Litera
Правильная ссылка на статью:
Былевский П.Г. — Культурологический подход к развитию общегражданской культуры безопасности интернет-коммуникаций // Litera. – 2023. – № 8. DOI: 10.25136/2409-8698.2023.8.43827 EDN: XATBPE URL: https://nbpublish.com/library_read_article.php?id=43827

Культурологический подход к развитию общегражданской культуры безопасности интернет-коммуникаций

Былевский Павел Геннадиевич

ORCID: 0000-0002-0453-526X

кандидат философских наук

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

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

pr-911@yandex.ru

Статья из рубрики "Коммуникации"

DOI:

10.25136/2409-8698.2023.8.43827

EDN:

XATBPE

Дата направления статьи в редакцию:

17-08-2023

Аннотация: Проблемой, решаемой в настоящей статье, является определение возможностей и преимуществ культурологического подхода к решению проблемы развития общегражданской культуры безопасности интернет-коммуникаций. Предметом исследования служат структурно-функциональные особенности этой культуры, а объектом – эволюция формирования соответствующего комплекса убеждений, знаний, умений и навыков. Рассматривается тема расширения с узкопрофессиональной до общегражданской культуры безопасности интернет-коммуникаций. Анализируется увеличение доли и значения социально-культурных аспектов по сравнению с техническими факторами. Внимание уделяется содержательным аспектам общегражданской культуры безопасности интернет-коммуникаций: недостаточности методик трансляции на массовую аудиторию правил и актуальных примеров, а также недооценке формирования интуитивной осторожности, умений своевременно распознавать угрозы и правильно реагировать на инциденты. Новизна заключается в постулировании высокой репрезентативности культуры безопасности финансовых интернет-сервисов, обусловленной сочетанием массовости гражданских пользователей

и операций с денежными средствами, высоко привлекательными для злоумышленников. Именно здесь впервые сформировалась массовая интернет-преступность, эволюционировали угрозы и методы атак и, соответственно, средства безопасности. Сделан вывод: опыт противодействия «социальной инженерии» в сфере массовых финансовых сервисов полезен как основа формирования и развития общегражданской культуры безопасности интернет-коммуникаций, включая противодействие социально-культурным угрозам: фейк-новостям, дезинформации, деструктивному и запрещённому контенту. Результатом является выявление адекватности культурологического подхода к формированию и развитию общегражданской культуры безопасности интернет-коммуникаций: пользователями и потенциальными жертвами злоумышленников являются практически все граждане; увеличивается перечень и возрастает значение не столько технических, сколько социально-культурных угроз. Делается вывод: для противодействия социально-культурным угрозам интернет-коммуникаций недостаточно усилий только государства и профессиональных организаций, а также технических средств; требуется разработка методик формирования и повышения профильной общегражданской культуры методами культурологии как профильной науки.

Ключевые слова:

интернет-коммуникации, информационная безопасность, массовая общегражданская культура, социально-культурные угрозы, социальная инженерия, дезинформация, деструктивный контент, фейк-новости, гибридная война, культура безопасности

Введение

Универсальное развитие и применение интернет-коммуникаций наполняет культуру безопасности социально-культурным содержанием, превращая её как в национальную [1], так и в общегражданскую потребность, что подтверждается утверждением «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» (Распоряжение Правительства России от 22 декабря 2022 г. № 4088-р). Совокупность знаний, умений и навыков безопасного пользования компьютерно-телекоммуникационными сетевыми технологиями определена в этом документе именно как культура информационной безопасности.

В этой области всё большее значение приобретают социально-культурные факторы – и угрозы, и средства безопасности. Кроме того, интернет-коммуникации становятся всё более развитым и значимым фактором не только государственных и корпоративных компьютерно-телекоммуникационных систем, но и в социально-культурной жизни практически всех граждан [2]. В защите интернет-коммуникаций, кроме государственных и корпоративных средств безопасности, всё большую роль приобретает культура информационной безопасности граждан-пользователей.

1. Культурологический подход как профильный для культуры безопасности интернет-коммуникаций

Сетевой доступ разных уровней, особенно надстройка глобальных интернет-коммуникаций, открывает всё новые возможности пользоваться зарубежными, а в российском сегменте – самыми разнообразными отечественными ресурсами и сервисами (государственные услуги, торговля, транспорт, связь, пресса, книги, фильмы, видеоролики, социальные сети и т.д.) [3]. Расширение возможностей удовлетворения

социально-культурных потребностей посредством интернет-коммуникаций шло по мере формирования соответствующих сервисов и контента, в тесной взаимосвязи с увеличением технологических возможностей компьютерного и сетевого оборудования [4].

Интернет-коммуникации объединяют воедино возможности персональных устройств, корпоративных и государственных компьютерных систем на разных уровнях: локальном, национальном, международном и глобальном. Сетевые возможности многократно расширились покрытием в России большинства населённых территорий и транспортных путей широкополосным (в т.ч. беспроводным) сетевым доступом, массовым использованием мобильных устройств и «интернета вещей». Возможности универсального (везде, всегда и для каждого) пользования компьютерно-телекоммуникационными сетевыми технологиями являются технологической основой «цифровой трансформации» (включая «большие данные», «искусственный интеллект» и другие «сквозные технологии») [5].

Использование преимуществ интернет-коммуникаций постепенно проявляет обременение различными угрозами и рисками ущерба от инцидентов: технических неисправностей, атак злоумышленников, дискриминационных действий глобальных цифровых платформ и недружественных стран. У угроз и рисков, как у технологических решений, сервисов и пользовательских аудиторий интернет-коммуникаций, есть свои жизненные циклы. Некоторые риски, существующие давно, с начальных этапов развития технологий, могут неожиданно возрастать, достигать критических уровней, актуализироваться в качестве критических угроз. Угрозы, актуальные в течение определённого периода, уходят на второй план, становятся достоянием истории. Эволюционируют, сложно взаимодействуя, все элементы интернет-коммуникаций, включая типы угроз, рисков и ущерба, а также средства и культура безопасности [6].

Лишь упомянув здесь гипотетическую антиутопию «цифрового концлагеря», отметим реальную сопутствующую базовую угрозу: мобильные компьютерные устройства (смартфоны, планшеты, гаджеты, «умная» бытовая техника) технически, конструктивно и программным обеспечением, предназначены преимущественно для работы в беспроводных сетях, вне которых многие важные сервисы и функции становятся недоступными. При инциденте недоступности выхода в беспроводную сеть, технического или по воле провайдера связи, мобильное компьютерное устройство становится практически неработоспособным («карета превращается в тыкву»). В первом случае инцидент носит технический характер, во втором могут присутствовать самые разнообразные социально-культурные аспекты [7], например, кибердиверсии или зарубежные санкции. Перечень этих социально-культурных аспектов безопасности интернет-коммуникаций для пользователей может расширяться и реально увеличивается от «социальной инженерии» до тотального отслеживания и дискриминационной цензуры со стороны глобальных цифровых платформ.

Эффективно управлять развитием культуры безопасности интернет-коммуникаций как важнейшей составляющей пользовательских компетенций [8] помогает культурология как наиболее профильная наука, использующая, в частности, эволюционный и структурно-функциональный подходы. Культурологический анализ, в частности, позволяет рассмотреть структурную эволюцию угроз интернет-коммуникаций на основе комплексного сопоставления тенденций развития технологий, сервисов, контента, массовой пользовательской аудитории, защищаемых социально-культурных и других

ценностей [9].

Общее понимание закономерностей указанных процессов обеспечивает определение актуальных угроз, типов нарушителей (злоумышленников), уязвимостей, средств защиты и особенностей культуры безопасности как для существующей массовой пользовательской аудитории интернет-коммуникаций, так и для её различных групп. Первоначально предотвращение, минимизация, ограничение приемлемыми рамками ущерба, сопутствующего интернет-коммуникациям [10], относились к профессиональной культуре информационной безопасности [11]. Но в 2014 – 2022 годах развитие компьютерно-телекоммуникационной сетевой инфраструктуры в контексте трансформации глобальных и международных отношений привело к изменению ранжирования угроз, поставив на повестку дня в России формирование и развитие массовой общегражданской культуры безопасности интернет-коммуникаций.

2. Репрезентативность культуры безопасности дистанционных финансовых сервисов

Культурологический подход исходит из наличия в интернет-коммуникациях ценностей, включающий социально-культурные, которые могут подвергаться угрозам и нуждаются в защите, в том числе в особой культуре безопасности. Рассмотрим базовые понятия культуры безопасности интернет-коммуникаций. Необходимый элемент – наличие конфиденциальных значимых ценностей, права на которые ограничены, принадлежат только легальным пользователям. Не санкционированный доступ к этим ценностям является угрозой, поскольку тогда посторонний может извлечь выгоду в ущерб легальному пользователю. Ценности (активы, ресурсы, люди, убеждения, сведения и т.п.) относятся к базовым понятиям информационной безопасности: нет значимых ценностей – нечего и защищать. При наличии значимых ценностей без обеспечения необходимой зрелости систем обеспечения безопасности интернет-коммуникации и сервисы просто не могут существовать [12].

Субъектами безопасности выступают люди (группы, организации): легальные пользователи интернет-коммуникаций, обеспечивающие безопасность, и интернет-преступность (злоумышленники, нарушители). Компьютерно-телекоммуникационное оборудование, программное обеспечение и данные, Интернет и другая сетевая среда являются техническими средствами социально-культурных коммуникаций, оперирования ценностями. Технологии и оборудование, социально-культурные факторы являются элементами функционирования и использования динамической системы интернет-коммуникаций, а также обеспечения и нарушения безопасности. Основными элементами безопасности интернет-коммуникаций выступают люди (легальные пользователи и нарушители), ценности (защищаемые и атакуемые), технические и социально-культурные средства (с одной стороны, обеспечения, с другой – нарушения безопасности).

Структурно-функциональный анализ позволяет определить переломный момент и ключевую сферу формирования как массовой интернет-преступности, так и первых элементов общегражданской культуры безопасности интернет-коммуникаций. Основная предпосылка, «кормовая база» для распространения преступности на интернет-коммуникации – это наличие пользователей, оперирующих ценностями, несанкционированный доступ к которым высоко прибылен и мало рискован. Важным фактором служит соотношение с одной стороны, квалификации и инструментария нарушителей, с другой стороны – уязвимостей защиты интернет-коммуникаций.

Питательной средой, на основе которой зародилась современная интернет-преступность,

стали массовые дистанционные банковские сервисы (банкоматы, банкинг, платежи и переводы денежных средств через интернет), сформировавшиеся в 2000-е годы. Ранее произошла конверсия компьютерно-телекоммуникационных технологий из государственной и военной сфер для гражданского применения, вначале корпоративного, а потом и массового персонального. Компьютерная преступность переживала эмбриональную стадию развития, а культура безопасности оставалась узкопрофессиональной.

Появление и распространение массовых гражданских интернет-коммуникаций и сервисов являлось необходимой предпосылкой, но само по себе не вело к появлению современной интернет-преступности. Недостающим и решающим фактором, триггером и драйвером криминализации интернет-коммуникаций на тот момент стали массовые финансовые дистанционные сервисы, операции с денежными средствами – универсальной ценностью рыночного общества, непосредственно конвертируемой в любой товар, услугу. Значительные преимущества финансовых интернет-сервисов для бизнеса и клиентов существовали и для криминала, злоумышленников. Двумя главными факторами риска изначально выступали, во-первых, базовая анонимность пользователей, во-вторых, технологическая (местоположения серверов и маршрутизация) и правовая трансграничность интернет-коммуникаций. Злоумышленники могли организовывать хищения денежных средств в России из других стран, оставаясь практически вне досягаемости для расследования и правосудия.

2000-е годы можно считать первым этапом проявления актуальности культурологического подхода к безопасности массовых интернет-коммуникаций. Создание и распространение массовых финансовых интернет-сервисов и угроз хищений является переломной точкой: возникает необходимость защиты массового клиента – граждан, обладающих правом распоряжаться денежными средствами. Непосредственным ресурсом выступает профессиональная культура корпоративной информационной безопасности. На такой основе создаётся надстройка: профессиональная культура обеспечения безопасности клиентских сервисов, интернет-коммуникаций пользователей. Этот этап требует развития компетенций профессионалов информационной безопасности, защищающих клиентов, пользователей без их существенного участия.

Становление в России отрасли информационной безопасности банков, выстраивание системы государственного регулирования, организационно-технических и нормативно-правовых средств позволило к началу 2010-х годов понизить риски клиентских интернет-сервисов до приемлемых величин. Защищённость финансовых интернет-коммуникаций со стороны банковских, финансовых организаций удалось довести до необходимого уровня, профессиональная культура информационной безопасности массовых сервисов достигла пика развития. Финансовая отрасль оказалась первичной как для формирования интернет-преступности, так и для выстраивания профессиональной системы безопасности интернет-коммуникаций дистанционных сервисов. Банковские профессионалы информационной безопасности научились достаточно надёжно защищать граждан-клиентов от попыток хищений денежных средств злоумышленниками посредством технических средств (вредоносного программного обеспечения и т.п.).

3. Повышение роли социально-культурных факторов безопасности интернет-коммуникаций

2010-е годы – второй этап актуализации необходимости культурологического подхода к безопасности интернет-коммуникаций, характеризуется новыми реалиями социально-культурных факторов, угроз и средств защиты. По мере падения прибыльности атак на

финансовые интернет-сервисы интернет-преступность, злоумышленники вынуждены пополнять свой арсенал новыми не техническими средствами атак и искать высокодоходные цели среди нефинансовых ценностей в интернет-коммуникациях. Решение этой задачи облегчает значительное расширение интернет-ресурсов, сервисов, социально-культурного контента, пользовательской аудитории, её вовлечённости, оперирование в интернет-коммуникациях нефинансовыми ценностями высокого уровня [13], атаки на которые способны приводить к получению прибылей и других выгод.

Официальная статистика главного государственного регулятора информационной безопасности финансовой сферы, Банка России, показывает смещение главного вектора и инструментария атак злоумышленников. С середины 2010-х самые массовые и результативные атаки совершаются уже не на технические инструменты финансовых сервисов, а на сознание клиентов. Технические инструменты несанкционированного доступа к распоряжению денежными средствами (вредоносное программное обеспечение и др.) всё больше уступают место «социальной инженерии», интернет-мошенничествам («телефонным», в социальных сетях, по электронной почте, в мессенджерах и т.п.) [14]. Новые реалии подтвердила официальная статистика, «Отчёт Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019)».

Проявился предел возможностей профессиональной культуры безопасности: финансовых организациям уже не могли защитить от мошенников интернет-коммуникации клиента без его собственного активного участия. Был сделан вывод о необходимости формирования и развития, регулярной актуализации массовой культуры безопасности клиентов финансовых интернет-сервисов [15]. В защите от «социальной инженерии» главная роль принадлежит клиентам, а банковские специалисты выступают партнёрами и педагогами, разработчиками правил безопасности и методик обучения.

Процессы, аналогичные финансовой сфере, протекали в интернет-коммуникациях и сервисах с не финансовыми ценностями, атакуемыми интернет-преступностью и злоумышленниками. В то время как пользовательская аудитория социальных сетей и мессенджеров превысила половину человечества, эти интернет-коммуникации были заражены разнообразными деструктивными материалами, побуждавшими к самоубийствам, наркомании, экстремальному поведению и экстремистской деятельности, детской травле, школьным расстрелам и т.п. [16] Государственные меры нормативно-правового ограничения, блокировки доступа к незаконному контенту, привлечения к ответственности его создателей и распространителей оказались необходимыми и действенными, но недостаточными [17]. Как ранее в финансовой сфере, проявилась необходимость формирования и развития массовой, но уже общегражданской многопрофильной культуры безопасности интернет-коммуникаций.

С 2022 года по нынешнее время длится третий этап повышения актуальности культурологического подхода к безопасности интернет-коммуникаций по мере всё большего проявления нового комплекса угроз безопасности российских пользователей. Интернет-коммуникации всё более насыщаются новыми угрозами: фейк-новостями и дезинформацией [18], нацеленной на разрушение традиционных ценностей и социально-культурной идентичности российских граждан [19]. Перечень нарушений больше не ограничивается атаками международной интернет-преступности, пополняясь дискриминационными мерами (цензурой и др.) глобальных цифровых корпораций,

базирующихся в США, антироссийскими технологическими санкциями недружественных государств и другими подобными действиями в формате «гибридных войн» [20].

В ещё большей мере, чем на предыдущем этапе, в 2010-е годы, становится и государственной, и личной необходимостью формирование массовой общегражданской культуры безопасности интернет-коммуникаций, включая социально-культурные аспекты, а также защиту традиционных ценностей [21]. Для решения этой задачи ценным материалом выступает опыт формирования такой безопасности клиентов интернет-сервисов, накопленный в финансовой сфере. С другой стороны, полученный при этом опыт, обретённый гражданами, может выполнять для взрослых роль начального «всеобуча» культуре информационной безопасности не менее важный [22], чем для школьников соответствующие разделы предметов общей безопасности жизни и информатики.

Результаты

Результаты проведённого исследования показывают, что становится востребованным профильный, культурологический подход к культуре безопасности интернет-коммуникаций, в то время как прежние исследования и разработки велись в рамках других научных дисциплин, вначале технических, потом юриспруденции, педагогики, психологии и т.п. Применение инструментария культурологии, в частности, эволюционного и структурно-функционального подходов, позволяет выстроить динамическую системную модель – культурологическую парадигму информационной безопасности.

Такая теоретическая конструкция отражает закономерности становления, специфику и взаимосвязи различных элементов профессиональной, специализированной и общегражданской культуры информационной безопасности. Позиционирование в общей системе позволяет определить особенности и структурно-функциональные характеристики общегражданской культуры безопасности интернет-коммуникаций. Культурологическая методология может эффективно применяться для разработки методик и других средств развития и повышения данного направления культуры.

В частности, проведённый культурологический анализ позволил сделать вывод о том, что опыт обеспечения информационной безопасности дистанционных банковских сервисов является базовым и высоко репрезентативным для формирования и развития соответствующей массовой общегражданской культуры. Эволюция технологий, сервисов, угроз и пользователей интернет-коммуникаций требует конкретного анализа структурно-функциональных элементов обеспечения безопасности, учёт особенностей, сочетаний и взаимодействия технических и социально-культурных факторов в разработке средств повышения профильной культуры.

Библиография

1. Guitton M., Fréchette J. Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy // Computers in Human Behavior Reports. 2023. Vol. 10. DOI: 10.1016/j.chbr.2023.100282
2. Васильева Я.В., Калинюк Е.В. Проблемы развития системы обеспечения информационной безопасности Российской Федерации // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2023. №3. С. 94-99. DOI: 10.37882/2223-2974
3. Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brożek P. Global Digital

Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency // Journal of Open Innovation: Technology, Market, and Complexity. 2022. Vol. 8. Iss.4. DOI: 10.3390/joitmc8040195

4. Чижиков В.В. Информационные технологии как трансляторы культуры и искусства в виртуальной реальности // Вестник Московского государственного университета культуры и искусств. 2023. № 1 (111). С. 89-97. DOI: 10.24412/1997-0803-2023-1111-89-97
5. Былевский П.Г. Пользовательские и персональные данные – анализ рисков извлечения знаний // Вопросы защиты информации. 2023. № 1 (140). С. 35-40. DOI: 10.52190/20732600_2023_1_35
6. Богоудинова Р.З., Бородина С.Д., Мансурова А.Р. Информационная безопасность в современном мире: методологический аспект // Вестник Казанского государственного университета культуры и искусств. 2022. № 4. С. 16-20. EDN: IHZDFC
7. Taherdoost H. Cybersecurity vs. Information Security // Procedia Computer Science. 2022. Vol. 215. Pp. 483-487. DOI: 10.1016/j.procs.2022.12.050
8. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.-K. The role of national cybersecurity strategies on the improvement of cybersecurity education // Computers & Security. 2022. Vol. 119. DOI: 10.1016/j.cose.2022.102754
9. Узлова Н.В. Духовные и культурные ценности в парадигме национальной безопасности // Общество: философия, история, культура. 2023. № 4 (108). С. 89-92. DOI: 10.24158/fik.2023.4.12
10. Прохоров Ю.Н. Предотвращение ущерба потребителей от использования инструментов цифровизации: методологические основы формирования этики применения систем искусственного интеллекта // Финансовые рынки и банки. 2023. № 2. С. 35-41. EDN: RVDWWN
11. Timofeyev Yu., Dremova O. Insurers' responses to cyber crime: Evidence from Russia // International Journal of Law, Crime and Justice. 2022. Vol. 68. DOI: 10.1016/j.ijlcj.2021.100520
12. Miloslavskaya N., Tolstaya S. Information Security Management Maturity Models // Procedia Computer Science. 2022. Vol. 213. Pp. 49-57. DOI: 10.1016/j.procs.2022.11.037
13. Наговицын Р.С., Кривоногов А.Д. Гражданско-патриотическое воспитание студентов вуза культуры с использованием веб-сайтов на основе искусственного интеллекта // Вестник Казанского государственного университета культуры и искусств. 2023. № 1. С. 21-26. EDN: BKIXDN
14. AlGhanboosi B., Ali S., Tarhini A. Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach // Computers in Human Behavior. 2023. Vol. 144. DOI: 10.1016/j.chb.2023.107702
15. Родивилин И.П. Современная специфика детерминации преступлений в сфере обращения охраняемой законом информации // Вестник Удмуртского университета. Серия Экономика и право. 2021. Т. 31. № 2. С. 305-311. DOI: 10.35634/2412-9593-2021-31-2-305-311
16. Даниелян З.В. Информационная культура учителя как фактор профилактики подросткового кибербуллинга // Казанский педагогический журнал. 2021. № 1 (144). С. 64-70. EDN: FIVVJU
17. Малышева И.В. Социальные сети как правовой феномен // Сибирский юридический вестник. 2023. № 2 (101). С. 10-16. DOI: 10.26516/2071-8136.2023.2.10

18. Francisco M. Artificial intelligence for environmental security: national, international, human and ecological perspectives // Current Opinion in Environmental Sustainability. 2023. Vol. 61. DOI: 10.1016/j.cosust.2022.101250
19. Федоров А.В. Дезинформация как инструмент и составная часть информационного противоборства Запада // Южно-российский журнал социальных наук. 2022. Т. 23. № 2. С. 18-36. DOI: 10.31429/26190567-23-2-18-36
20. Лапшинова К.В., Подольская А.А. Феномен информационной войны в оценках молодежи Московского региона // Социально-гуманитарные технологии. 2022. № 3 (23). С. 11-16. EDN: XITITL
21. Дементьев С.А. Безопасность человека в сети интернет: проблемы и перспективы // Вестник Южно-Российского государственного технического университета (НПИ). Серия: Социально-экономические науки. 2023. Т. 16. № 2. С. 229-235. DOI: 10.17213/2075-2067-2023-2-229-235
22. Берестоk Т.Б. Теоретические подходы к изучению информационно-психологической безопасности в просоциальном поведении субъектов 60+ // Обзор педагогических исследований. 2021. Т. 3. № 8. С. 227-237. EDN: CJMQE

Результаты процедуры рецензирования статьи

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

Предметом исследования в представленной на рецензирование статье («Культурологический подход к развитию общегражданской культуры безопасности интернет-коммуникаций») является проблема развития культуры информационной безопасности. При этом под культурой информационной безопасности, как это определено распоряжением Правительства России, автором понимается совокупность знаний, умений и навыков безопасного использования людьми компьютерно-телекоммуникационных сетевых технологий. Существенным моментом, по мнению рецензента, является опора автора на государственный нормативный документ и уточнение базового субъекта информационной безопасности — гражданина России. Соответственно, помимо обозначенных автором структурно-функционального и эволюционного культурологических подходов, представленное исследование включает в себя и опору на актуальный в области методического обеспечения государственной культурной политики России ценностно-нормативный подход, который подразумевает, что принимаемые государством правовые нормативы обусловлены необходимостью сохранения и эксплуатации некоторой совокупности ценностей, складывающихся в процессе жизнедеятельности общества в исторически развивающуюся систему, программирующую формы индивидуальной и коллективной деятельности. В этом контексте, развитие культуры информационной безопасности, как элемент исторического процесса, выступает в качестве объекта изучения, в котором автор акцентировал внимание на эволюции самой проблемы (предмета) обеспечения информационной безопасности, которая из узко технической области на первоначальном этапе развития компьютерно-телекоммуникационных сетевых технологий переместилась на текущий момент в область общегражданской и государственной безопасности. Статья, таким образом, посвящена культурологической проблематизации обеспечения безопасного использования людьми компьютерно-телекоммуникационных сетевых технологий, где, в свою очередь, проблема понимается как абстрактная категория, обретающая по аналогии с культурной формой конкретное содержание в зависимости от исторической

динамики использования людьми компьютерно-телекоммуникационных сетевых технологий.

Автор четко обозначил структурную классификационную схему элементов функционирования динамической системы интернет-коммуникаций по принципу соблюдения/несоблюдения нормативов безопасности: люди, разделяющиеся на легальных пользователей и нарушителей, ценности (защищаемые и атакуемые), технические и социально-культурные средства (с одной стороны, обеспечения, с другой — нарушения безопасности).

Вполне резонно отметив, что эволюция проблемы обеспечения информационной безопасности граждан обусловлена расширением ценностных характеристик интернет-коммуникации (атакуемых и защищаемых в рамках интернет-коммуникации ценностей), автор выделяет три этапа эволюции проблемы в российском сегменте.

Первый этап (2000-е гг.) им охарактеризован как финансово-технический: связанный с преодолением рисков осуществления с помощью интернет-коммуникации финансовых операций преимущественно корпорациями и финансовыми институтами, которые и формировали технические средства и специальные службы информационной безопасности, повлекшие становление профессиональной культуры информационной безопасности массовых сервисов.

Второй этап (2010-е гг.) характеризуется сохранением финансовой стороны интересов злоумышленников, но ввиду повышения профессиональной культуры информационной безопасности, объект атак смещается с технических средств массовых сервисов на их пользователей. Актуализируется, соответственно, проблема элементарной массовой культуры финансовой и информационной безопасности граждан, которая решалась за счет пропедевтики информационной грамотности банковскими специалистами и педагогами, «разработчиками правил безопасности и методик обучения».

Однако, начиная с 2022 г. объектом атак становится не столько область финансов, сколько область индивидуального и общественного психического здоровья, в которой, по мысли автора, злоумышленниками все чаще применяются технологии «социальной инженерии», направленные на деструкцию социального поведения пользователей компьютерно-телекоммуникационных средств коммуникации. Помимо этого, целью атак становятся стратегические объекты экономической, социальной, военной инфраструктуры. Соответственно, целью атак злоумышленников становится не столько отдельный гражданин, а общество в целом — его комплексная социокультурная сфера, что определенным образом характеризует и атакующего субъекта: происходит не только профессионализация злоумышленников, но и организация их в криминальные и военизированные спецподразделения для нанесения максимального ущерба намеченному противнику. Как следствие, расширение сегодня области проблем обеспечения информационной безопасности до государственного уровня, требует не только нормативного регулирования и государственной охраны специализированными подразделениями госбезопасности, но и внимания теоретиков, их тесного сотрудничества в междисциплинарной области, которая могла бы методически обеспечить безопасность социокультурной сферы общества в условиях интенсивной информатизации.

Таким образом, предмет исследования автором рассмотрен на достаточно высоком теоретическом уровне, итоговые выводы обоснованы и заслуживают доверия.

Методология исследования, как отмечено выше, помимо инструментария эволюционного и структурно-функционального культурологических подходов, базируется на актуальном для отечественной культурологии аналитическом комплексе ценностно-нормативной теории культуры. Несмотря на то, что автор отдельно не формализует программу исследования, она ясно просматривается в логике раскрытия эволюции проблемы

культуры информационной безопасности российского общества.

Актуальность поднятой автором темы крайне высока. Рецензент подчеркивает, что, как и многие технологические достижения, информационные технологии могут использоваться не только во благо, но также в криминальных и военно-политических целях во вред человеку и обществу, поэтому подчёркнутая автором необходимость культурологического подхода, обладающего эвристическим преимуществом глубоких междисциплинарных связей, представляется вполне уместной и своевременной.

Научная новизна, отраженная в авторской тематической выборке научной литературы, типологии и классификации рисков и угроз в области культуры информационной безопасности, структуры функционирования динамической системы интернет-коммуникаций и периодизации развития проблематики культуры информационной безопасности в российском обществе, не вызывает сомнений, итоговый вывод хорошо обоснован и заслуживает доверия.

Стиль в целом выдержан научный, хотя во фрагменте: «Проявился предел возможностей профессиональной культуры безопасности: финансовых организациям уже не могли защитить от мошенников интернет-коммуникации клиента без его собственного активного участия», — мысль автора не ясна и требует уточнения. Структура статьи отражает логику изложения результатов научного исследования.

Библиография хорошо отражает проблемное поле исследования, оформлена с учетом требований редакции и ГОСТа.

Апелляция к оппонентам корректна и уместна.

Статья, безусловно, представляет интерес читательской аудитории журнала «Litera», поскольку раскрывает существенную проблемную область медиакоммуникации, и после небольшой доработки может быть рекомендована к публикации.