КУЛЬТУРОСООБРАЗНЫЕ ПРАКТИКИ

Научная статья
УДК 008, 130:2, 004.56
DOI: 10.20323/1813-145X_2023_6_135_232
EDN: XANZER

Культурологические аспекты формирования информационной безопасности граждан

Павел Геннадиевич Былевский
Кандидат философских наук, доцент кафедры информационной культуры цифровой трансформации, доцент кафедры международной информационной безопасности, Московский государственный лингвистический университет. 119034, г. Москва, ул. Остоженка, дом 38 стр.1
pr-911@yandex.ru, https://orcid.org/0000-0002-0453-526X

Аннотация. В статье исследуется проблематика формирования массовой общегражданской культуры информационной безопасности россиян на основе «конверсии» исторически унаследованной совокупности профессиональных знаний, умений и навыков использования компьютерно-телекоммуникационных технологий для государственных нужд. Достижению поставленной цели может способствовать профильное научное осмысление − применение культурологической парадигмы: ценностного подхода, эволюционного и структурно-функционального методов в исследовании особенностей и динамики становления информационной безопасности в России.

В ходе представляемого исследования классифицированы направления обеспечения безопасности согласно видам защищаемых ценностей (в том числе социально-культурных традиций и идентичности), выделены особенности, связанные с компьютерно-телекоммуникационными технологиями и цифровой трансформацией. Культура информационной безопасности подразделена на профессиональную, специализированную (в том числе в области компьютерно-телекоммуникационных технологий) и общегражданскую, массовую.

Важным результатом исследования являются выводы о непродуктивности трансляции шаблонов профессиональной подготовки и недостаточности простой популяризации для формирования и развития массовой общегражданской культуры информационной безопасности. Напротив, предлагается принцип «конверсии», означающий, что формирование каждого из видов культуры информационной безопасности своеобразно, характеризуется различными сочетаниями технических и социокультурных, базовых и вспомогательных факторов, сроков, этапов и возможных методик. Культурологическая парадигма информационной безопасности может применяться для дальнейшей научной, образовательной и практической профильной деятельности, служить методологическим инструментом реализации Концепции формирования и развития культуры информационной безопасности граждан, утверждённой Правительством России 22 декабря 2022 г.

Ключевые слова: культурологическая парадигма; конверсия; методологический инструмент; информационная безопасность; массовая общегражданская культура; «всеобуч»; компьютерно-телекоммуникационные технологии; цифровизация

Для цитирования: Былевский П. Г. Культурологические аспекты формирования информационной безопасности граждан // Ярославский педагогический вестник. 2023. № 6 (135). С. 232-239. http://dx.doi.org/10.20323/1813-145X_2023_6_135_232. https://elibrary.ru/XANZER

CULTURE CONFORMABLE PRACTICES

Original article

Cultural aspects in forming the culture of citizens' information security

Pavel G. Bylevsky
Candidate of philosophical sciences, associate professor of department of information culture of digital transformation, associate professor of department of international information security, Moscow state linguistic university. 119034, Moscow, Ostozhenka st., 38, building 1
pr-911@yandex.ru, https://orcid.org/0000-0002-0453-526X

Abstract. The article examines the problems of the formation of a mass civil culture of information security of Russians based on the «conversion» of a historically inherited set of professional knowledge, skills of professional use of computer and telecommunication technologies for state needs. Achieving this goal can be facilitated by a specialized scientific understanding − the development of a cultural paradigm: the application of a value approach, evolutionary and structural-functional methods in the study of the features and dynamics in the formation of information security in Russia.

In the course of the presented research, the directions of ensuring security are classified according to the types of protected values (including socio-cultural traditions and identity), the features associated with computer and telecommunication technologies and digital transformation as their universal application are highlighted. The culture of information security is divided into professional, specialized (including in the field of computer and telecommunication technologies) and general civil, mass.

An important result of the study is the conclusions about the unproductivity of the translation of templates of professional training tools and the insufficiency of simple popularization for the formation and development of a mass general civil culture of information security. On the contrary, the principle of «conversion» is proposed, meaning that the formation of each type of information security culture is peculiar, characterized by various combinations of technical and socio-cultural, basic and auxiliary factors, deadlines, stages and possible methods. The cultural paradigm of information security can be used for further scientific, educational and practical profile activities, serve as a methodological tool for implementing the Concept of formation and development of citizens' information security culture approved by the Government of Russia on December 22, 2022.

Key words: cultural paradigm; information security; mass civil culture; «universal education»; computer and telecommunication technologies; digitalization

For citation: Bylevskiy P. G. Cultural aspects in forming the culture of citizens' information security. *Yaroslavl pedagogical bulletin. 2023; (6):* 232-239. (In Russ.). http://dx.doi.org/10.20323/1813-145X_2023_6_135_232. https://elibrary.ru/XANZER

Введение

Проявившийся в последние годы новый комплекс проблем безопасности использования компьютерно-телекоммуникационных технологий, в том числе специфически гуманитарных, социально-культурных, усилил потребность в формировании и развитии профильной общегражданской культуры [Колин, 2022, с. 29–48], что и привело к принятию 22 декабря 2022 года Правительством России «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации». Выполнению поставленных задач может служить профильное научное и методологическое осмысление − применение культурологической парадигмы информационной безопасности, включающей технические и гуманитарные аспекты, профессиональное и общегражданское направления.

Решение этой проблемы, недооцениваемой ранее, требует разработки и реализации действенных мер, применения профильной научной и методологической основы [Покуль, 2023, с. 541–542]. Таковой может служить культурологическая парадигма информационной безопасности, системно и динамически представляющая социокультурные особенности, эволюцию и тенденции, структуру и функции деятельности по защите ценностей применительно к современному использованию компьютерно-телекоммуникационных технологий.

Культурологические аспекты защиты ценностей в обеспечении информационной безопасности.

Культурологическая парадигма открывает возможность отразить специфику, особенности общегражданской культуры информационной безопасности, её позиционирование по отноше-

нию к другим смежным видам (профессиональной, специализированной и др.). Культурологический подход способен служить методологическим инструментом более точного определения защищаемых ценностей, а также угроз и рисков, средств и выработки мер преодоления «цифровой беспечности», повышения культуры информационной безопасности применительно к особенностям использования компьютерно-телекоммуникационных технологий в различных сферах, включая массовую, общегражданскую (учитывающую современные особенности массового сознания) [Злотникова, 2020, с. 46–56].

Культурологические аспекты информационной безопасности включают несколько направлений:

− определение защищаемых ценностей, «активов» разного рода: имущества, оборудования, программного обеспечения и данных, компьютерных систем и т.п.);

− защиту собственно социально-культурных ценностей общества и личности,

− массовую и профессиональную, специализированную культуру деятельности обеспечения безопасности, в том числе жизнедеятельности и технической, включая компьютерную.

Культурологическая «аксиология безопасности» (и информационной безопасности) определяет ценности всех видов, подлежащие защите от ущерба с архаических «первобытных» эпох. В ходе исторического развития из «общей безопасности» выделяется собственно социально-культурная безопасность − традиционных ценностей, идентичности и т.п. Далее можно выделить культуру (совокупности знаний, умений, навыков) обеспечения безопасности как всеобщей деятельности, в дальнейшем массовой и профессиональной (по мере расширения и углубления разделения труда, увеличения количества профессий, специализаций). Существует также специфическая техническая культура безопасности − самой техники и технических инструментов обеспечения других видов безопасности. Это направление включает безопасность компьютеров, телекоммуникаций и машинной автоматизации, включая их универсально широкое и повсеместное применение в современной «цифровизации» [Alraja, 2023].

Исторически, эволюционно современная культура информационной безопасности является продолжением и синтетически воплощает несколько предшествующих направлений деятельности, включающих социально-культурные. С точки зрения культурологии главными понятиями безопасности можно признать:

− ценности как объекты защиты;

− потенциальный ущерб: угрозы и риски его осуществления;

− людей, коллективы и институты как объекты и субъекты защиты;

− средства и меры обеспечения безопасности (нормативные, организационные, технические и социокультурные).

− деятельность (процессы) обеспечения безопасности.

Культура обеспечения безопасности (знания, умения и навыки), или защита от возможного ущерба ценностей (природы, имущества, людей, знаний), в минимальном объёме является изначальным неотъемлемым условием существования общества и личности [Голушко, 2022, с. 1483–1495]. Увеличение многообразия и оформление самостоятельных отраслей сопровождается спецификацией безопасности на государственную, общественную, политическую, идеологическую, военную, социальную, культурную, экономическую, финансовую, личной жизни [Liu, 2022] и другие области. По мере развития производительных сил и общественных отношений, разделения труда обеспечение безопасности выделяется в отдельный вид и сферу деятельности, позже в профессии, целые отрасли, межотраслевые спецификации и институты [Закс, 2022, с. 186–195].

Исторически возможны самые разные сочетания сфер, видов деятельности, особенностей культуры обеспечения безопасности. Например, продовольственная безопасность, по-видимому, являлась всеобщей человеческой способностью, а военная − в зависимости от конкретно-исторических особенностей общества могла быть делом всего взрослого населения, «вооружённого народа», но также и немногочисленной профессиональной армии, «преторианской гвардии».

Формирование структурно-функциональных элементов культуры информационной безопасности.

История обеспечения безопасности, рассматриваемая как социально-культурная деятельность, включает такие различные задачи, как защита господствующей идеологии, территориальной целостности и богатств, граждан и социальных общностей, власти и её представителей, предметов культуры, документов и денежных средств. Эволюционную предысторию совре-

менной информационной безопасности представляют несколько направлений деятельности, связанных с защитой ценностей, в том числе собственно социально-культурных (идентичности и др.). Для любого из направлений этой деятельности может быть рассмотрен культурный аспект, на определённом этапе развития достигающий уровня профессиональной культуры.

В политической сфере защищаются такие ценности как власть, государство, право, общественный строй, территория, народонаселение. Экономической защите подлежат продовольственные, энергетические и сырьевые ресурсы, производство, торговля, финансы. В социально-культурной сфере защищаются религия, наука, искусство, мораль и нравственность, обычаи, социальные потребности. Защите в первую очередь подлежит главная ценность – люди и коллективы, организации − носители того или иного вида ценностей. Затем − природные и произведённые человеком средства производства и потребления, в том числе предметы техники и культуры (объекты, документы и др.).

Угрозами ценностям являются природные и общественные катаклизмы, а также деятельность нарушителей, включая злоумышленников, − людей, коллективов, организаций. Для нарушения безопасности защищаемых объектов могут быть использованы технические (инструменты, орудия и материалы), а также социально-культурные средства − нормативные, организационные, знания, умения, навыки и т. д. Рисками нарушения безопасности ценностей выступают различные виды и степени возможного ущерба, вплоть до утраты для прежних владельцев, полного уничтожения.

Эти «извечные» социально-культурные реалии (сочетание расширения перечня и значимости ценностей, сопряжённых угроз и рисков, средств и правил безопасности) проецируются на современное расширяющееся использование компьютерно-телекоммуникационных сетевых технологий практически во всех областях профессиональной [Jaeger, 2020] и бытовой жизнедеятельности. Информационная безопасность выступает защитой человеческих ценностей, в первую очередь, самих людей, а также природных и социально-культурных объектов, процессов и систем от угроз, сопряжённых с преимуществами компьютерно-телекоммуникационных сетевых решений, в том числе в универсальном формате «цифровизации», включая обоюдоострые возможности «виртуализации» [Хренов, 2023, с. 208–217].

Эволюционная динамическая сложность аксиологии защиты ценностей показывает, что для формирования массовой общегражданской, как и профессиональной, специализированной культуры информационной безопасности малоэффективно шаблонное, механическое применение организационных средств, методик и приёмов формирования подобных профессиональных компетенций [Жестовский, 2022, с. 100–107]. Также недостаточно простой популяризации, упрощения и иллюстрирования яркими примерами из повседневной жизни [Van Daalen, 2022]. Чтобы выработать концепцию, комплекс средств и мер, методики и план формирования и повышения такой культуры, необходимо тщательно изучать специфику целевых социальных групп, актуальное состояние применения компьютерно-телекоммуникационных технологий, угроз и инцидентов, учитывать общие и локальные тенденции развития информационной безопасности.

Разработка эффективных мер повышения общегражданской культуры информационной безопасности требует предварительных ответов на ряд вопросов методологического характера, включая следующие:

− каковы структура и функции, основные характеристики и целевые показатели освоения общегражданской культуры информационной безопасности;

− в чём сходства и совпадения, а в чём отличия от других видов подобных профессиональных, специализированных знаний, умений и навыков [Ма, 2022];

− в какой степени применимы для «всеобуча» средства формирования и развития культуры общей безопасности жизни, техники безопасности, в частности использования компьютерного оборудования и телекоммуникаций.

Соотношение и взаимодействие профессиональной и общегражданской культуры информационной безопасности.

Ответы на поставленные вопросы имеют не только теоретическое, но и практическое, прикладное значение: определение того, что для общегражданской аудитории можно напрямую транслировать из профессиональной подготовки специалистов по информационной безопасности, а что нуждается в популяризации, значительной доработке и создании новых обучающих средств. Лучше понять структуру, функции и особенности массовой культуры информационной безопасности помогает анализ сравнительно недавней (1990–2010-е гг.) эволюции создания и при-

менения компьютерно-телекоммуникационных решений, а также сопряженных угроз, рисков и, соответственно, обеспечения безопасности.

Следует учитывать, что основы профессиональной культуры информационной безопасности закладываются при обучении в организациях среднего общего, специального и высшего образования [Казинец, 2022, с. 22–25], а общегражданская культура формируется другими институтами различного профиля (прессой, социальной рекламой, корпоративными правилами обслуживания [Ефимова, 2021] и т. п.). Существует несколько разрозненных направлений обучения, формирования различных видов культуры информационной безопасности. Как для научного осмысления, так для разработки эффективных образовательных методик необходимо изучение тенденций развития этих направлений, выявление закономерностей сближения и взаимодействия.

Наблюдаются различные до противоположности пути формирования культуры информационной безопасности, с одной стороны, общегражданской, с другой стороны, профессиональной, особенно у технических специалистов, тем более в компьютерно-телекоммуникационных технологиях. Профессиональная культура информационной безопасности, в том числе специализированная, формируется при получении среднего специального и высшего образования, в ходе профессиональной деятельности, повышения квалификации. Для профессионалов обеспечения безопасности в различных отраслях существуют те или иные сочетания гуманитарных и технических аспектов [Былевский, 2022, с. 40–45].

Безопасность промышленных и других объектов (в том числе пожарная, радиационная, биологическая и др.), кроме технических требований к оборудованию, помещениям и территориям, обязательно включает технику безопасности, соответствующее обучение сотрудников и контроль соблюдения [Карпов, 2021, с. 68–75]. В государственной безопасности важнейшими являются политический фактор и секретность. В военной сфере сопоставима важность, с одной стороны идеологических, психологических вопросов, с другой стороны − материально-технического оснащения и снабжения, включая компьютерное и компьютеризованное оборудование и средства связи. Для профессионалов, базовой специальностью которых являются компьютерно-телекоммуникационные технологии, первостепенными угрозами выступают атаки нарушителей-«хакеров» с помощью технических средств (вредоносного программного обеспечения, «вирусов»), приводящие к поломкам оборудования, хищениям и порче программного обеспечения и данных [Khando, 2021]. Осознание гуманитарных угроз типа мошенничества совершается в формате «технически» звучащих терминов вроде «социальной инженерии».

Основы общегражданской культуры информационной безопасности закладываются школьными и вузовскими учебными дисциплинами [Алисов, 2021, с. 137–143], базово − информатикой и основами безопасности жизнедеятельности [Магомедов, 2021, с. 58–64], а у массовой взрослой аудитории − прессой, социальной рекламой и повседневным общением, в том числе в социальных сетях, специальным обучением. Правила безопасного использования служат не только элементом пользовательской культуры, умения работать с компьютерными устройствами в сетях, главным образом в интернете, но и «надстройкой» над базовыми, повседневными представлениями об угрозах, рисках и соблюдении безопасности (в отношении мошенничеств, краж, шантажа и др. угроз [Былевский, 2023, с. 46–56]).

«Гуманитарные» угрозы, связанные с компьютерно-телекоммуникационными технологиями, пополняются синхронным анализом больших пользовательских данных − слежкой в режиме реального времени, моделированием «цифровых двойников» окружающего мира [Хренов, 2022, с. 201–210], граждан и социальных групп, автоматизированной дезинформацией, организацией «псевдособытий» [Шапинская, 2021, с. 162–169], манипулированием сознанием, вовлечением в деструктивные сообщества, в экстремистскую, антигосударственную и антиобщественную деятельность. Для обеспечения информационной безопасности сотрудникам технических профилей приходится осваивать социально-культурные аспекты посредством смежных гуманитарных дисциплин: культурологии, а также социологии, психологии, массовых коммуникаций и др., привлекать к совместной работе специалистов из этих областей.

Заключение

Формирование и развитие культуры информационной безопасности граждан («всеобуч») − новое актуальное направление государственной политики России, требующее профильного научного осмысления в культурологии. Под такой

культурой следует понимать совокупность сформированных знаний, умений и навыков безопасного использования компьютерно-телекоммуникационных технологий, высшей универсальной стадией развития и применения которых является современная цифровая трансформация.

«Конверсия» компьютерно-телекоммуникационных технологий и обеспечения их безопасности из военных и других закрытых сфер в массовые сервисы − не односторонний процесс «трансляции». Необходимым сопутствующим встречным процессом является формирование массовой общегражданской культуры информационной безопасности с её специфическими функциями, структурой и особенностями. Использование подходов культурологии (включая ценностный подход) для классификации защищаемых ценностей, эволюционного и структурно-функционального методов, анализа актуальных угроз и практики противодействия инцидентам позволяет специфицировать средства формирования и развития культуры информационной безопасности применительно к социально-культурным особенностям профессий, специализаций, коллективов и индивидов.

Библиографический список

1. Алисов Е. А. Развитие представлений младших школьников об информационной безопасности в процессе формирования информационной культуры / Е. А. Алисов, Д. Ю. Калинченко // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2021. Т. 26. № 191. С. 137–143.

2. Былевский П. Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56.

3. Былевский П. Г. Некоторые особенности интеграции инновационных технологий и методик в высшее гуманитарное образование // Инновационные технологии обучения в вузах : сборник статей национальной научно-практической конференции [27–28 апреля 2022 года]. Сочи; Москва : Московский инновационный университет, 2022. С. 40–45.

4. 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.

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

6. Жестовский А. Г. Культура информационной безопасности морского специалиста и условия ее формирования / А. Г. Жестовский, Д. Я. Околот, И. Д. Рудинский // Педагогика. Вопросы теории и практики. 2022. Т. 7. № 1. С. 100–107.

7. Закс Л. А. Институты как социокультурный феномен / Л. А. Закс, Н. А. Стрижкова // Ярославский педагогический вестник. 2022. № 4 (127). С. 186–195.

8. Злотникова Т. С. Массовое сознание в философской традиции и в современных интерпретациях / Т. С. Злотникова // Вопросы философии. 2020. № 10. С. 46–56.

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

10. Карпов В. В. Педагогические особенности формирования культуры безопасности в процессе подготовки бакалавров техносферной безопасности // Ученые записки Забайкальского государственного университета. 2021. Т. 16. № 1. С. 68–75.

11. Колин К. К. О проблеме формирования системы информационного образования в России в условиях цифровой трансформации общества // Знание. Понимание. Умение. 2022. № 2. С. 29–48.

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

13. Покуль А. А. Культура информационной безопасности граждан Российской Федерации в условиях цифровизации экономики // Евразийский юридический журнал. 2023. № 6(181). С. 541–542.

14. Хренов Н. А. История медиа как история становления виртуальной реальности: знак в процессах коммуникации и инструмент отчуждения // Ярославский педагогический вестник. 2023. № 1 (130). С. 208–217.

15. Хренов Н. А. Человечество в ситуации очередной в истории медиа «мировой революции» // Ярославский педагогический вестник. 2022. № 5 (128). С. 201–210.

16. Шапинская Е. Н. Впечатления на продажу: современные тенденции в культуре потребления // Ярославский педагогический вестник. 2021. № 1 (118). С. 162–169.

17. Alraja M., Butt U., Abbod M. Information security policies compliance in a global setting: An employee's perspective // Computers & Security. June 2023. Vol. 129. DOI: 10.1016/j.cose.2023.103208.

18. Jaeger L., Eckhardt A., Kroenung J. The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis // Information & Management. May 2020. Vol. 58. Iss. 3. DOI: 10.1016/j.im.2020.103318.

19. Khando Kh., Gao Sh., Islam S., Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review // Computers & Security. July 2021. Volume 106. DOI: 10.1016/j.cose.2021.102267.

20. Liu X. Research on consumers' personal information security and perception based on digital twins and Internet of Things // Sustainable Energy Technologies and Assessments. October 2022. Vol. 53, Part C. DOI: 10.1016/j.seta.2022.102706.

21. Ma X. IS professionals' information security behaviors in Chinese IT organizations for information security protection // Information Processing & Management. January 2022. Vol. 59. Iss. 1. DOI: 10.1016/j.ipm.2021.102744.

22. Van Daalen O. In defense of offense: information security research under the right to science // Computer Law & Security Review. September 2022. Vol. 46. DOI: 10.1016/j.clsr.2022.105706.

Reference list

1. Alisov E. A. Razvitie predstavlenij mladshih shkol'nikov ob informacionnoj bezopasnosti v processe formirovanija informacionnoj kul'tury = Development of ideas of younger students about information security in the process of forming information culture / E. A. Alisov, D. Ju. Kalinchenko // Vestnik Tambovskogo universiteta. Serija: Gumanitarnye nauki. 2021. T. 26. № 191. S. 137–143.

2. Bylevskij P. G. Kul'turologicheskaja dekonstrukcija social'no-kul'turnyh ugroz ChatGPT informacionnoj bezopasnosti rossijskih grazhdan = Cultural deconstruction of social and cultural threats in ChatGPT information security of Russian citizens // Filosofija i kul'tura. 2023. № 8. S. 46–56.

3. Bylevskij P. G. Nekotorye osobennosti integracii innovacionnyh tehnologij i metodik v vysshee gumanitarnoe obrazovanie = Some features of integrating innovative technologies and techniques into higher humanitarian education // Innovacionnye tehnologii obuchenija v vuzah : sbornik statej nacional'noj nauchno-prakticheskoj konferencii [27–28 aprelja 2022 goda]. Sochi; Moskva : Moskovskij innovacionnyj universitet, 2022. S. 40–45.

4. Golushko T. K. Informacionnyj immunitet kak kljuchevoe ponjatie informacionno-psihologicheskoj bezopasnosti lichnosti = Information immunity as a key concept of information and psychological security of the individual // Vestnik Tambovskogo universiteta. Serija: Gumanitarnye nauki. 2022. T. 27. № 6. S. 1483–1495.

5. Efimova O. V. Razvitie kul'tury bezopasnosti v integracii s cifrovoj kul'turoj = Developing safety culture in integration with digital culture / O. V. Efimova, Ju. V. Komarova // Avtomatika, svjaz', informatika. 2021. № 3. S. 14–16.

6. Zhestovskij A. G. Kul'tura informacionnoj bezopasnosti morskogo specialista i uslovija ee formirovanija = Marine specialist's information security culture and conditions for its formation / A. G. Zhestovskij, D. Ja. Okolot, I. D. Rudinskij // Pedagogika. Voprosy teorii i praktiki. 2022. T. 7. № 1. S. 100–107.

7. Zaks L. A. Instituty kak sociokul'turnyj fenomen = Institutions as a sociocultural phenomenon / L. A. Zaks, N. A. Strizhkova // Jaroslavskij pedagogicheskij vestnik. 2022. № 4 (127). S. 186–195.

8. Zlotnikova T. S. Massovoe soznanie v filosofskoj tradicii i v sovremennyh interpretacijah = Mass consciousness in the philosophical tradition and in modern interpretations / T. S. Zlotnikova // Voprosy filosofii. 2020. № 10. S. 46–56.

9. Kazinec V. A. Informacionnaja bezopasnost' kak chast' cifrovoj kul'tury vypusknikov pedagogicheskih universitetov = Information security as part of the digital culture of teachers' university graduates / V. A. Kazinec, E. A. Red'ko // Sovremennoe pedagogicheskoe obrazovanie. 2022. № 5. S. 22–25.

10. Karpov V. V. Pedagogicheskie osobennosti formirovanija kul'tury bezopasnosti v processe podgotovki bakalavrov tehnosfernoj bezopasnosti = Pedagogical features of safety culture formation in the process of technosphere safety training of bachelors // Uchenye zapiski Zabajkal'skogo gosudarstvennogo universiteta. 2021. T. 16. № 1. S. 68–75.

11. Kolin K. K. O probleme formirovanija sistemy informacionnogo obrazovanija v Rossii v uslovijah cifrovoj transformacii obshhestva = On the problem of forming an information education system in Russia in the context of digital transformation of society // Znanie. Ponimanie. Umenie. 2022. № 2. S. 29–48.

12. Magomedov R. V. Formirovanie kul'tury bezopasnosti zhiznedejatel'nosti uchashhihsja v uslovijah cifrovoj transformacii obrazovanija = Building a culture of student safety in the context of digital transformation of education / R. V. Magomedov, I. S. Minbulatova // Izvestija Dagestanskogo gosudarstvennogo pedagogicheskogo universiteta. Psihologo-pedagogicheskie nauki. 2021. T. 15. № 2. S. 58–64.

13. Pokul' A. A. Kul'tura informacionnoj bezopasnosti grazhdan Rossijskoj Federacii v uslovijah cifrovizacii jekonomiki = Culture of information security of citizens of the Russian Federation in the context of economy digitalization // Evrazijskij juridicheskij zhurnal. 2023. № 6(181). S. 541–542.

14. Hrenov N. A. Istorija media kak istorija stanovlenija virtual'noj real'nosti: znak v processah kommunikacii i instrument otchuzhdenija = Media history as the story of the formation of virtual reality: a sign in communication processes and a tool for alienating // Jaroslavskij pedagogicheskij vestnik. 2023. № 1 (130). S. 208–217.

15. Hrenov N. A. Chelovechestvo v situacii ocherednoj v istorii media «mirovoj revoljucii» = Humanity in the situation of the next «world revolution» in the history of media // Jaroslavskij pedagogicheskij vestnik. 2022. № 5 (128). S. 201–210.

16. Shapinskaja E. N. Vpechatlenija na prodazhu: sovremennye tendencii v kul'ture potreblenija = Selling

experiences: current trends in consumption culture // Jaroslavskij pedagogicheskij vestnik. 2021. № 1 (118). S. 162–169.

17. Alraja M., Butt U., Abbod M. Information security policies compliance in a global setting: An employee's perspective // Computers & Security. June 2023. Vol. 129. DOI: 10.1016/j.cose.2023.103208.

18. Jaeger L., Eckhardt A., Kroenung J. The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis // Information & Management. May 2020. Vol. 58. Iss. 3. DOI: 10.1016/j.im.2020.103318.

19. Khando Kh., Gao Sh., Islam S., Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review // Computers & Security. July 2021. Volume 106. DOI: 10.1016/j.cose.2021.102267.

20. Liu X. Research on consumers' personal information security and perception based on digital twins and Internet of Things // Sustainable Energy Technologies and Assessments. October 2022. Vol. 53, Part C. DOI: 10.1016/j.seta.2022.102706.

21. Ma X. IS professionals' information security behaviors in Chinese IT organizations for information security protection // Information Processing & Management. January 2022. Vol. 59. Iss. 1. DOI: 10.1016/j.ipm.2021.102744.

22. Van Daalen O. In defense of offense: information security research under the right to science // Computer Law & Security Review. September 2022. Vol. 46. DOI: 10.1016/j.clsr.2022.105706.

Статья поступила в редакцию 20.09.2023; одобрена после рецензирования 26.10.2023; принята к публикации 22.11.2023.
The article was submitted 20.09.2023; approved after reviewing 26.10.2023; accepted for publication 22.11.2023.