопасность разработки и применений новых цифровых сервисов. Для формирования культурологической парадигмы информационной безопасности требуется синтетическое осмысление и организационно-методическое обеспечение практики противодействия новым угрозам, связанным с цифровой трансформацией, универсальным распространением и применением компьютерно-сетевых технологий.

Подытоживая изложенное, можно прогнозировать увеличение потребности в культурологах соответствующих специализаций в работе организаций и подразделений информационной безопасности, а также для разработки разделов учебных программ и преподавания в системах профессиональной подготовки таких специалистов [19]. В настоящий момент вряд ли существует достаточный резерв культурологов, теоретиков и работников культуры, специализирующихся на социально-культурных аспектах информационной безопасности. Для таких специалистов в необходимых количествах потребуется расширение профессиональных и образовательных стандартов новыми специализациями, а также создание, в том числе на базе существующих, новых профильных образовательных программ высшего образования, курсов повышения квалификации и профессиональной переподготовки.

Заключение: выводы и результаты

Проведённое исследование позволяет следующим образом определить нарратив информационной безопасности для культурологов, теоретиков и работников культуры. Развитие компьютерно-сетевых технологий и интернет-сервисов, распространение их в ходе цифровой трансформации до общегражданских масштабов привели к решающему увеличению

значения социально-культурных аспектов информационной безопасности. С одной стороны, современный профессионализм информационной безопасности не сводится к организационно-техническим и нормативно-правовым аспектам [20], а требует противодействия угрозам сознанию, личности пользователей. С другой стороны, необходимы формирование и развитие массовой культуры информационной безопасности, поскольку угрозы ценностям граждан (в том числе традиционным и социально-культурной идентичности) приобрели цифровой характер, напрямую связаны с преимуществами интернет-сервисов. Новизна результатов исследования заключается в установлении высокого потенциала культурологического нарратива информационной безопасности в решении проблемы формирования общегражданской культуры информационной безопасности, профессиональной и массовой.

Главный вывод исследования заключается в актуальности применения культурологического подхода как профильного для осмысления и научно-методического обеспечения развития общегражданской культуры информационной безопасности. Культурологическая парадигма информационной безопасности включает систему взаимодействия профильной специализации профессиональной и общегражданской, массовой культуры информационной безопасности. Прогнозируется и доказывается эффективность создания специализированной подготовки культурологов, теоретиков и работников культуры в области профессиональной и массовой информационной культуры безопасности.

ЛИТЕРАТУРА

1. Буравлева Н.А., Атаманова И.В. Психологические характеристики деятельности, традиционные ценности и ценности безопасности вузовской молодежи в контексте инновативности // Сибирский психологический журнал. 2022 — № 84 — С. 48–69. DOI: 10.17759/psylaw.2021110415.
2. Shillair R., Esteve-González P., Dutton W.H., Creese S., Nagyfejeo E., Solms B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise // Computers & Security. 2022 — Т. 119. DOI: 10.1016/j.cose.2022.102756.
3. Труфанова Е.О., Хан Ш.Д. Трансформации культурной идентичности в цифровую эпоху // Вопросы философии. 2022 — № 12 — С. 84–94. DOI: 10.21146/0042-8744-2022-12-84-94.
4. Шайгерова Л.А., Шилко Р.С., Ваханцева О.В. Культурное опосредование идентичности цифрового поколения: перспективы анализа интернет-активности и социальных медиа // Вестник Московского университета. Серия 14: Психология. 2022 — № 2 — С. 73–107. DOI: 10.11621/vsp.2022.02.04.
5. Alsharida R., Al-rimy B., Al-Emran M., Zainal A. A systematic review of multi perspectives on human cybersecurity behavior // Technology in Society. 2023 — Т. 73. DOI: 10.1016/j.techsoc.2023.102258.
6. Khan N.F., Yaqoob A., Khan M. S., Ikram N. The cybersecurity behavioral research: A tertiary study // Computers & Security. 2022 — Т. 120. DOI: 10.1016/j.cose.2022.102826.
7. Ebert N., Schaltegger Th., Ambuehl B., Schöni L., Zimmermann V., Knieps M. Learning from safety science: A way forward for studying cybersecurity incidents in organizations // Computers & Security. 2023 — Т. 134. DOI: 10.1016/j.cose.2023.103435.

8. Карепова С.Г., Карепов Г.Е. Социокультурный аспект информационной безопасности: «мусорное искусство» как инструмент социальной реальности // Гуманитарные, социально-экономические и общественные науки. 2023 — № 2 — С. 29–33. DOI: 10.23672/SAE.2023.24.38.001

9. Булва В.И. Феномен социальных сетей в контексте информационной безопасности // Международная жизнь. 2023 — № 3 — С. 52–61. EDN: YXFOLG.

10. Былевский П.Г., Цацкина Е.П. Феноменологический анализ явления «культура отмены» // Вестник Московского государственного лингвистического университета. Гуманитарные науки. 2022 — № 2(857) — С. 162–169. DOI: 10.52070/2542-2197_2022_2_857_162.

11. Галяшина Е.И., Богатырев К.М. Понятие «традиционные российские духовно-нравственные ценности» в контексте обеспечения медиабезопасности в интернет-среде // Lex Russica (Русский закон). 2022 — Т. 75 — № 10(191) — С. 138–151. DOI: 10.17803/1729-5920.2022.191.10.138-151.

12. Бегишев И.Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021 — Т. 11 — № 4 — С. 207–220. DOI: 10.17759/psylaw.2021110415.

13. Gao W., Li L., Xue Y., Zhang J. Design of security management model for communication networks in digital cultural consumption under Metaverse — The case of mobile game // Egyptian Informatics Journal. 2023 — Т. 24 — №. 2 — С. 303–311. DOI: 10.1016/j.eij.2023.05.004.

14. Venkatachalam P., Mishra R. Fifteen shadows of socio-cultural AI: A systematic review and future perspectives // Futures. 2021 — Т. 132. DOI: 10.1016/j.futures.2021.102817.

15. Мельников С.Ю., Пересыпкин В.А. Об эволюции классических вероятностных моделей языка в естественно-языковых приложениях // Вестник современных цифровых технологий. 2023 — № 16 — С. 4–14. EDN: YDIGDT.

16. Былевский П.Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023 — № 8 — С. 46–56. DOI: 10.7256/2454-0757.2023.8.43909.

17. Younus I., Al-Hinkawi W., Lafta S. The role of historic building information modeling in the cultural resistance of liberated city // Ain Shams Engineering Journal. 2023 — Т. 14 — № 10. DOI: 10.1016/j.asej.2023.102191.

18. Малюк А.А., Малюк З.П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности // Безопасность информационных технологий. 2021 — Т. 28 — № 4 — С. 6–21. DOI:10.26583/bit.2021.4.01.

19. Казинец В.А., Редько Е.А. Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022 — № 5 — С. 22–25. EDN: PTLIUR.

20. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023 — № 5 — С. 131–144. DOI:10.31857/S102694520025209-0.

Bylevskiy Pavel Gennadievich
Moscow State Linguistic University, Moscow, Russia
E-mail: pr-911@yandex.ru
ORCID: https://orcid.org/0000-0002-0453-526X
RSCI: https://elibrary.ru/author_profile.asp?id=283871

Information security narrative for cultural scientists, theorists and cultural workers

Abstract. The purpose of the study is to determine the role, possibilities and theoretical principles of participation of cultural scientists, theorists and cultural workers in the development and implementation of measures to counter threats associated with the use of computer technologies and Internet communications. The subject of the study is the cultural narrative of scientific publications on information security in 2021–2023. The object of the study is the current risks to traditional values and identity caused by universal digital transformation and, after the start of a Special military operation in Ukraine in 2022, the aggravation of international relations with technologically leading countries and global Internet services based in the United States. The relevance of the topic is determined, in particular, by the approval by the Russian Government on December 22, 2022 of the «Concept of formation and development of the culture of information security of citizens of the Russian Federation». The research methodology is characterized by the application of a cultural paradigm (an approach to the culture of information security as a dynamic system of human activity), structural, functional and evolutionary methods. Publications in the journals HAC K1, K2 and Scopus Q1, Q2 were used as materials.

The novelty of the article lies in the study of the potential of the cultural narrative of information security in solving the problem of forming a general civil culture of information security, professional and mass. The research was carried out within the framework of the state assignment of the Moscow State Pedagogical University on the topic of research «Cultural identity in the modern world: analytical models, methods of construction and forms of presentation» (state registration number AAAA-A19-119072590048-4). The result of the study is a conclusion about the increasing share and importance of socio-cultural factors in information security in comparison with technical ones. Cultural theory and cultural studies are defined as specialized disciplines for improving both professional and civil information security culture. The cultural paradigm of information security includes a system of interaction between the profile specialization of professional and general civil, mass culture of information security. The effectiveness of the creation of specialized training for cultural scientists, theorists and cultural workers in the field of professional and mass information security culture is predicted and proved.

Keywords: information security culture; cultural studies; socio-cultural risks; Internet communications; disinformation in social networks; psychological warfare; destructive content; traditional values; socio-cultural identity