Социальная диагностика информационной безопасности цифрового социума: методологические и нормативно-правовые аспекты

УДК 316.2 DOI 10.26425/2658-347X-2019-3-25-32

Получено 16.09.2019 Одобрено 21.10.2019 Опубликовано 31.12.2019

Кибакин Михаил Викторович

Д-р социол. наук, профессор, доцент, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва, Российская Федерация

ORCID: 0000-0001-6373-0869

E-mail: MVKibakin@fa.ru

АННОТАЦИЯ

Представлена целостная экспертная методика социальной диагностики информационной безопасности российского общества, которая в своей методологической и нормативно-правовой основе опирается на закрепленную в отечественном праве концепцию национальной безопасности как способности государственных и общественных институтов противостоять угрозам интересам личности, общества и государства. Изложена сущность цифрового общества как объекта защиты от неблагоприятного воздействия на технологическом уровне (компьютерная, программно-аппаратная база цифровых коммуникаций), а также на уровне контента, распространяемого в информационно-коммуникационной сети «Интернет» (далее – Интернет). Выполнено описание субъектов виртуальной коммуникации с точки зрения их возможностей и практики защиты от неблагоприятного информационного воздействия. Дана характеристика различных ситуаций социального взаимодействия, которым может угрожать неправомерный доступ к персональной информации – в финансово-экономических и служебных отношениях.

Отдельно проведен анализ статуса должностных лиц – субъектов реализации государственных полномочий в органах власти, который может представлять особую уязвимость при слабой урегулированности злонамеренного распространения ложной информации в Интернете. Особое внимание уделено обоснованию возможностей раннего выявления информационных угроз функционированию базовых социальных институтов – социального доверия и устойчивости социальных отношений, солидарности, цивилизационной идентичности, межконфессионального мира и толерантности в сложном обществе.

Авторская методика в статье представлена как социологическая исследовательская технология, включающая интерпретацию и операционализацию групп информационных угроз, закрепленных в государственной концепции национальной безопасности, корректного применения экспертных процедур для оценки защищенности от этих угроз, а также последующей математико-статистической и логической интерпретацией полученных данных. Изложены предложения по использованию методики социальной диагностики информационной безопасности в практике социального управления в процессе трансформации современного социума на основе цифровых технологий.

Ключевые слова

Социальная диагностика, Интернет, цифровой социум, информационная безопасность, интернет-контент, информационные угрозы, цифровые технологии, цифровая социология

Цитирование

Кибакин М.В. Социальная диагностика информационной безопасности цифрового социума: методологические и нормативно-правовые аспекты//Цифровая социология. 2019. Т. 2. № 3. С. 25–32.

Social diagnostics of information security of digital society: methodological and regulatory aspects

DOI 10.26425/2658-347X-2019-3-25-32

Received 16.09.2019 Approved 21.10.2019 Published 31.12.2019

Kibakin Mikhail

Doctor of Sociological Sciences, professor, associate professor, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ORCID: 0000-0001-6373-0869

E-mail: MVKibakin@fa.ru

ABSTRACT

A holistic expert method of social diagnostics of information security of the Russian society, which in its methodological and regulatory framework is based on the concept of national security, as the ability of state and public institutions to resist threats to the interests of the individual, society and the state has been presented. The essence of digital society as an object of protection from adverse effects at the technological level (computer, software and hardware base of digital communications), as well as at the level of content distributed in the information and communication network "Internet" has been stated. The subjects of virtual communication in terms of their capabilities and practice of protection from adverse information impact have been described. The characteristic of various situations of social interaction, which may be threatened by unauthorized access to personal information – in financial, economic and official relations, – has been given.

A separate analysis has been made of the status of officials-subjects of the implementation of state powers in the authorities, which may be particularly vulnerable in the weak regulation of malicious dissemination of false information in the information and communication network "Internet". Special attention has been paid to the substantiation of the possibilities of early detection of information threats to the functioning of basic social institutions – social trust and stability of social relations, solidarity, civilizational identity, interfaith peace and tolerance in a complex society.

The author's methodology has been presented in the article as a sociological research technology that includes the interpretation and operationalization of groups of information threats enshrined in the state concept of national security, the correct application of expert procedures to assess security against these threats, as well as the subsequent mathematical-statistical and logical interpretation of the data obtained. The proposals for the use of methods of social diagnostics of information security in the practice of social management in the process of transformation of modern society on the basis of digital technologies have been explained.

Keywords

Social diagnostics, Internet, digital society, information security, Internet content, information threats, digital technologies, digital sociology.

For citation

Kibakin M.V. (2019) Social diagnostics of information security of digital society: methodological and regulatory aspects. *Digital sociology*. Vol. 2, no 3, pp. 25–32. DOI: 10.26425/2658-347X-2019-3-25-32

В современных условиях развития цифрового социума, что включает в себя процессы становления институтов цифровизации социальных коммуникаций, построения цифровой экономики и расширения финансовых сервисов на основе виртуальных технологий удаленного доступа, а также глобализации информационных потоков, их все большую включенность в повседневную жизнь человека, важнейшей проблемой является обеспечение информационной безопасности социума.

В связи с этим закономерным является глубокая научно-методологическая проработка информационной безопасности, как объекта философского, правового, социально-политического изучения [Перчук, 2002; Артамонова, 2014; Мнацаканян, 2016], а также активное обсуждение этой проблематики в научной среде [Комкова, 2013; Понкин, Редькина, 2019; Шарахина, 2019] и публикации результатов научного изучения проблем развития цифрового социума [Алиева, 2019].

Методологической основой социальной диагностики информационной безопасности является прежде всего объектно-охранительная концепция защищенности базовых социальных институтов, социума и субъектов социальных отношений от внешних и внутренних угроз – факторов, которые могут нанести непосредственный вред их функционированию и жизнедеятельности.

Не менее важной на этом уровне является концепция защиты прав человека, применительно к обеспечению личных данных, создание условия защищенности частной жизни. Это связано с тем, что при всех положительных сторонах использования интернет-коммуникаций, в том числе социальных сетей, необходимо знать и помнить о возможности негативного использования предоставляемых персональных данных. Так, очевидно, что несанкционированное использование личной (частной, персональной информации) субъектов социального взаимодействия в цифровом обществе в противоправных целях может нанести не «виртуальный», а реальный (иногда непоправимый) вред человеку, а именно:

– опорочить честное имя, историю жизни, личную честь среди неограниченного числа лиц;

– унизить личное достоинство, что резко снижает социальную активность и социальное самочувствие;

– разрушить деловую репутацию, нанеся материальные убытки.

Прежде всего в условиях глобальной цифровизации существует опасность доступа к персональной информации пользователей социальной сети посторонним субъектам социального взаимодействия[1]. В нашей стране законодательно определено, что персональные данные:

– всякие сведения физического лица, как субъекта с частной жизнью;

– связанные с субъектом социального взаимодействия непосредственно или опосредованно.

К конституционным нормам в нашей стране отнесены:

– гарантии неприкосновенности частного социального пространства, частной жизни;

– гарантии защиты тайны, как семейной, так и личной;

– гарантии принятия мер по обеспечению неприкосновенности приватной жизни человека;

– гарантии защищенности чести человека, его доброго имени;

– гарантии законодательного обеспечения тайны обмена информации путем почтовых отправлений и переговоров по телефону;

– гарантии тайны сообщений посредством почты, телеграфа и других способов.

Лишь сам человек может дать разрешение на сбор информации о его приватной жизни, а также и хранение частных (персональных) сведений, тем более распространение личной информации о человеке. Особо в законодательстве закреплено понятие конфиденциальности персональной информации, которая может быть в целях социальной диагностики использовано в качестве квалифицирующего индикатора информационной безопасности личности.

Объектом социальной диагностики уровня защищенности от информационных угроз в цифровой социологии является процесс обработки личных сведений (персональных данных). При этом в качестве первичной информации могут быть выделены характеристики:

– поиска персональных сведений;

– широты сбора социальных фактов;

– фиксации (записи) конфиденциальной информации;

– алгоритмы систематизации личных характеристик;

– насыщение информацией специальных баз данных;

– надежное сохранение собранных первичных данных.

В силу постоянного развития социальных процессов, изменчивости социальных характеристик, в социологических исследованиях информационной безопасности необходима фиксация динамичных характеристик:

– постоянное уточнение персональных сведений, их обновление в рамках принятых регламентов;

– изменение квалификации выраженности характеристик.

Наконец, целесообразно фиксировать управленческо-организационные аспекты информационных процессов, как объекта социологического анализа, к которым относятся:

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» / СЗ РФ от 12.12.2016 № 50 ст. 7074. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601/ (дата обращения: 09.09.2019).

– релевантность регламентов извлечения персональных данных из баз данных;

– профессиональное (служебное) использование личных сведений;

– содержание и оптимальность механизмов передачи личной информации, в том числе распространение среди неопределенного круга лиц;

– порядок предоставления персональных сведений на законных основаниях уполномоченным субъектам социального управления;

– условия доступа к конфиденциальной информации;

– эффективность мер защиты информации, в том числе ее обезличивание, системное блокирование личных сведений на различных информационных и справочных ресурсах, правомерное удаление отдельных сведений, а также безвозвратное уничтожение данных о субъектах информационной защиты.

Социальные противоречия при реализации нормативных установлений в сфере защиты персональных данных в контексте информационной безопасности связаны с действием следующих факторов:

– недостаточной урегулированности прав на использование автоматизированных (обезличенных) систем сбора и обработки сведений частного характера;

– фрагментарностью норм, определяющих статус, полномочия и ответственность субъектов сбора данных – операторов, институтов информационной поддержки государственного управления, информационных сервисов;

– объективной неопределенностью социальных ситуаций трансформации персональных данных в общедоступные (например в отношении публичных лиц), а также наоборот (ограничение информации, которая противоречит принципам морали и нравственности).

В ситуации нормативного регулирования вопросов защиты личных сведений в системе обеспечения информационной безопасности личности важно указать на широкое использование механизма возмещение нанесенных убытков и (или) разумную компенсацию установленного морального вреда в институционально закрепленном судебном порядке в случае доказанного нарушения принципа неприкосновенности частной жизни. Одновременно в условиях цифрового общества, активного вовлечения населения в социальные интернет-практики, нормативно-правовое регулирование «отстает» от динамичного развития современных форм коммуникации, что приводит к тому, что защита персональной информации участников различных социальных сетей российским законодательством недостаточно эффективно.

Еще одной угрозой является возможность формировать через социальную сеть базу пользователей для рассылки спама. Открытость персональной информации пользователя социальной сети позволяет сформировать досье на каждого без нарушения законодательства. Такие досье могут использоваться третьими лицами в различных целях, например, при решении вопроса о приеме на работу.

Еще одной проблемой является возможность несанкционированного изменения личной информации, что может нанести вред репутации пользователя.

Социальные сети, в свою очередь, ведут большую работу по совершенствованию своих систем безопасности. Отечественным законодательством предусмотрено право уполномоченных государственных структур на использование следующих институциональных механизмов информационной безопасности личности:

– обращение в судебные институты, подача исков по принятию мер защиты конкретного субъекта правоотношений;

– задействование административных регламентов по ограничению, прекращению, а в ряде случаев приостановлению процессов обработки личных сведений, доступных персональных данных;

– побуждению правоохранительных органов к квалификации противоправности и наказуемости неправомерного сбора и введения в оборот первичных данных.

Особое значение имеет вопрос о правомерности использования информации в социальных сетях при изучении сведений о потенциальном работнике работодателем или кадровой службой. Многие работодатели наблюдают за работниками в социальных сетях, проверяют представленные ими сведения. С одной стороны, доступ к своей информации в социальных сетях для других пользователей этого ресурса человек устанавливает самостоятельно. Если информация общедоступна, работодателю не требуется получать специальное разрешение для того, чтобы ознакомиться с ней.

Служебное поведение государственного служащего, как носителя определенной информации, находится под особым социальным контролем, которые включает в себя различные механизмы регулирования его профессиональной активности.

К ним относятся прежде всего юридические нормы по закреплению статуса государственного служащего, его особых прав при реализации функций государственного управления, дополнительных гарантий его неприкосновенности при исполнении служебных обязанностей и законодательно закрепленных полномочий, при одновременном ограничении и запрета его социальной активности[2]. Эти нормы могут рассматриваться в качестве косвенных регуляторов включения государственного служащего в социальные сети, социальной активности в информационно-коммуникационной сети «Интернет».

[2] Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (ред. от 01.05.2019) / СЗ РФ от 02.08.2004 № 31 ст. 3215. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601 (дата обращения: 09.09.2019).

Государственно-правовые механизмы защиты государственной службы от информационных угроз, источником которых является интернет-активность государственных служащих, делятся по характеру воздействия на эту сферу социальных отношений на:

– механизмы предписывающего характера, включающие нормы реализации конкретных моделей поведения, действий и регламентов при выполнении стандартных и нестандартных задач профессиональной деятельности;

– запретительные механизмы, ограничивающие или делающие невозможными совершение определенных поступков, использования в некоторых форм социальной активности, которые все больше распространяются на социальную активность в виртуальном пространстве;

– механизмы рекомендательного характера, которые закрепляют общие правила, установления и квалификацию социальной активности, оценку связанных с ними информационных угроз, как нормы, которым целесообразно следовать для обеспечения личной информационной безопасности.

Следующая группа регуляторных механизмов профессиональной деятельности государственного служащего в условиях развития цифрового общества носит социокультурный, нравственно-ценностный характер. Важно указать при этом, что личная мораль государственного служащего является не только субъективным, личностно детерминированной и основанной лишь на собственных представлениях о «должным» и «желаемым» мировоззренческой модели, но и прежде всего культурно-историческими установлениями общества, в том числе «цифрового социума». При этом социальный контроль в системе информационной безопасности личности с особыми полномочиями предполагает установление и социальную диагностику соблюдения ими:

– нравственных, этических стандартов решения профессиональных задач;

– норм уважения и доброжелательности в коммуникациях с населением.

Целесообразно выделить группу организационно-управленческих механизмов предотвращения возникновения и негативного воздействия информационных угроз на государственного служащего, которые наиболее наглядно проявляются в системе подбора кадров. Эти механизмы должны снижать возможности включения в систему государственной службы лиц, которые готовы реализовать принципы демократизма и свободы самовыражения, с присущим им субъективностью и поливариантностью оценки моральных, этических, нравственных категорий, без должного соблюдения норм профессионального поведения и служебной этики. Это достигается как путем совершенствования норм отбора, так и системной постоянной профессиональной подготовки, а также рационального и законного использования санкционных мер к нарушителям правил профессионального поведения и деятельности. Наиболее эффективными при этом являются меры внешнего воздействия на человека, если они связаны интериоризацией человеком ценностей и норм общества, традиционной морали, которая в условиях цифрового общества продолжает оставаться основой личного сознательного выбора социально одобряемых норм поведения. Соответственно, кадровые механизмы должны включать формы формирующего воздействия на сознание государственного служащего, в том числе его установки на соблюдение правил распространения информации.

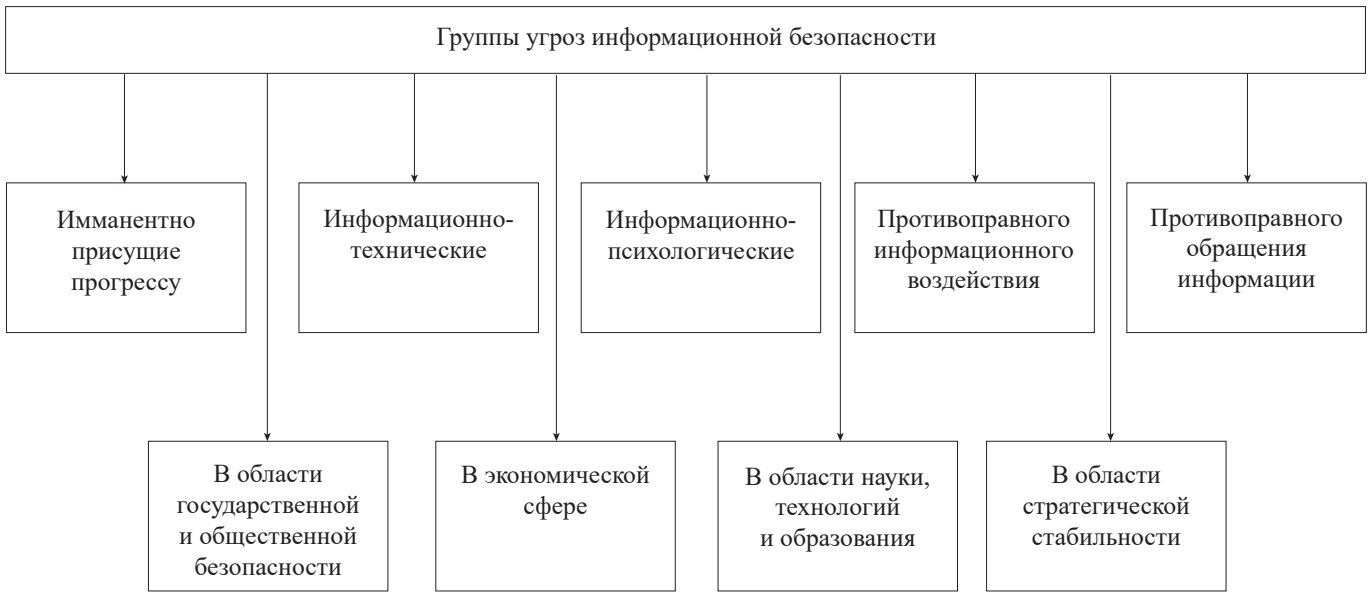
Свое место в характеристике механизмов обеспечения информационной безопасности государственных служащих, их ответственного поведения в социальных сетях, информационном пространстве является использование хорошо зарекомендовавшего себя зарубежного опыта внедрения системы предотвращения возникновения информационных угроз, в частности принятия всевозможных корпоративных правил, стандартов, принципов. Одним из примеров этого является Моральный кодекс американского общества государственного управления, который в определенной степени может послужить источником для уточнения правил поведения российских государственных служащих в цифровом обществе.

Однако, как показывает практика, периодически работники государственной власти допускают в своем поведении в социальных сетях отклонения от норм этики, позволяют себе высказывать оскорбления в адрес оппонентов и различные аморальные поступки. В связи с этим, неоднократно поднимался вопрос о создании свода правил поведения государственных служащих в Интернете, и в частности в социальных сетях.

На методическом уровне социальные диагностические процедуры опираются на индикативную нормативную модель, представляющую собой результат процедур интерпретации и операционализации актуальных угроз информационной безопасности нашей страны и российского социума[3], что отражено в рисунке 1.

Соответственно, система подлежащие эмпирическому изучению сведения в области информационной безопасности личности, государства и социума представлены группой угроз (на высшем уровне обобщения), информационными угрозами (на среднем уровне обобщения), а также индикаторами (на первичном уровне) – непосредственно подлежащими фиксации первичными данными.

[3] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» / СЗ РФ от 12.12.2016 № 50 ст. 7074. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601/ (дата обращения: 09.09.2019).



Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

***Рис.1.* Актуальные угрозы информационной безопасности**

Figure 1. Current threats to information security

Диагностическая модель включает совокупность первичных индикаторов информационной защищенности, а также их иерархические связи для объединения на уровне угроз и групп угроз.

Первая группа – информационные угрозы, имманентно присущих социально-экономическому развитию и влияющих на функционирование цифрового социума.

Социологическое исследование предполагает экспертную оценку защищенности от потенциальной информационной угрозы в силу внедрения информационных технологий в государственные институты и критические системы жизнеобеспечения без достаточной увязки с обеспечением безопасности, то есть использования информационных технологий в условиях недостаточного обеспечения информационной безопасности.

Вторая группа включает информационные угрозы функционированию институтов цифрового социума информационно-технического характера.

Учитывая технологическое доминирование США в контроле за всемирными интернет-ресурсами, глобальной информационно-коммуникационной инфраструктурой, социальной диагностике подлежит уровень противодействия информационной угрозе, связанной с технической разведкой различных стран в отношении институтов национальной безопасности, а также сил и средств, привлекаемых для обороны страны.

В третьей группе представлены угрозы информационно-психологического характера, влияющие прежде всего на социокультурную сферу цифрового социума.

В целях социальной диагностики информационной безопасности определяются способность нашего государства и общества противостоять:

– информационной угрозе, связанной с информационно-психологическим воздействием деструктивных акторов социального, религиозного, этнического характера, а также некоторых правозащитных организаций и инициативных групп на дестабилизацию внутриполитической и социальной ситуации в российском социуме, социальных стратах и региональных локальных социальных сообществах;

– информационной угрозе в связи с предвзятостью зарубежных источников информации, информационных ресурсов Интернета против российского общества, его ценностей, традиций, символов и цивилизационной миссии;

– информационной угрозе воздействия на российское население в целях размывания традиционных российских духовно-нравственных ценностей, а также целенаправленного воздействия на молодежь России в целях размывания традиционных российских духовно-нравственных ценностей.

Четвертая группа угроз связанна с использованием противоправными структурами механизмов информационного воздействия на все сферы функционирования цифрового социума, жизнедеятельности людей.

Эта область информационной безопасности приобретает особое значение в условиях различных региональных конфликтов. В современном цифровом обществе различные экстремистские организации, террористы получили возможность и используют

механизмы массового информационного негативного воздействия на основе цифровых платформ на мотивационно-ценностную основу сознания различных категорий людей. Цифровые технологии передачи экстремистской информации используются для достижения целей разрушения, вражды, ненависти, нетерпимости к представителям других религий, культур, национального самосознания.

В цифровой социологии социальные диагностические процедуры позволяют определить содержание и эффективность явных и скрытых технологий информационного влияния на установки личности, переформулирования у них морально-нравственной основы поведения. В отдельных случаях это может привести к привлечению новых сторонников в организации экстремистского и террористического характера.

Система индикаторов позволяет в рамках предлагаемой модели и оценку устойчивости институтов (объектов) критической информационной инфраструктуры в условиях информационно-психологического противоборства.

Пятая группа информационных угроз связана с противоправным обращением информации в цифровом социуме.

При этом требуется диагностика компьютерной преступности, которая приобретает в ряде случаев более тяжкий характер.

Требуется также фиксация социально «чувствительных» параметров информационной безопасности, а именно защищенность от противоправного использования информационных технологий в сфере нарушения конституционных прав и свобод человека и гражданина через неправомерный доступ к персональным данным, нарушения принципа обеспечения неприкосновенности частной жизни, личной и семейной тайны.

Особую, шестую группу составляют информационные угрозы в области государственной и социальной безопасности, социальная диагностика которых включает:

– определение уровня защищенности от атак компьютерными цифровыми информационно-технологическими средствами на различные объекты информационной инфраструктуры, которые имеют критическое значение для нашей страны;

– способность снижать уровень негативного воздействия применения информационных технологий в целях нанесения ущерба политической и социальной стабильности страны.

Седьмую группу составляют информационные угрозы в экономической сфере цифрового социума.

Социологическое исследование для определения защищенности от этих угроз включает определение возможностей Российской Федерации компенсировать уязвимости отечественной технологической базы цифрового социума недостаточного уровня развития конкурентоспособных информационных технологий, зависимость от зарубежных информационных технологий, вычислительных технологий и средств связи на цифровых платформах.

Восьмая группа – информационные угрозы в сфере науки, технологий и образования цифрового социума.

Критичными в этой области являются:

– недостаточный уровень научных исследований в области информационных технологий;

– низкий уровень внедрения отечественных разработок в области информационной безопасности;

– неполное кадровое обеспечение в области информационной безопасности;

– низкая осведомленность населения в вопросах личной информационной безопасности;

– недостаточная системность проводимых в нашей стране мероприятий по обеспечению безопасности ее информационной инфраструктуры с точки зрения ее целостности, доступности и устойчивого функционирования.

Совокупность информационных угроз стратегической стабильности и равноправного стратегического партнерства российского общества с общественно-политическими системами общечеловеческой цивилизации составляет девятую группу.

Экспертной оценке в этой области подлежат:

– информационная угроза враждебного доминирования некоторых государств в информационном пространстве цифрового социума;

– информационная угроза несправедливого использования Интернета со стороны ряда государств, связанного с нанесением ущерба информационному пространству нашей страны, несправедливое управление со стороны некоторых государств обеспечением безопасного и устойчивого функционирования Интернета, входящей в информационное пространство российского социума.

Таким образом, цифровая социология в соответствии с современным уровнем развития сетевых технологий коммуникации, использования информационно-коммуникационных сетей в развитии общественных отношений, может обоснованно включить в объектно-предметную область своих исследование диагностику информационных вызовов, опасностей и угроз, а также обеспечения информационной безопасности цифрового социума.

БИБЛИОГРАФИЯ

Алиева Н.З. (2019). Глобальное цифровое пространство: методология проектирования безопасности человека и социума: монография. Новочеркасск: Лик. 111 с.

Артамонова Я.С. (2014). Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: автореф. дис…. д-ра полит. наук. Москва, 56 с.

Комкова К.С. (2013). Безопасность персональной информации в социальных сетях: правовой аспект//Вестник южного научного центра, том 9, № 3, С. 71–73.

Мнацаканян А.В. (2016). Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: автореф. дис. … канд. юр. наук. Москва, 41 с.

Перчук Е.Е. (2002). Информатизация и информационная безопасность: Философско-методологические аспекты: автореф. дис…. канд. филос. наук, Москва, 25 с.

Понкин И.В., Редькина А.И. (2019). Цифровые онтологии права и цифровое правовое пространство//Пермский юридический альманах. № 2. С. 24–37.

Шарахина Л.В. (2019). Сегментирование целевых аудиторий, использование лидеров общественного мнения, экспертное позиционирование бренда в цифровом пространстве//Российская школа связей с общественностью. № 13. С.84–92.

REFERENCES

Alieva N.Z. (2019), *Global digital space: methodology for designing human and social security: monograph* [*Global'noe tsifrovoe prostranstvo: metodologiya proektirovaniya bezopasnosti cheloveka i sotsiuma: monografiya*], Lik, Novocherkassk, 111 p. [in Russian].

Artamonova Ya.S. (2014), *Information security of Russian society: theoretical foundations and practice of political support: autoref. dis…. Dr. politich. Sciences* [*Informatsionnaya bezopasnost' rossiiskogo obshchestva: teoreticheskie osnovaniya i praktika politicheskogo obespecheniya: avtoref. diS…. d-ra politich. nauk*], Moscow, 56 p.

Komkova K.S. (2013), "Security of personal information in social networks: legal aspect" ["Bezopasnost' personal'noi informatsii v sotsial'nykh setyakh: pravovoi aspect"], *Vestnik Yuzhnogo nauchnogo tsentra*, vol. 9, no. 3, pp. 71–73.

Mnatsakanyan A.V. (2016), *Information security in the Russian Federation: criminal law aspects: autoref. dis. ... kand. Jus. sciences* [*Informatsionnaya bezopasnost' v Rossiiskoi Federatsii: ugolovno-pravovye aspekty: avtoref. dis. ... kand. yur. nauk*], Moscow, Russia.

Perchuk, E.E. (2002), *Informatization and information security: Philosophical and methodological aspects: autoref. dis…. cand.philos. sciences* [*Informatizatsiya i informatsionnaya bezopasnost': Filosofsko-metodologicheskie aspekty: avtoref. diS…. kand.filos. nauk*], Moscow, Russia.

Perchuk E.E. (2002), "Informatization and information security: Philosophical and methodological aspects", [Informatizatsiya i informatsionnaya bezopasnost': Filosofsko-metodologicheskie aspekty:], *Autoref. dis…. Cand. philos. sciences'* [*avtoref. diS…. kand. filos. nauk*], Moscow.

Sharakhina L.V. (2019), "Segmentation of target audiences, use of public opinion leaders, expert brand positioning in the digital space" [Segmentirovanie tselevykh auditorii, ispol'zovanie liderov obshchestvennogo mneniya, ehkspertnoe pozitsionirovanie brenda v tsifrovom prostranstve], *Russian school of public relations* [*Rossiiskaya shkola svyazei s obshchestvennost'yu*], no. 13, pp. 84–92.

TRANSLATION OF FRONT REFERENCES

[1] (2016), Decree of the President of the Russian Federation of December 5, 2016 No. 646 "On approval of the information security Doctrine of the Russian Federation", Collection of laws of the Russian Federation of December 12, 2016, No. 50, article 7074. Available at: http://www.consultant.ru/document/cons_doc_LAW_48601/ (accessed 09.09.2019).

[2] (2004), Federal law of July 27, 2004 No. 79-FZ "On the state civil service of the Russian Federation" (as amended on December 27, 2019)", Federal law of the Russian Federation of August 2, 2004, No. 31 article 3 215. Available at: http://www.consultant.ru/document/cons_doc_LAW_48601/ (accessed 09.09.2019).