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

2023, Том 14, № 3 / 2023, Vol. 14, Iss. 3 https://sfk-mn.ru/issue-3-2023.html

URL статьи: https://sfk-mn.ru/PDF/28KLSK323.pdf

DOI: 10.15862/28KLSK323 (https://doi.org/10.15862/28KLSK323)

5.10.1. Теория и история культуры, искусства (культурология)

Ссылка для цитирования этой статьи:
Былевский, П. Г. Формирование культуры информационной безопасности граждан России: эволюционная периодизация / П. Г. Былевский // Мир науки. Социология, филология, культурология. — 2023. — Т. 14. — № 3. — URL: https://sfk-mn.ru/PDF/28KLSK323.pdf. DOI: 10.15862/28KLSK323

For citation:
Bylevskiy P.G. Formation of the culture of information security of Russian citizens: evolutionary periodization. *World of Science. Series: Sociology, Philology, Cultural Studies*. 2023; 14(3): 28KLSK323. Available at: https://sfk-mn.ru/PDF/28KLSK323.pdf. (In Russ., abstract in Eng.). DOI: 10.15862/28KLSK323

УДК 008+004.056

Былевский Павел Геннадиевич
ФГБОУ ВО «Московский государственный лингвистический университет», Москва, Россия
Доцент кафедры «Информационной культуры цифровой трансформации
и 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

Формирование культуры информационной безопасности граждан России: эволюционная периодизация

Аннотация. Предметом теоретического анализа, представленного в статье, является периодизация становления культуры информационной безопасности в России, совершённая при помощи метода культурологического эволюционного анализа. Выполнение этой задачи предваряет последующую разработку культурологической парадигмы, структурно-функциональной модели и практических методик повышения информационной безопасности российских граждан. Принятие Правительством России 22 декабря 2022 года Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации подтверждает актуальность указанной темы.

Культурологический анализ существующих концепций выработки культуры информационной безопасности (по материалам теоретических, исследовательских и научно-практических работ последних лет) показал ограниченность узкой специализации (технической, нормативно-правовой, организационной, психологической, педагогической др.). Сделан вывод о том, что востребован профильный системный подход культурологии, выявляющий специфику перечня и сочетаний различных элементов, дисциплин и стадий формирования профессиональной культуры информационной безопасности в разных отраслях и в общегражданской сфере.

Эволюционный анализ позволяет определить пять этапов исторического развития цифровых компьютерно-телекоммуникационных сетевых технологий, начиная с создания в конце 1940-х годов до современного универсального распространения «цифровой

трансформации». Выявлено, что применение этих технологий изначально требует формирования соответствующей пользовательской культуры, включая обеспечение безопасности. Развитие и усложнение технологий, областей и способов их применения сопровождается эволюцией угроз и рисков, требующей развития направлений и содержания культуры информационной безопасности как профессиональной, так и общегражданской.

Результатом теоретического анализа является вывод о том, что культурология является профильной научной дисциплиной для выбора и определения соотношений технических и социально-культурных компонентов, последовательности этапов и инструментов формирования и развития различных видов культуры информационной безопасности. Разработка парадигмы, динамичной системной культурологической модели информационной безопасности позволяет научно осмыслить особенности и соотношение профессиональной, специализированной и массовой общегражданской культуры безопасности применения компьютерно-телекоммуникационных сетевых технологий. Также сделан вывод, что понятийно-категориальный аппарат и методология культурологии обеспечивают более адекватную разработку эффективных практических методик и других инструментов развития культуры информационной безопасности российских граждан.

Ключевые слова: культура информационной безопасности; угрозы; риски; противодействие; социальная инженерия; дезинформация; фейк-новости; фальсификация истории

Введение: проблема, методы и материалы

Актуальность проблемы формирования и развития общегражданской культуры информационной безопасности обусловлена повсеместным развитием и массовым применением компьютерно-телекоммуникационных сетевых технологий, включая универсальность цифровой трансформации, и обострением международных отношений с 2022 года. Несмотря на неуклонное увеличение всё больших значительных разнообразных преимуществ таких технологий, проявляются, порой неожиданно, обременяющие их сопутствующие угрозы и риски [1]. Целый комплекс подобных новых факторов вызвал утверждение 22 декабря 2022 года Правительством России «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации».[1]

Без обеспечения безопасности сопряжённый ущерб разных уровней (личностного, национального и международного) может превосходить преимущества применения новых технологий, вплоть до критического и неприемлемого масштаба [2]. Технологической основой необходимости в информационной безопасности служат компьютерно-телекоммуникационные сетевые технологии, а социально-культурной — возможность сопутствующих нарушений, способных привести к ущербу пользователям. Противодействие сопряженным рискам и угрозам требует соответствующего комплекса знаний, умений, навыков и убеждений, а в современных условиях — сложной динамичной системы культуры обеспечения информационной безопасности. Культура информационной безопасности превращается в неотъемлемый фактор обеспечения государственного суверенитета и национальной безопасности [3].

[1] Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации (утверждена распоряжением Правительства Российской Федерации от 22 декабря 2022 г. № 4088-р (Дата опубликования: 23.12.2022). С. 1–9. [Электронный ресурс] URL: http://publication.pravo.gov.ru/Document/View/0001202212230035 (дата обращения 12.08.2023).

Уже в первоначальном становлении узкопрофессиональной, преимущественно технической, культуры информационной безопасности неотъемлемо присутствуют как дополнительные вторичные, но необходимые смежные гуманитарные аспекты обеспечения безопасности: нормативно-правовые, педагогические, психологические и социально-культурные [4]. Нормативно-правовые инструменты включали законы, стандарты, нормативные акты, инструкции и правила; психолого-педагогические методики применялись при обучении, в учебно-воспитательном процессе; к социально-культурным факторам относились личностные убеждения и моральные ценности, опыт, мастерство, авторитет [5].

Публичного системного культурологического осмысления информационной безопасности не производилось, поскольку кроме технических компетенций было достаточно традиций корпоративного самосознания сотрудников спецслужб и военнослужащих. Для научного обоснования и выработки практических методик развития различных направлений и видов культуры информационной безопасности востребована культурологическая парадигма — динамическая системная модель. Определение её структурно-функциональных элементов и стадий развития требует предварительного изучения истории становления методом культурологического эволюционного анализа.

Пять этапов становления культуры информационной безопасности российских граждан

Культурологический эволюционный анализ позволяет выделить пять этапов формирования культуры информационной безопасности в соответствии с периодизацией развития и распространения компьютерно-телекоммуникационных сетевых технологий в России (предварительно, до 1991 года, в СССР).

Первый этап — формирование «корпоративной» узкопрофессиональной культуры применения в государственной сфере (конец 1940-х — 1980-е годы). Технологической основой служат централизованные цифровые электронно-вычислительные машины (ЭВМ), вычислительные центры и их сети на основе проводной и радиоэлектронной связи. Сферой использования являются армия (противовоздушная оборона, ракетные войска и т. п.) и государственное управление (в т. ч. для ведения статистики, отраслевое, в науке и промышленности). Коммерческая конкуренция в СССР отсутствует, риски кибердиверсий пренебрежимо низки, угрозы исходят в основном от зарубежных спецслужб и технических разведок. Культура работы на ЭВМ носит специализированно профессиональный характер, выходя за пределы техники безопасности лишь в вопросах защиты государственной тайны.

Второй этап в связи с массовым производством доступных и простых в использовании настольных персональных компьютеров, программного системного и прикладного обеспечения характеризуется распространением компьютерных телекоммуникационных технологий на гражданские сферы, включая коммерческую деятельность, преимущественно корпоративную (1990-е годы). За вычетом угроз со стороны иностранных спецслужб или коммерческой разведки, компьютерной преступности как значимого явления ещё не существует. Первое вредоносное программное обеспечение («вирусы») создаётся «из любви к искусству» или «из хулиганских побуждений», а не как техническое средство получения выгоды за счёт жертвы.

Культура информационной безопасности начинает приобретать гражданский и негосударственный характер, поначалу в профессиональном формате применительно к отраслевым особенностям. Обеспечение информационной безопасности чаще всего выступает дополнительной обязанностью системных администраторов, ещё не выделяясь в отдельное направление деятельности, в специализированные профильные должности и подразделения организаций. На этом этапе в культуру информационной безопасности включены

28KLSK323
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

преимущественно технические аспекты обеспечения устойчивой бесперебойной работы и предотвращения поломок оборудования, программного обеспечения и данных. Защищались, часто в рамках охраны объектов, компьютерное и сетевое оборудование, программное обеспечение, конфиденциальные (секретные) сведения [6]. Средства защиты носили технический характер, в основном программно-аппаратный.

Третий этап — 2000-е годы, широкое использование корпоративных систем и индивидуальных персональных настольных компьютеров. Для этого этапа существенно появление массовых телекоммуникационных сервисов, корпоративных и индивидуальных: мобильной (сотовой) телефонной связи и «медленного» подключения к единой глобальной сети Интернет (web 1.0, электронная почта, мессенджеры) [7]. Среди таких массовых сервисов следует отметить как особенно значимое для содержания и распространения культуры информационной безопасности дистанционное банковское обслуживание (банкоматы, мобильные платежи и интернет-банкинг с настольных персональных компьютеров клиентов).

Социально-культурную значимость информационной безопасности банков следует рассмотреть подробнее, она является репрезентативной, показательной для других отраслей из-за совмещения комплекса важных факторов. Во-первых, дистанционные банковские сервисы позволяют оперировать с денежными средствами, наиболее привлекательной целью для злоумышленников, лёгко конвертируемой в большинство других видов ценностей. Во-вторых, это негосударственная коммерческая сфера, массово охватывающая граждан, потенциально всех, обладающих правом распоряжаться денежными средствами. В-третьих, дистанционное банковское обслуживание создаёт возможность доступа повсеместно, из специально не защищённых публичных мест и домохозяйств. Интернет, телекоммуникационная среда дистанционного банкинга является не доверенной средой, трансграничной и с базовой анонимностью пользователей.

Особая ценность, большая привлекательность защищаемых активов определяют необходимость значительных ресурсов и высокой квалификации для совершения атак злоумышленниками и на порядки больших (включая культуру информационной безопасности) для их защитников. На этом этапе происходит становление, стремительное развитие и стремительное распространение («цунами») массовой компьютерной преступности, преимущественно хищений денежных средств в дистанционном банковском обслуживании. Приоритет принадлежит техническим средствам несанкционированного доступа, в основном специализированному вредоносному программному обеспечению («вирусам»).

Трансформация профессиональной культуры информационной безопасности на этом этапе носит скорее «реактивный», то есть реагирующий, чем прогностический, предупредительный характер [8]. Хотя государственные меры защиты персональных данных граждан относились больше не к реальным, а прогнозируемым на то время угрозам. По практической необходимости к техническим средствам обеспечения информационной безопасности и противодействия нарушителям добавляются организационные и нормативно-правовые инструменты, а также педагогические — развивается система подготовки профильных специалистов. Всё же задачу создания эффективной системы противодействия техническим угрозам информационной безопасности, основанной на технических же средствах, можно было считать выполненной, что подтверждали статистические данные Банка России[2], главного государственного регулятора информационной финансовой отрасли.

[2] Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2018–31.08.2019. С. 1–41. [Электронный ресурс] URL: https://cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (дата обращения 12.08.2023).

Четвёртый этап — 2010-е годы, характеризуется практически всеобщей массовостью пользования компьютерно-телекоммуникационными сетевыми технологиями, увеличением разнообразия, качественным усложнением сервисов. Универсальный характер этих преобразований обозначен понятием цифровой трансформации или цифровизации [9]. Происходит взаимодополняющее развитие, с одной стороны, централизованных вычислений, сетей, с другой стороны — детализированной спецификации всё большего разнообразия индивидуальных компьютерных устройств. Раскрываются и реализуются всё новые небывалые прежде возможности новых технологий, но также и связанные с ними угрозы и риски информационной безопасности, требующие соответствующего развития культуры её обеспечения.

Большинство населённых территорий России покрывается широкополосным (быстрым, потоковым) доступом в Интернет, включая беспроводной (в том числе мобильный, на базе сотовой связи стандартов 4G), позволяющий транслировать видео в высоком разрешении в реальном времени. Развиваются облачные вычисления и технологии распределённых реестров (блокчейн), создаются центры обработки данных, предоставляющие дистанционные корпоративные и индивидуальные услуги. Начинают широко внедряться интерактивные технологии web 2.0, позволяющие пользователю оценивать и комментировать, а также создавать и публиковать контент (текстовые, иллюстрированные и видеоблоги) [10]. Создаются и обретают миллиардные аудитории пользователей глобальные (в основном базирующиеся в США) и национальные публичные цифровые платформы — видеохостинги и социальные сети. Получают массовое распространение мобильные персональные компьютерные устройства (смартфоны, планшеты и гаджеты), относительно автономные от электросетей благодаря аккумуляторам и рассчитанные на постоянное подключение к беспроводным сетям, интернету. Развивается «интернет вещей» (Internet Of Things) — промышленная и бытовая техника, возникают возможность и необходимость автоматизации анализа «больших данных» и дистанционных сервисов (технологий «искусственного интеллекта») [11].

В информационной безопасности появляются новые угрозы и риски, требующие обновления и расширение перечня средств противодействия, с необходимостью включающие развитие профессиональной, также уже и общегражданской культуры [12]. Пользователями стали практически все граждане, чьё ежедневное пользование интернетом стало измеряться часами; увеличение разнообразия сетевых сервисов привело к разрастанию целей злоумышленников — перечня различных ценностей высокого уровня, мишеней и потенциальных жертв. Приобрели высокую ценность «большие пользовательские данные», как для коммерческой аналитики для целевой рекламы и маркетинга, так и для недобросовестного манипулирования общественным сознанием [13]. Из-за усиления профессиональной защиты корпоративных компьютерных систем и клиентских сервисов, включая банковские, связанной с повышением профессиональной культуры информационной безопасности, их «взлом» стал для злоумышленников слишком трудоёмким, невыгодным. Напротив, значительно расширилось количество клиентов дистанционных банковских сервисов, не обладающих должной общегражданской культурой информационной безопасности, в том числе использования финансовых инструментов.

В отличие от предыдущего этапа, когда основным видом компьютерных преступлений была кража чужих денег в дистанционном банковском обслуживании, у злоумышленников появились многие новые ценные цели, увеличилось количество угроз и видов нарушений информационной безопасности (в том числе преступлений). В такой репрезентативной области информационной безопасности, как финансовая отрасль, в статистическом отчёте государственного регулятора в 2019 году был отмечен качественный сдвиг основного вектора мишеней и инструментария атак злоумышленников с технических на социально-культурные. Исходя из привычной для технических специалистов терминологии, новый феномен был

28KLSK323
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

определён «социальной инженерией» (включая «телефонные мошенничества»), к которому отнесли подавляющее большинство, 97 % атак.

Мишенью вместо прежних компьютерных средств дистанционного банковского обслуживания стало сознание, психологическое состояние клиентов, а средством хищений не технические «отмычки» (вредоносное программное обеспечение и др.), а «схемы» манипулирования сознанием. Классификация самых распространённых нарушений информационной безопасности стала соотноситься с мошенничеством, а не как прежде с кражей или взломом с применением технических средств (компьютерных). Был сделан вывод невозможности защитить от социальной инженерии клиента без его осведомлённости, умения распознать угрозу и правильно реагировать. Для государственных и финансовых организаций проявилась необходимость повышать осведомлённость клиентов и населения об актуальных угрозах и общей проблематике, формировать и развивать общегражданскую культуру информационной безопасности [14].

В этот же период в области интернет-сервисов был обозначен целый комплекс новых угроз также преимущественно социально-культурного характера, в противодействии которым ключевая роль принадлежит не новым техническим средствам защиты, а повышению культуры информационной безопасности [15]. Речь идёт о криминальной, экстремистской и другой незаконной деятельности, деструктивном контенте на веб-ресурсах, в социальных сетях, видеохостингах, мессенджерах и др. (фейк-новостям, побуждении к самоубийствам, «школьным расстрелам», «кибербуллингу» и т. п.). Регулировать, отслеживать незаконный контент и блокировать нарушающие законодательство интернет-ресурсы была уполномочена Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Однако параллельно был принят курс на формирование основ общегражданской культуры информационной безопасности, для молодёжи, подростков [16] и детей («интернет-гигиены» и т. п.) [17] в рамках предметов информатики и общей безопасности жизни, а для остальных возрастных категорий — средствами социальной рекламы, официальной прессы и др.

Пятый этап — с 2020 года по настоящее время, связан со скачкообразным увеличением использования дистанционных интернет-сервисов в 2020 году, вызванного «коронавирусными» карантинными ограничениями на посещение публичных мест гражданами. Статистика Банка России зафиксировала резкий рост как дистанционных финансовых операций, так и атак «социальной инженерии». Второй «триггерной точкой» стало начало специальной военной операции на Украине в феврале 2022 года. При сохранении прежней технологической основы проявились новые негативные реалии [18], связанные с кризисным обострением международных отношений, исчерпанием однополярного глобализма.

Прекратилось сотрудничество с недружественными странами в противодействии международной киберпреступности. Напротив, в формате гибридных войн участились и усилились проводимые через интернет трансграничные компьютерные атаки на российские объекты критической инфраструктуры. Социально-культурными коннотациями обладали технологические антироссийские санкции недружественных стран и цензура российской официальной прессы со стороны глобальных цифровых платформ, базирующихся в США. Задачи достижения полноценного цифрового суверенитета и независимости от технологического импорта из недружественных стран оказались не только организационно-техническими, но также потребовали от профессионалов информационной безопасности существенной переоценки личных социально-культурных ценностей, существенной ревальвации патриотизма [19].

Недружественными странами с их территорий осуществляется целый комплекс различных социально-культурных, психологических атак на сознание российских граждан:

28KLSK323
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

«социальной инженерии» для хищений денежных средств, фейк-новостей, фальсифицированной аналитики и дезинформации, попыток организации массовых беспорядков и т. п. Государственная защита от вредоносного социально-культурного контента на интернет-ресурсах, включая прессу и социальные сети, обязательно должна дополняться формированием общегражданской массовой культуры информационной безопасности [20]. Выводы, сделанные в финансовой сфере во второй половине 2010-х годов, получили подтверждение и в других отраслях и социально-культурных областях [21], практически во всех направлениях применения компьютерно-телекоммуникационных технологий, что и привело к необходимости выстраивания «всеобуча» информационной безопасности.

Заключение: выводы и результаты

Результатом теоретического анализа, совершённого посредством эволюционного культурологического метода, является определение пяти этапов формирования культуры информационной безопасности россиян, соответствующих различным уровням развития и применения компьютерно-телекоммуникационных сетевых решений с конца 1940-х годов до современности. Выявлено становление таких структурно-функциональных направлений, как профессиональная, специализированная и массовая, общегражданская культура информационной безопасности. Установлено, что даже для узкопрофессиональной культуры информационной безопасности техническим аспектам изначально сопутствуют социально-культурные, роль которых увеличивается по мере усложнения технологий и расширения их гражданских применений. Общегражданская культура информационной безопасности становится необходимой при цифровой трансформации (универсальном повсеместном постоянном применении гражданами компьютерно-телекоммуникационных сетевых технологий) и нарастании угроз общественным и личным социально-культурным ценностям.

Таким образом, культурология является профильной научной дисциплиной для выбора и определения соотношений технических и социально-культурных компонентов, последовательности этапов и инструментов формирования и развития различных видов культуры информационной безопасности. Разработка парадигмы, динамичной системной культурологической модели позволяет классифицировать и упорядочить профессиональную, специализированную и массовую общегражданскую культуру безопасности применения компьютерно-телекоммуникационных сетевых технологий. Культурологический понятийно-категориальный аппарат и методология являются адекватными средствами для развития культуры информационной безопасности российских граждан, практической разработки необходимого методического обеспечения.

ЛИТЕРАТУРА

1. Люханова С.В. Риски России в эпоху четвёртой промышленной революции // Менеджмент в России и за рубежом. — 2021. — № 4. — С. 22–28. EDN: MAHIJH.
2. Da Veiga A., Astakhova L., Botha A., Herselman M. Defining organisational information security culture — Perspectives from academia and industry // Computers & Security. May 2020. Vol. 92. DOI: 10.1016/j.cose.2020.101713.
3. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51–57. DOI: 10.25136/2409-7543.2023.1.40078.

28KLSK323
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

4. Hughes-Lartey K., Li M., Botchey F., Qin Zh. Human factor, a critical weak point in the information security of an organization's Internet of things // Heliyon. March 2021. Vol. 7. Iss. 3. DOI: 10.1016/j.heliyon.2021.e06522.

5. Рудинский И.Д., Околот Д.Я. Культура информационной безопасности. Понятие и содержание // Информатизация образования и науки. 2020. № 3(47). С. 39–44. EDN: SYDCQC.

6. Tolah A., Furnell S., Papadaki M. An empirical analysis of the information security culture key factors framework // Computers & Security. September 2021. Vol. 108. DOI: 10.1016/j.cose.2021.102354.

7. Краснова Г.В. Формирование культуры личной информационной безопасности в развивающемся обществе // Социология и право. — 2018. — № 2(40). — С. 54–60. EDN: UTCKTU.

8. Lin C., Wittmer J., Luo X. Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance // Information & Management. September 2022. Vol. 59. Iss. 6. DOI: 10.1016/j.im.2022.103650.

9. Ефимова О.В., Комарова Ю.В. Развитие культуры безопасности в интеграции с цифровой культурой // Автоматика, связь, информатика. 2021. № 3. С. 14–16. EDN: RDYFSO.

10. Gebremeskel B., Jonathan G., Yalew S. Information Security Challenges During Digital Transformation // Procedia Computer Science. 2023. Vol. 219. Pp. 44–51. DOI: 10.1016/j.procs.2023.01.262.

11. Ameen N., Tarhini A., Shah M., Madichie N., Paul J., Choudrie J. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce // Computers in Human Behavior. January 2021, Vol. 114. DOI: 10.1016/j.chb.2020.106531.

12. Троян Н.А. Влияние цифровых технологий на повышение уровня культуры информационной безопасности граждан России // Мониторинг правоприменения. 2023. № 1(46). С. 20–26. DOI: 10.21681/2226-0692-2023-1-20-26.

13. Былевский П.Г. Пользовательские и персональные данные — анализ рисков извлечения знаний // Вопросы защиты информации. 2023. № 1(140). С. 35–40. DOI: 10.52190/2073-2600_2023_1_35.

14. 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.

15. Литвишков В.М., Вилкова А.В., Швырев Б.А. Измерение изменения культуры информационной безопасности // Уголовно-исполнительная система: право, экономика, управление. 2020. № 5. С. 27–29. DOI: 10.18572/2072-4438-2020-5-27-29.

16. Магомедов Р.В., Минбулатова И.С. Формирование культуры безопасности жизнедеятельности учащихся в условиях цифровой трансформации образования // Известия Дагестанского государственного педагогического университета. Психолого-педагогические науки. 2021. Т. 15. № 2. С. 58–64. DOI: 10.31161/1995-0675-2021-15-2-58-64.

17. Ерина Ю.С., Кокаева И.Ю. Формирование культуры информационной безопасности у студентов — будущих учителей — в процессе профессиональной подготовки // Вестник КемГУКИ. — 2017. — № 41. — С. 186–194. EDN: YKHJDX.

18. 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.

19. Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12: Политические науки. 2022. № 2. С. 31–45. EDN: BJJUXI.

20. Tejay G., Mohammed Z. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective // Information & Management. April 2023. Vol. 60. Iss. 3. DOI: 10.1016/j.im.2022.103751.

21. Кирсанов А.И. Информационная культура — стратегический ресурс политической безопасности личности в информационном обществе // Власть. — 2021. — Т. 29. — № 2. — С. 62–70. DOI: 10.31171/vlast.v29i2.7997.

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

Formation of the culture of information security of Russian citizens: evolutionary periodization

Abstract. The subject of the theoretical analysis presented in the article is the periodization of the formation of the culture of information security in Russia, carried out using the method of cultural evolutionary analysis. The fulfillment of this task precedes the subsequent development of a cultural paradigm, a structural and functional model and practical methods for improving the information security of Russian citizens. The adoption by the Russian Government on December 22, 2022 of the Concept of Formation and Development of the Culture of Information Security of the Citizens of the Russian Federation confirms the relevance of this topic.

The culturological analysis of the existing concepts of developing a culture of information security (based on the materials of theoretical, research and scientific-practical works of re-cent years) has shown the limitations of a narrow specialization (technical, regulatory, organizational, psychological, pedagogical, etc.). It is concluded that a profile systematic approach of culturology is in demand, which is the specifics of the list and combinations of various elements, disciplines and stages of the formation of a professional culture of information security in different sectors and in the general civil sphere.

The evolutionary analysis allows us to identify five stages of the historical development of digital computer and telecommunication network technologies, starting from the creation in the late 1940s to the modern universal distribution — «digital transformation». It is revealed that the use of these technologies initially requires the formation of an appropriate user culture, including ensuring safety. The development and complication of technologies, areas and methods of their application is accompanied by the evolution of threats and risks that require the development of directions and content of information security culture, both professional and civil.

The result of the theoretical analysis is the conclusion that cultural studies is a specialized scientific discipline for the selection and determination of the ratios of technical and socio-cultural components, the sequence of stages and tools for the formation and development of various types of information security culture. The development of a paradigm, a dynamic system culturological model of information security allows us to scientifically comprehend the features and correlation of professional, specialized and mass civil security culture of the use of computer and telecommunication network technologies. It is also concluded that the conceptual and cate-gorical apparatus and methodology of cultural studies provide a more adequate development of effective practical techniques and other tools for the development of the culture of information security of Russian citizens.

Keywords: information security culture; threats; risks; counteraction; social engineering; disinformation; fake news; falsification of history