Научная статья
УДК 008,130:2,004.56
DOI: 10.20323/2499_9679_2024_1_36_238
EDN: EUJLFO

Структурное становление культуры информационной безопасности российских 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, д. 38, стр.1
pr-911@yandex.ru, https://orcid.org/0000-0002-0453-526X

Аннотация. Статья исследует закономерности структурного становления культуры информационной безопасности российских граждан теоретико-культурными и культурологическими методами. Материалами послужили научные статьи по указанной проблематике, опубликованные в 2021-2023 годах в журналах перечня ВАК (категории К1, К2) и индексируемые в международной научной базе Scopus (категории Q1, Q2). Установлено, что основой эволюции функциональной структуры культуры информационной безопасности служит развитие компьютерно-сетевых технологий (интернет-коммуникаций), их распространение на все гражданские отрасли вплоть до непрерывного общегражданского бытового использования. Определена периодизация (с 1960-х годов до современности) структурного развития, появления, изменения соотношения и способов взаимодействия различных видов (профессиональной и специализированной, общегражданской и различных социальных групп граждан) культуры информационной безопасности.

Проведенный анализ показал первоначальное формирование культуры информационной безопасности как узкопрофессиональной в области защиты государственной, военной тайны, с преобладанием организационно-технической проблематики. Выявлено, что дальнейшее распространение компьютерно-сетевых технологий на практически все профессии, превращение большинства граждан в постоянных пользователей интернета привело к значительным структурным изменениям культуры информационной безопасности.

Результатом исследования является вывод, что современная общегражданская культура информационной безопасности необходимо включает многочисленные и разнообразные социально-культурные аспекты, в том числе защиту традиционных ценностей и культурной идентичности личности. Эти аспекты интегрируются в профессиональную подготовку специалистов по информационной безопасности, так же как и профильные организационно-технические, правовые вопросы – в формирование, развитие и повышение соответствующей массовой культуры. Полученные результаты могут быть использованы в реализации «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации», утверждённой распоряжением Правительства Российской Федерации № 4088-р от 22 декабря 2022 г.

Ключевые слова: культурологическая парадигма; информационная безопасность; массовая общегражданская культура; профессиональная культура; компьютерно-телекоммуникационные технологии; цифровизация; традиционные ценности; культурная идентичность

Для цитирования: Былевский П. Г. Структурное становление культуры информационной безопасности российских граждан // Верхневолжский филологический вестник. 2024. № 1 (36). С. 238–245. http://dx.doi.org/10.20323/2499_9679_2024_1_36_238. https://elibrary.ru/EUJLFO

Original article

Structural formation of russian citizens' information security culture

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

Abstract. The article investigates the structural formation patterns of russian citizen's information security culture using theoretical-cultural and culturological methods. The materials for the study include scientific articles on the

relevant problems published in 2021–2023 in the journals listed in the Higher Attestation Commission (categories K1, K2) and indexed in the international scientific database Scopus (categories Q1, Q2). It is established that the development of computer-network technologies (Internet communications) and their spread to all spheres of society including continuous everyday use by the general public is the basis for functional structure of information security culture to evolve. The author defines the periods (from the 1960s to the present) of structural development, appearance, changes in the ratio and ways of interaction between various types of information security culture (professional and specialized, general civic and different social groups). The analysis has shown the initial formation of an information security culture as highly professional in the field of protecting state and military secrets, with prevailing organizational and technical issues. It has been revealed that the further spread of computer-network technologies to almost all professional spheres, and the majority of citizens turning into regular Internet users led to significant structural changes in the information security culture.

As a result, the author concludes that the modern civic information security culture necessarily embraces numerous and diverse socio-cultural aspects, including the protection of traditional values and a person's cultural identity. These aspects are integrated into information security specialists' professional training, as well as specialized organizational, technical, and legal issues are an integral part of forming, developing, and enhancing the corresponding mass culture. The obtained results can be used for implementing the «Concept of forming and developing the information security culture of the Russian Federation citizens», the order of the Russian Federation Government No. 4088-r of December 22, 2022.

Key words: cultural paradigm; information security; mass civil culture; professional culture; computer and telecommunication technologies; digitalization; traditional values; cultural identity

For citation: Bylevsky P. G. Structural formation of russian citizens' information security culture. *Verhnevolzhski philological bulletin. 2024;(1):238–245. (In Russ.).* http://dx.doi.org/10.20323/2499_9679_2024_1_36_238. https://elibrary.ru/EUJLFO

Введение

Исследование структуры культуры информационной безопасности является актуальным научным и практическим вопросом, напрямую связанным с решением задач улучшения защиты граждан, общества и государства от современных угроз, связанных с использованием компьютерных технологий и интернет-коммуникаций. Анализ истории становления информационной безопасности помогает лучше понять особенности её отдельных видов (профессиональной, массовой и др.), их взаимодействия, текущую динамику и перспективы изменений.

Появление в российских государственных документах трактовки обеспечения информационной безопасности именно как культуры является особенностью современного этапа развития общества, социально-культурных процессов и компьютерно-телекоммуникационных технологий. Выполнение задач, поставленных «Концепцией формирования и развития культуры информационной безопасности граждан Российской Федерации», утверждённых распоряжением Правительства Российской Федерации № 4088-р от 22 декабря 2022 г., требует профильного научного подхода в рамках теории культуры и культурологии, прежде системно в этой области не применявшегося.

1. Методы и материалы исследования становления культуры информационной безопасности

Для исследования становления структуры культуры информационной безопасности применяются теоретико-культурный, а также культурологические эволюционный и структурно-функциональные подходы. Материалом исследования служат не только организационно-технические аспекты современной структуры культуры информационной безопасности, но социально-культурные факторы, ставшие, в сравнении с предшествующим периодом 1990–2010 гг., не менее значимыми, и «удельный вес» и значение их всё более возрастают [Uchendu и др., 2021].

Теоретико-культурный подход позволяет рассмотреть социально-культурные факторы как соответствующих профессиональных специализаций, так и формирования и развития безопасного использования компьютерно-телекоммуникационных технологий и интернет-сервисов российскими гражданами в бытовой, досуговой деятельности [Gao, 2023]. Культурологический анализ эволюции развития и применения компьютерно-телекоммуникационных технологий и интернет-сервисов, сопряжённых угроз и средств безопасности позволяет подробнее и точнее определить особенности современной системы профессиональной и общегражданн-

ской культуры информационной безопасности, специфику различных профессий и социальных групп. Эволюционный, исторический анализ помогает лучше понять современные тенденции, точнее определить структурные особенности развития культуры информационной безопасности профессиональной и общегражданской, применительно к особенностям различных профессий и социальных групп граждан [Былевский, 2023, с. 157–167].

Средства и меры, методики формирования и развития структуры культуры информационной безопасности для конкретной области определяются оценкой ряда существенных технических и социально-культурных характеристик:

− отрасли, сферы, направлений применения;

− назначений и состояния компьютерно-телекоммуникационных технологий;

− субъектов − взаимодействующих организаций, социальных групп и личностей;

− защищаемых ценностей, существующих угроз и рисков;

− динамикой предшествующей эволюции, тенденциями и прогнозами.

Выработка программ развития формирования и развития культуры массовой общегражданской информационной безопасности должна учитывать структурное разнообразие проблематики защиты ценностей, формировавшееся и проявлявшееся в исторической эволюции [Shiau, 2023]. История этого становления представляет много разнообразных примеров различных систем определения, ранжирования и иерархий ценностей, и, соответственно, угроз и рисков. Особое внимание должно уделяться роли технических средств, от простых орудий труда до автоматизированных систем машин, включая компьютерно-телекоммуникационные технологии, и современный этап «цифровизации» − их универсального применения.

Становление современной структуры информационной безопасности в России началось с массового гражданского использования электронно-вычислительной техники, в особенности персональных компьютеров в 1990-е годы. Так же, как и за рубежом, в США и странах Западной Европы, этот процесс носил характер «конверсии»: компьютерные технологии и оборудование, созданные в государственном секторе в первую очередь для военных нужд, начали адаптироваться для гражданских отраслей, для корпоративного и личного, в том числе коммерческого использования [Анзина, 2023, с. 14–21]. Информационная безопасность начинала формироваться как «компьютерная», а деятельность, направленная на её обеспечение, как доступное немногим «тайное знание», тесно связанное с защитой государственной (в том числе военной), а за рубежом также и коммерческой тайны.

Профессиональная специализация и эволюция защиты ценностей (включая технические средства связи, документооборота, самих пользователей) исторически начинается в критически важных областях: в политике (государственном управлении) и идеологии, в международных отношениях (дипломатии), военном деле и торговой, финансовой деятельности. Так же разработка и производство компьютерно-телекоммуникационных технологий − электронно-вычислительных машин (ЭВМ) и радиоэлектроники − осуществлялись государственными структурами для собственных важнейших нужд, поскольку требовало концентрации значительных ресурсов. В первую очередь для военных целей: сначала для шифрования секретной связи и переписки, а затем автоматизации расчётов и управления противовоздушной обороной, бомбардировками, артиллерийскими и ракетными (также с атомными боеголовками) обстрелами противника. Распространение прежде секретных военных компьютерно-телекоммуникационных технологий на гражданскую сферу значительно меняло структуру, характер и перечень защищаемых ценностей, угроз и рисков, требовало адаптации, своеобразной «конверсии» также и правил безопасности [Yin, 2023].

2. Динамика усложнения структуры культуры информационной безопасности

Усложнение структуры культуры информационной безопасности было обусловлено вначале преимущественно организационно-технологическими, но затем всё более социально-культурными факторами, чей удельный вес и значение далее нарастали. К организационно-технологическим факторам следует отнести универсальное и повсеместное развитие и распространение компьютерно-телекоммуникационных технологий, обозначаемое понятием «цифровой трансформации» всех отраслей, профессии и повседневного быта, досуга практически всех граждан.

К социально-культурным факторам реструктуризации культуры информационной безопасности относится вовлечение в обработку посредством сетевых компьютерных технологий, интернет-коммуникаций возрастающего количества и разнообразия всё более значимых ценностей

[Крестиненко, 2023, с. 221–228]. Причём ценностей уже не только и не столько вещных (оборудования, программного обеспечения, данных, электронных денежных средств и т. п.), но и нравственных, моральных, художественных и т.п., а также самой продолжительности пользовательской активности граждан. Существенно, до нескольких часов в сутки, возросло время пользовательской активности граждан в интернете, всё более приобретавшей черты небезопасного поведения [Alsharida, 2023] и одной из первостепенных потребностей, вплоть до деструктивной зависимости.

«Конверсия» компьютерных технологий в гражданскую сферу совершалась на первых порах преимущественно стихийно, при минимальной роли и государства, и тогда ещё аморфного гражданского общества. Персональные компьютеры использовали вне связи со сколько-нибудь значительными ценностями и без возможностей доступа к массовой публичной сети типа Интернета, потенциальный ущерб и риски были минимальны. Поэтому правила безопасности были мало актуальными, сводясь поначалу к немногочисленным универсальным несложным правилам для всех и каждого на все случаи жизни [Vedadi, 2021].

Первый период рассматриваемой эволюционной динамики структурного усложнения культуры информационной безопасности в гражданских отраслях связан с распространением компьютерного оборудования относится к 1960−1980-х годам. В структурном плане это была профессиональная культура обеспечения безопасности корпоративных централизованных вычислительных центров [Ebert, 2023] для индустриального применения в делопроизводстве, документообороте, учёте, планировании и контроле деловых процессов.

Второй период начинается в середине 1980-х и связан с созданием и началом массового использования настольных персональных компьютеров, как в профессиональной деятельности, так и в быту. Формировалась основа такого нового структурного направления как культура безопасности непрофессиональных пользователей, в перспективе разросшегося до массовых, общегражданских масштабов.

Третий период ведёт отсчёт с середины 1990-х, по мере конверсии сетевых технологий оборонным ведомством США и выстраивания единой сети Интернет, ставшей международной, а затем и глобальной. Локальные и глобальные сетевые решения позволили сочетать возможности объединения в сети настольных персональных компьютеров и централизованных индустриальных центров обработки данных, суперкомпьютеров. Новые перспективы вызвали взрывной рост объёмов, повышение разнообразия и усложнение структуры спроса на новые применения компьютерно-телекоммуникационных технологий. Растущий и всё более разносторонний спрос стимулировал разработки и массовое производство различных типов компьютеров и компьютеризованных устройств, комплексных системных сетевых решений. Увеличивается структурное разнообразие различных видов использования компьютерного оборудования, профессиональных особенностей сопутствующей культуры безопасности.

Четвёртый период гражданского применения компьютерно-телекоммуникационных решений − развернувшаяся в 2010-е годы «цифровизация», которая характеризуется широким распространением беспроводных «широкополосных» сетей, созданием и массовым производством непрерывно работающих в них в режиме 24x7 автономных аккумуляторных мобильных компьютерных устройств. Среди таких сетевых мобильных устройств − «интернет вещей» [Hughes-Lartey, 2021]: промышленные роботизированные модули и бытовые персональные компьютеры (планшеты и смартфоны), компьютеризованные специализированные устройства («гаджеты») и бытовая автоматизированная техника [Ameen, 2021]. Новые возможности комплексной автоматизации промышленной и бытовой техники, сбора и анализа статистики, включая пользовательскую [Venkatachalam, Mishra, 2021], породили социально-культурную проблематику и новые риски технологий «искусственного интеллекта» [Мусаева, 2022, с. 166–173].

Этот этап, характеризующийся массовым распространением технологий автоматизированного анализа больших данных и «искусственного интеллекта», называют цифровой трансформацией. Многочасовое использование персональных компьютерных устройств, постоянно подключенных к интернет-коммуникациям, структурно распространилось не только на практически все профессии, но и стало неотъемлемым в повседневной жизни большинства граждан. Универсальные, общегражданские масштабы распространения «цифровой культуры» привели к изменению структуры угроз, и, соответственно, необходимости реструктуризации и развития культуры информационной безопасности уже как общегражданской. Возникает необходимость

создания массовой разветвлённой разносторонней системы обучения, формирования и развития культуры информационной безопасности для всех граждан [Shillair, 2022]. Такая система должна быть регулярно обновляемой и структурно включать разнообразные элементы от общего понимания не доверенного характера интернет-среды до специфических навыков лингвистической безопасности [Слышкин, 2022а, с. 64–69].

3. Результаты исследования: факторы повышения значения социально-культурных аспектов информационной безопасности

Условия распространения компьютерно-сетевых технологий на гражданские отрасли и в массовое бытовое использование в России имели, в сравнении с США и Европой, специфическую проблематику. Реставрация капитализма в России происходила в радикально-либеральной редакции, максимально снижавшей роль государства в нормативном и ином регулировании, контроле и надзоре в области безопасности гражданского применения компьютерно-сетевых технологий. Негативные черты российской «конверсии» информационной безопасности в гражданскую сферу по-разному проявились в разные периоды, потребовав значительных комплексных корректирующих усилий, в том числе со стороны государства [Дубень, 2023, с. 51–57].

Во-первых, защита коммерческой, финансовой, банковской тайны и активов от угроз, связанных с использованием компьютеров, телекоммуникаций и сетей, развивалась запоздало, поскольку их гражданское распространение шло одновременно со становлением рыночной экономики. Причина в том, что в СССР в 1950−1980-е годы индустриальное гражданское использование ЭВМ, вычислительных центров и сетей развивалось в сфере государственного управления, включая промышленные предприятия. Безопасность вычислений и передачи данных включала технические, организационные аспекты и государственную тайну, исключая защиту коммерческих секретов из-за отсутствия частной собственности на средства производства. Напротив, рыночная, капиталистическая экономика США и стран Западной Европы подразумевала защиту коммерческой и банковской, финансовой тайны.

Во-вторых, трансграничный характер интернета крайне затруднял противодействие нарушениям информационной безопасности и преступлениям, совершавшимся дистанционно из-за рубежа.

В-третьих, внедрение компьютерно-телекоммуникационных решений в России в 1990-е − 2000-е годы происходило в формате технологической «капитуляции», периферийного неоколониализма: отказа от собственных разработок в пользу приоритета импортной продукции. Тем самым наносился ущерб технологическому суверенитету, нарастала зависимость от импорта, в том числе средств информационной безопасности, переносившихся без учёта наших национальных особенностей. Усиливался внешний технологический и организационный контроль за государственной, общественной и частной компьютерно-телекоммуникационной инфраструктурой.

В России флагманом компьютерно-телекоммуникационных массовых сервисов в гражданской сфере, опережая развитие государственных электронных услуг, стали банки, попутно развивая информационную безопасность в силу высокой привлекательности для злоумышленников хищений денежных активов. Наиболее частыми, значительными по ущербу и высоко резонансными нарушениями информационной безопасности во второй половине 2000-х годов стали хищения денежных средств, совершавшиеся в системах дистанционного банковского обслуживания преимущественно техническими средствами (посредством вредоносного программного обеспечения и др.). Решить эту проблему удалось благодаря развитию нормативно-правовой базы, контрольно-надзорной деятельности, развитию взаимодействия банков друг с другом и государственными регуляторами, правоохранительными органами.

В начале 2010-х годов устранение организационно-технических «брешей» наряду с массовым распространением интернет- и мобильного банкинга привело к смещению главного вектора атак злоумышленников на денежные средства граждан и организаций. Технические инструменты хищений отошли на второй план как снизившие эффективность, уступив первенство «социальной инженерии», то есть мошенничествам (в том числе «телефонным») посредством компьютерно-телекоммуникационных устройств. Именно тогда главным средством противодействия «социальной инженерии» было признано повышение культуры информационной безопасности клиентов, осведомлённости их об актуальных приёмах злоумышленников и правилах безопас-

ного использования финансовых дистанционных сервисов.

В 2010-е годы, кроме «социальной инженерии» в финансовой сфере, активно изучаются другие гуманитарные угрозы, наиболее массово проявившиеся в социальных сетях [Малгаров, 2022. с. 349–352], а позже и в групповом общении в интернет-мессенджерах. Это, главным образом, угрозы вовлечения пользователей социальных сетей, в первую очередь детей и подростков [Осипенко, 2022, с. 158–163], в деструктивные сообщества (самоубийств, травли, «школьных расстрелов», потребления наркотиков, азартных игр, экстремального поведения, «нетрадиционных ценностей» [Слышкин, 2022b, с. 53–60] и т. п.). Для успешного противодействия были признаны необходимыми не только ограничительные меры государства и усилия общественности, но и формирование массовой культуры информационной безопасности у школьников и студентов [Нынюк, 2022, с. 81–83].

Заключение

С февраля 2022 года, с началом специальной военной операции на Украине, на смену международному сотрудничеству в противодействии киберпреступности пришёл «гибридный» кибертерроризм с участием государственных спецслужб недружественных стран. Усиление с их стороны антироссийских санкций, в том числе в области компьютерно-телекоммуникационных технологий, потребовало обретения полноценного технологического суверенитета [Кочетков, 2022, с. 31–45], независимости от импорта. В гуманитарной сфере издержки монополизма глобальных социальных платформ, базирующихся в США, проявились в небывалых прежде цензуре российской официальной прессы, антироссийских «фальшивых новостях» и дезинформации. В результате последовали встречные государственные ограничения их деятельности в РФ [Гурова, Малыгина, Слышкин, 2022, с. 30–36], установленные для обеспечения информационной безопасности общества и граждан.

Проведённое исследование обусловливает выводы как о распространении культуры информационной безопасности на всех граждан России, так и её качественном развитии: структурном усложнении, включая элементы противоборства, защиты традиционных ценностей общества и самозащиты культурной идентичности личности [Hengstler и др., 2023]. Возрастание удельного веса и роли социально-культурных факторов требует учёта в совершенствовании профессиональной деятельности специалистов по информационной безопасности, включая соответствующие изменения программ их обучения, подготовки. С другой стороны, специализированные предметы, курсы и специализации, связанные с информационной безопасностью, будут всё шире внедряться в систему образования граждан [Hassandoust, 2022] наряду с усилением профильной составляющей в повестке средств массовой информации и социальной рекламы. Полученные результаты могут быть использованы в реализации «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации», утверждённой распоряжением Правительства Российской Федерации № 4088-р от 22 декабря 2022 г.

Библиографический список

1. Анзина Т. И. Информационная безопасность как составляющая корпоративной культуры менеджера // Этносоциум и межнациональная культура. 2023. № 5 (179). С. 14–21. EDN: BYGPZY

2. Былевский П. Г. Культурологический подход к развитию общегражданской культуры безопасности интернет-коммуникаций // Litera. 2023. № 8. С. 157–167. DOI: 10.25136/2409-8698.2023.8.43827

3. Гурова А. С., Малыгина Л. Е., Слышкин Г. Г. Дискурс иноагентов: комизм – способ воздействия на сознание реципиента // Верхневолжский филологический вестник. 2022. №4 (31). С. 30–36. DOI: 10.20323/2499_9679_2022_4_31_30_36

4. 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

5. 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

6. Крестиненко Н. В. Трансформация функций запретов в сетевой культуре // Верхневолжский филологический вестник. 2023. № 2 (33). С. 221–228. DOI: 10.20323/2499_9679_2023_2_33_221

7. Малгаров И. И. Информационная культура и безопасность школьников в цифровой среде // Общество: социология, психология, педагогика. 2022. № 12 (104). С. 349–352. DOI: 10.24158/spp.2022.12.55

8. Мусаева А. С. Терминообразование в сфере искусственного интеллекта // Верхневолжский филологический вестник. 2022. №2 (29). С. 166–173. DOI: 10.20323/2499-9679-2022-2-29-166-173

9. Нынюк Р. Н. Проблемы виктимологической безопасности несовершеннолетних в цифровом пространстве // Труды Оренбургского института (филиа-

ла) Московской государственной юридической академии. 2022. № 2 (52). С. 81–83. EDN: QTNMNF

10. Осипенко Л. Е., Козицына Ю. В., Коротков А. В. Цифровой профиль школьника: потенциальные возможности и безопасность цифровой социализации // Общество: социология, психология, педагогика. 2022. № 8 (100). С. 158–163. DOI: 10.24158/spp.2022.8.23

11. Слышкин Г. Г., Малыгина Л. Е., Павлова Е. С. Лингвобезопасность в аспекте ценностных, идеологических и социальных изменений // Верхневолжский филологический вестник. 2022. №1 (28). С. 64–69. DOI: 10.20323/2499-9679-2022-1-28-64-69

12. Слышкин Г. Г., Малыгина Л. Е., Павлова Е. С. Радикальный феминный и маскулинный медиадискурс в аспекте лингвобезопасности // Верхневолжский филологический вестник. 2022. № 2 (29). С. 53–60. DOI: 10.20323/2499-9679-2022-2-29-53-60

13. Alsharida R., Al-rimy B., Al-Emran M., Zainal A. A systematic review of multi perspectives on human cybersecurity behavior // Technology in Society. 2023. Vol. 73. DOI: 10.1016/j.techsoc.2023.102258

14. 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

15. 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. Vol.134. DOI: 10.1016/j.cose.2023.103435

16. 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. Vol. 24, Iss. 2. July, Pp. 303-311. DOI: 10.1016/j.eij.2023.05.004

17. Hassandoust F., Subasinghage M., Johnston A. A neo-institutional perspective on the establishment of information security knowledge sharing practices // Information & Management. January 2022. Vol. 59. Iss. 1. DOI: 10.1016/j.im.2021.103574

18. Hengstler S., Kuehnel S., Masuch K., Nastjuk I., Trang T. Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior // Computers & Security. October 2023. Vol.133. DOI: 10.1016/j.cose.2023.103370

19. 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

20. Shiau W.-L., Wang X., Zheng F. What are the trend and core knowledge of information security? A citation and co-citation analysis // Information & Management. February 2023. Vol. 60. Iss. 3. DOI: 10.1016/j.im.2023.103774

21. 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. Vol. 119. DOI: 10.1016/j.cose.2022.102756

22. Uchendu B., Nurse J., Bada M., Furnell S. Developing a cyber security culture: Current practices and future needs // Computers & Security. June 2021. Vol. 109. DOI: 10.1016/j.cose.2021.102387

23. Vedadi A., Warkentin M., Dennis A. Herd behavior in information security decision-making // Information & Management. December 2021. Vol. 58. Iss. 8. DOI: 10.1016/j.im.2021.103526

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

25. Yin Y., Hsu C., Zhou Zh. Employees' in-role and extra-role information security behaviors from the P-E fit perspective // Computers & Security. October 2023. Vol. 133. DOI: 10.1016/j.cose.2023.103390

Reference list

1. Anzina T. I. Informacionnaja bezopasnost' kak sostavljajushhaja korporativnoj kul'tury menedzhera = Information security as a part of a manager's corporate culture // Jetnosocium i mezhnacional'naja kul'tura. 2023. № 5 (179). S. 14–21. EDN: BYGPZY

2. Bylevskij P. G. Kul'turologicheskij podhod k razvitiju obshhegrazhdanskoj kul'tury bezopasnosti internet-kommunikacij = A culturological approach to developing a civic culture of Internet communications security // Litera. 2023. № 8. S. 157–167. DOI: 10.25136/2409-8698.2023.8.43827

3. Gurova A. S., Malygina L. E., Slyshkin G. G. Diskurs inoagentov: komizm – sposob vozdejstvija na soznanie recipienta = Foreign agents' discourse: comic effect as a way to influence the recipient's mind // Verhnevolzhskij filologicheskij vestnik. 2022. №4 (31). S. 30–36. DOI: 10.20323/2499_9679_2022_4_31_30_36

4. Duben' A. K. Informacionnaja bezopasnost' v sisteme nacional'noj bezopasnosti: aktual'nye problemy informacionnogo prava = Information security in the system of national security: topical problems of information law // Voprosy bezopasnosti. 2023. № 1. S. 51–57. DOI: 10.25136/2409-7543.2023.1.40078

5. Kochetkov A. P., Maslov K. V. Cifrovoj suverenitet kak osnova nacional'noj bezopasnosti Rossii v global'nom cifrovom obshhestve = Digital sovereignty as the basis for Russia's national security in the global digital society // Vestnik Moskovskogo universiteta. Serija 12: Politicheskie nauki. 2022. № 2. S. 31–45. EDN: BJJUXI

6. Krestinenko N. V. Transformacija funkcij zapretov v setevoj kul'ture = Transformation of prohibition functions in network culture // Verhnevolzhskij filologicheskij vestnik. 2023. № 2 (33). S. 221–228. DOI: 10.20323/2499_9679_2023_2_33_221

7. Malgarov I. I. Informacionnaja kul'tura i bezopasnost' shkol'nikov v cifrovoj srede = Information culture

and schoolchildren's safety in the digital space // Obshhestvo: sociologija, psihologija, pedagogika. 2022. № 12 (104). S. 349–352. DOI: 10.24158/spp.2022.12.55

8. Musaeva A. S. Terminoobrazovanie v sfere iskusstvennogo intellekta = Terms formation in the artificial intelligence sphere // Verhnevolzhskij filologicheskij vestnik. 2022. №2 (29). S. 166–173. DOI: 10.20323/2499-9679-2022-2-29-166-173

9. Nynjuk R. N. Problemy viktimologicheskoj bezopasnosti nesovershennoletnih v cifrovom prostranstve = The problems of victimization security of the minors in the digital space // Trudy Orenburgskogo instituta (filiala) Moskovskoj gosudarstvennoj juridicheskoj akademii. 2022. № 2 (52). S. 81–83. EDN: QTNMNF

10. Osipenko L. E., Kozicyna Ju. V., Korotkov A. V. Cifrovoj profil' shkol'nika: potencial'nye vozmozhnosti i bezopasnost' cifrovoj socializacii = Digital profile of schoolchildren: potential and security of digital socialization // Obshhestvo: sociologija, psihologija, pedagogika. 2022. № 8 (100). S. 158–163. DOI: 10.24158/spp.2022.8.23

11. Slyshkin G. G., Malygina L. E., Pavlova E. S. Lingvobezopasnost' v aspekte cennostnyh, ideologicheskih i social'nyh izmenenij = Linguistic security in the aspect of value, ideological and social changes // Verhnevolzhskij filologicheskij vestnik. 2022. №1 (28). S. 64–69. DOI: 10.20323/2499-9679-2022-1-28-64-69

12. Slyshkin G. G., Malygina L. E., Pavlova E. S. Radikal'nyj feminnyj i maskulinnyj mediadiskurs v aspekte lingvobezopasnosti = Radical feminine and masculine media discourse in terms of linguistic security // Verhnevolzhskij filologicheskij vestnik. 2022. № 2 (29). S. 53–60. DOI: 10.20323/2499-9679-2022-2-29-53-60

13. Alsharida R., Al-rimy B., Al-Emran M., Zainal A. A systematic review of multi perspectives on human cybersecurity behavior // Technology in Society. 2023. Vol. 73. DOI: 10.1016/j.techsoc.2023.102258

14. 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

15. 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. Vol.134. DOI: 10.1016/j.cose.2023.103435

16. 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. Vol. 24, Iss. 2. July, Pp. 303-311. DOI: 10.1016/j.eij.2023.05.004

17. Hassandoust F., Subasinghage M., Johnston A. A neo-institutional perspective on the establishment of information security knowledge sharing practices // Information & Management. January 2022. Vol. 59. Iss. 1. DOI: 10.1016/j.im.2021.103574

18. Hengstler S., Kuehnel S., Masuch K., Nastjuk I., Trang T. Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior // Computers & Security. October 2023. Vol.133. DOI: 10.1016/j.cose.2023.103370

19. 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

20. Shiau W.-L., Wang X., Zheng F. What are the trend and core knowledge of information security? A citation and co-citation analysis // Information & Management. February 2023. Vol. 60. Iss. 3. DOI: 10.1016/j.im.2023.103774

21. 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. Vol. 119. DOI: 10.1016/j.cose.2022.102756

22. Uchendu B., Nurse J., Bada M., Furnell S. Developing a cyber security culture: Current practices and future needs // Computers & Security. June 2021. Vol. 109. DOI: 10.1016/j.cose.2021.102387

23. Vedadi A., Warkentin M., Dennis A. Herd behavior in information security decision-making // Information & Management. December 2021. Vol. 58. Iss. 8. DOI: 10.1016/j.im.2021.103526

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

25. Yin Y., Hsu C., Zhou Zh. Employees' in-role and extra-role information security behaviors from the P-E fit perspective // Computers & Security. October 2023. Vol. 133. DOI: 10.1016/j.cose.2023.103390

Статья поступила в редакцию 13.12.2023; одобрена после рецензирования 14.01.2024; принята к публикации 02.02.2024.
The article was submitted on 13.12.2023; approved after reviewing 14.01.2024; accepted for publication on 02.02.2024.