УДК 352.071
DOI: 10.31660/1993-1824-2024-1-101-115

Факторы и направления политики обеспечения информационной безопасности России

А. А. Попкова*, К. В. Парфенов

Тюменский индустриальный университет, Тюмень, Россия
**popkovaaa@tyuiu.ru*

Аннотация. Трансформационные процессы, происходящие в обществе, в настоящее время усилили роль информации в обеспечении функционирования государства и поставили обеспечение информационной безопасности в качестве одной из ключевых целей национальной политики. Геополитические аспекты информационного противоборства вышли в стадию когнитивной войны, в которой информационное воздействие направлено в первую очередь на дестабилизацию социально-политических и экономических процессов. Существенную роль в достижении данной цели играют возникновение и распространение недостоверной общественно значимой информации, более известной как фейковая в системе информационного пространства России. Несмотря на разрабатываемые документы политики обеспечения информационной безопасности, которые направлены на предотвращение распространения подобной информации, складывается обратная тенденция — количество фейков и их распространенность растет. Цель исследования — систематизация факторов и направлений политики обеспечения информационной безопасности России и определение значения фейковой информации в выстраивании приоритетов ее реализации. В статье представлен анализ правовых положений политики обеспечения информационной безопасности России, систематизация основных направлений ее реализации, а также вторичный анализ результатов исследования распространения фейковой информации в информационном пространстве государства. Систематизация предложенных факторов позволяет определить условия формирования и реализации эффективной политики обеспечения информационной безопасности в направлении противодействия деструктивному информационному воздействию на граждан.

Ключевые слова: информационная безопасность, политика обеспечения информационной безопасности, фейк, недостоверная общественно значимая информация

Для цитирования: Попкова, А. А. Факторы и направления политики обеспечения информационной безопасности России / А. А. Попкова, К. В. Парфенов. – DOI 10.31660/1993-1824-2024-1-101-115 // Известия высших учебных заведений. Социология. Экономика. Политика. – 2024. – № 1. – С. 101–115.

Factors and directions of information security policy in Russia

Alena A. Popkova*, Konstantin V. Parfenov

Industrial University of Tyumen, Tyumen, Russia
**popkovaaa@tyuiu.ru*

Abstract. The transformational processes taking place in society have now strengthened the role of information in ensuring the functioning of the state and put information security as one of the key objectives of national policy. Geopolitical aspects of information confrontation have entered the stage of cognitive warfare, in which the information impact is primarily aimed at destabilising socio-political and economic processes. The emergence and dissemination of inaccurate information of public importance, commonly referred to as fake news, plays a

significant role in compromising information security within information space of Russia. Although information security policy documents aim to prevent the dissemination of false information, the number of fake news and their prevalence are increasing. The aim of the study is to systematise the factors and directions of information security policy in Russia and to determine the significance of fake news. The article analyses the legal provisions of the policy for ensuring information security in Russia. It systematises the main directions of its implementation and provides a secondary analysis of the results of the study on the spread of fake news in information space of Russia. The proposed factors have been systematised to enable the determination of conditions for the formation and implementation of an effective information security policy. This policy aims to counteract destructive information influence on citizens.

Keywords: information security, information security policy, fake, unreliable socially significant information

For citation: Popkova, A. A., & Parfenov, K. V. (2024). Factors and directions of information security policy in Russia. Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (1), pp. 101-115. (In Russian). DOI: 10.31660/1993-1824-2024-1-101-115

Введение

Развитие информационного общества привело к доминирующей роли информации как в геополитических, так и в политических, экономических и социальных процессах отдельных государств и регионов. Все это потребовало активного вмешательства государства в конструирование информационного пространства, развитие информационных систем и инструментов информационного противоборства, формирования политики обеспечения информационной безопасности.

На сегодняшний день процессы, происходящие в информационной сфере, требуют от государств включения в политическую повестку обеспечения национальной безопасности вопроса информационной безопасности, охватывающей сферу не только функционирования государственных органов и учреждений, крупных экономических субъектов страны, но и обычных граждан, в жизнь которых информационные атаки и угрозы вносят существенный социальный дисбаланс.

По данным Лаборатории Касперского, Российская Федерация (РФ) стабильно занимает первое место по количеству кибератак, которых ежедневно осуществляется более двух миллионов [1]. Количество случаев мошенничества с использованием информационных технологий в 2023 году возросло на 86 %, их доля в общем количестве преступлений в России, по данным Министерства внутренних дел (МВД) РФ, составляет 30 %, а ущерб исчисляется 15 млрд руб. [2; 3]. Количество фейковой информации в информационном пространстве нашей страны за последние два года увеличилось в 8 раз и составило в 2023 году 12,5 млн, а в прогнозе на 2024 год определяется дальнейший рост ссылок на недостоверную информацию до 15 млн. Социальный эффект от данного информационного воздействия усиливается быстрой распространяемостью фейковой информации, только 5 наиболее топовых фейков 2023 года набрали 617,2 млн просмотров [4].

Постоянная трансформация информационной среды, механизмов ее конструирования требует изменения подходов к формированию и реализации политики информационной безопасности. Президент РФ В. В. Путин в 2023 году трижды инициировал заседание Совета Безопасности по вопросам информационной безопасности России с

целью обсуждения вопроса повышения эффективности мер в данной сфере. Оперативное реагирование на возникающие угрозы, формирующийся опыт Российской Федерации в ведении информационного противоборства требуют системного осмысления происходящих процессов и определения стратегических мер, направленных на снижение социальных последствий информационных атак, формирования информационного иммунитета среди населения и постоянного совершенствования политики информационной безопасности не догоняющего, а опережающего характера.

Материалы и методы

Исследование факторов и направлений политики обеспечения информационной безопасности основано, в первую очередь, на теоретико-методологическом анализе базовых категорий, позволившем сформировать понятие политики обеспечения информационной безопасности.

Выделение ключевых направлений реализации политики основано на правовом анализе Доктрин информационной безопасности, принятых в 2000 и в 2016 гг. [5; 6], Стратегии национальной безопасности Российской Федерации [7], Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8], Указа Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [9].

Эмпирическая часть статьи основана на вторичном анализе данных результатов социологических исследований, проведенных Всероссийским центром изучения общественного мнения в 2021–2023 гг. по различным аспектам информационной безопасности [10; 11], а также автономной некоммерческой организацией «Диалог. Регионы» в 2023 году по вопросам распространенности фейковой информации [12].

Результаты и обсуждение

«Развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия» было определено в 2021 году в качестве одного из ключевых национальных интересов России, а информационная безопасность стратегическим национальным приоритетом [7]. Развитие информационно-коммуникационных технологий, противодействие инициативам России в развитии системы международной информационной безопасности, распространение недостоверной и заведомо ложной информации, стремление к выведению из строя объектов критической информационной инфраструктуры государства определило необходимость трансформации действующей политики обеспечения информационной безопасности, целью которой является «укрепление суверенитета России в информационном пространстве».

По мнению Л. А. Кравченко и Д. В. Субоч, информационная безопасность в обществе достигается «проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства» [13].

Рост внимания к данным процессам определяется существенным ростом объема информации, распространяемой и используемой в сети Интернет. По данным Global Business Data Platform Statista поток данных в глобальном Интернете только за последние пять лет вырос более чем в три раза, с 46 600 гигабайт трафика в секунду в 2017 году до 150 700 гигабайт в 2024 году.

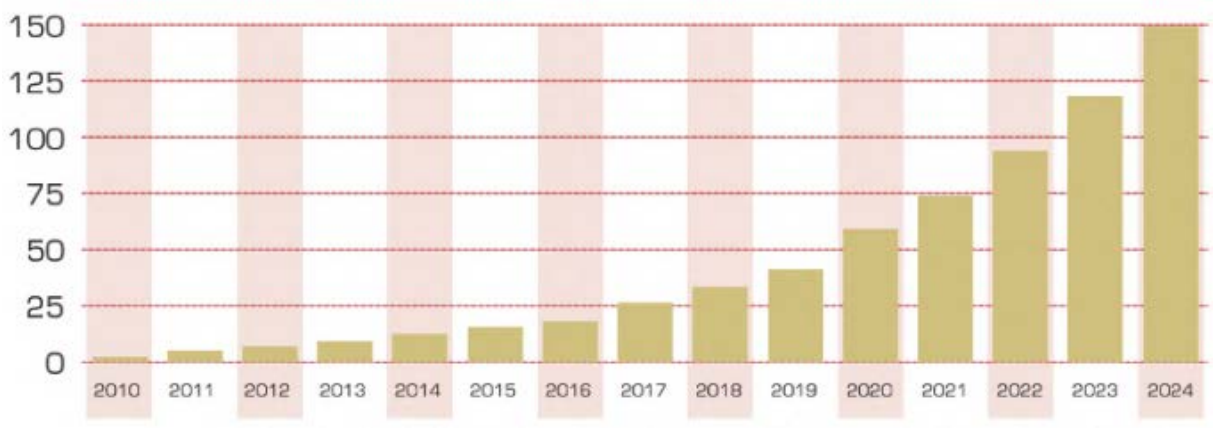

Рис. 1. ***Поток данных в глобальной сети Интернет [14]***

Развитие активности пользователей Сети отмечается и в нашей стране. По результатам исследования, проведенного социологическим агентством «Вебер», на конец 2023 года 93 % граждан РФ ежедневно используют Интернет, более половины из которых тратят на это до 4 часов в день, а 17 % — более 8 часов. Вторичный анализ результатов исследования показывает, что большинство россиян используют Сеть для получения информации о процессах, происходящих в стране и мире (63 %), а также в качестве поискового информационного ресурса (58 %) и коммуникативного пространства для общения (42 %) [14]. Распределение запрашиваемой информации по отраслям показывает, что на первом месте по запросам сфера политики (41 %), социальная сфера (33 %) и сфера международных отношений (31 %). Следовательно, Интернет на сегодняшний день стал информационно-коммуникативной средой, предоставляющей информацию по значимым для россиян вопросам. В связи с этим значимыми являются вопросы о достоверности этих данных, качестве формирования информационного пространства и минимизации рисков негативного информационного воздействия.

Информационная безопасность как объект политического воздействия сформировалась не сейчас, а в эпоху активизации кибервойн, кибермошенничества и тотального производства фейковой информации. В Российской Федерации в 2000 году была принята Доктрина информационной безопасности, определившая под объектом политики обеспечения информационной безопасности «состояние защищенности национальных интересов России в информационной сфере, определяемой совокупностью сбалансированных интересов личности, общества и государства» [5]. Усложнение информационного пространства, его глобализация и повышение значимости информационно-коммуникационных технологий для обеспечения эффективного функционирования

государства, его политической, экономической и социальной системы привело к нарастанию свойств и факторов информационной безопасности как объекта политики — «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [6]. Принятие указа Президента РФ «Об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности» в 2021 году подчеркнуло значимость и признание геополитического фактора в обеспечении информационной безопасности и становлении ее не только в качестве объекта внутренней, но и внешней политики государства [9].

На основе практики реализации политики обеспечения информационной безопасности ее базовые составляющие делятся на два блока:

- информационно-техническая безопасность: защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и др.; защита критических инфраструктур государства;
- информационно-психологическая безопасность: защита психологического состояния общества и государства от негативного информационного воздействия; проблема противостояния фейковым новостям.

Формулируя современное сущностное определение информационной безопасности, можно выделить следующее: под информационной безопасностью понимаются такие информационные условия функционирования объекта, в которых он сохраняет способность и возможность принимать и реализовывать решения в соответствии со своими целями и интересами и способен сопротивляться деструктивному информационному воздействию в интересах других субъектов.

В соответствии с анализом документов, принятых в сфере обеспечения информационной безопасности, можно выделить содержательные характеристики государственной политики обеспечения информационной безопасности как комплекса мер политического, социального, экономического и технического характера, направленных на формирование системы информационной безопасности страны.

Ключевыми направлениями реализации политики обеспечения информационной безопасности на современном этапе являются следующие:

- развитие активной информационной среды для предоставления достоверной информации;
- обеспечение защищенности и устойчивости информационной инфраструктуры государства;
- прогнозирование, выявление, предупреждение, ликвидация угроз информационной безопасности;
- предотвращение негативного информационно-технического воздействия на информационные ресурсы федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного само-

управления, государственных корпораций и учреждений, хозяйствующих субъектов, имеющих важное стратегическое значение;

- выявление, пресечение и предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий;
- защищенность и устойчивость функционирования объектов информационно-коммуникационной инфраструктуры и сфер, обеспечивающих ее деятельность;
- создание условий для снижения рисков утечек информации ограниченного доступа и персональных данных;
- предотвращение ущерба национальной безопасности государства в результате технической разведки иностранных государств;
- защита прав и свобод человека во время обработки персональных данных в информационных системах;
- укрепление информационной безопасности в военной сфере и сфере оборонно-промышленного комплекса;
- совершенствование системы информационного противоборства;
- противодействие деструктивному информационному воздействию на граждан и общество экстремистских и террористических организаций, специальных служб и пропагандистских структур иностранных государств;
- расширение применения технологии искусственного интеллекта при обеспечении информационной безопасности;
- реализация национальных программ проектов в области цифровизации экономики и государственного управления;
- развитие сотрудничества в сфере международной информационной безопасности;
- формирование системы распространения достоверной информации о внутренней и внешней политике России;
- обеспечение взаимодействия органов государственной власти и местного самоуправления и некоммерческих организаций в сфере обеспечения информационной безопасности.

Комплексный подход к формированию и реализации политики обеспечения информационной безопасности позволит обеспечить своевременное реагирование на угрозы, возникающие в информационном пространстве и направленные на дестабилизацию общегосударственных процессов.

Одним из наиболее значимых для общества направлений государственной политики обеспечения информационной безопасности является распространение достоверной информации и противодействие деструктивному информационному воздействию на граждан. Необходимость реализации государственных мер в данной сфере вызвана значительным ростом и распространением недостоверной (фейковой) информации. Сама сущностная природа фейка определяется недостоверностью произведенной информации и вирусном ее распространении с целью воздействия на поведение человека, его ценности и мышление, процессы принятия им решений. Сложность противодействия фейкам заключается в том, что каналы распространения данной информации и

каналы ее опровержения не совпадают, и в большинстве случаев потребитель не включен в систему ее опровержения [15].

Законодательно под категорией фейк определяется недостоверная общественно значимая информация, которая распространяется «под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу возникновения помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи» [16].

Вторичный анализ результатов социологического исследования, проведенного в конце 2023 года автономной некоммерческой организацией «Диалог. Регионы» (квотная выборка, 3 600 респондентов, распределение по полу и возрасту), показывает, что за период с 2021 по 2023 гг. количество создаваемой фейковой информации увеличилось почти в три раза. Темпы вирусного копирования фейков, несмотря на активную политику противодействия распространению подобной информации, растут и по прогнозам продолжат увеличиваться и в 2024 году достигнут 15 миллионов копий одного фейка (рис. 2).

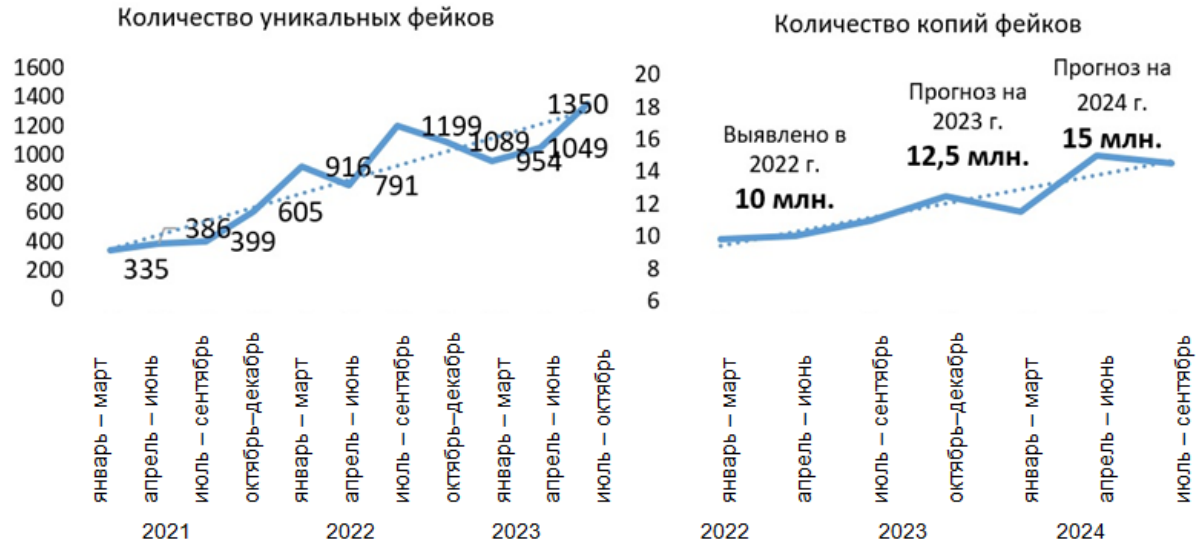

Рис. 2. ***Количество созданных фейков и степень их распространения (копирование) [13]***

Создание фейковой информации является целенаправленным действием, направленным на дезориентацию общества в информационном пространстве посредством разных форм и каналов распространения. Наиболее активно используются механизмы намеренного искажения информации и ложные заявления для деформации объективного понимания происходящего. Для визуального подтверждения и убедительности создаваемой информации активно используются архивные видео и фото, отредактированные для правдоподобности в специализированных программах (рис. 3).

Рис. 3 ***Механизмы появления фейков***

Противодействие созданию и распространению недостоверной информации стало ключевым направлением политики обеспечения информационной безопасности, так как сфера принятия государственных политических решений является наиболее подверженной данным угрозам. По данным исследования, именно вопросы проведения специальной военной операции, политическая сфера и социально значимые происшествия являются лидерами по созданию фейковой информации и ее востребованности среди российской аудитории (рис. 4). Фейковая активность в данных сферах свидетельствует о том, что стремление создателей подобного информационного контента направлена на дестабилизацию в первую очередь общественно-политической жизни общества.

Рис. 4. ***Распределение по тематике и количеству просмотров фейковой информации***

Эффективность фейковых данных определяется не столько созданным информационным продуктом, сколько степенью его проникновения в информационное пространство, достигаемой тиражированием и распространенностью подобной информации по разным каналам. Если в 2022 году среди ключевых каналов распространения фейков доминировали иностранные социальные медиа, то в 2023 году основной объем фейковой информации распространялся в Telegram, Одноклассниках, ВКонтакте и средствах массовой информации.

Существует дифференциация между пользователями и распространителями фейковой информации в нашей стране. Наиболее активно пользуются фейками мужчины в возрасте старше 40 лет. Для данной категории лиц недостоверные данные являются одним из видов информационных материалов, на основе которых они формируют суждения, принимают решения, определяют характер социального поведения.

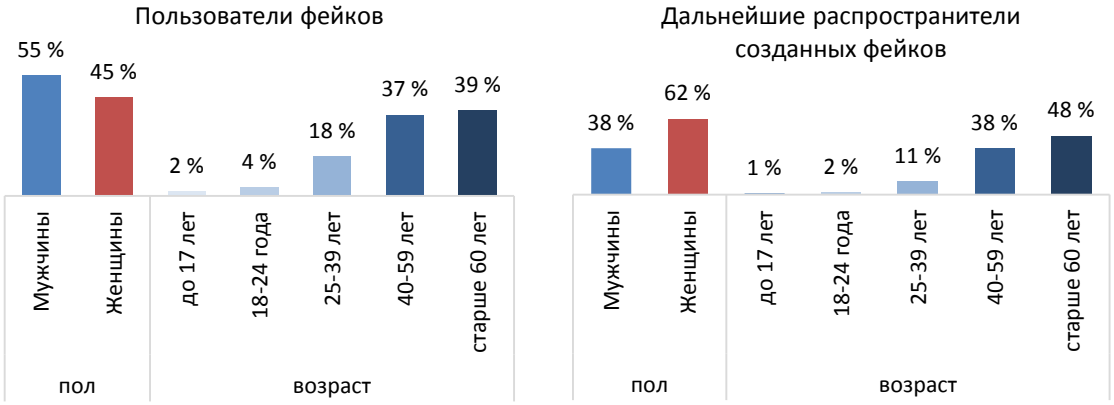

Рис. 5. ***Половозрастная характеристика пользователей и дальнейших распространителей созданных фейков***

В дальнейшем тиражируют фейковую информацию в большинстве женщины старше 40 лет, делясь ей в мессенджерах и увеличивая аудиторию распространения фейков.

Все это происходит на фоне функциональной природы фейков, которую современные исследователи определяют как комплекс задач, ключевой из которых является трансформация информационной повестки с концентрацией на конкретный информационный повод посредством фейковой новости и формирование вокруг него общественного внимания, определяющего социальные тенденции, выступающего в качестве катализатора общественной активности, социальной напряженности, формирующего негативные общественные настроения [17; 18].

Следовательно, активизация политики обеспечения информационной безопасности на современном этапе, одной из задач которой является создание механизмов выявления и опровержения недостоверной информации, является неотъемлемым процессом в деятельности любого государства и его системы национальной безопасности.

Выстраивание эффективной политики обеспечения информационной безопасности происходит в условиях современных социально-технологических и политических трансформаций, вызванных следующими факторами:

1. Технологический фактор — совокупность технологий, имеющих большие возможности по производству и распространению информации. В информационном пространстве на сегодняшний день практически нет барьеров, ограничивающих возможности производства и распространения информации с использованием цифровых технологий для конструирования двойников и профилей, обработки больших массивов данных, применения искусственного интеллекта. Многопрофильность и специфика применения данных технологий развивается такими темпами, что государство не успевает разрабатывать действующие нормы предотвращения формирования недостоверного контента и фактически вырабатывает ответные меры и действия на состоявшиеся факты информационно-психологического воздействия. В результате этого в информационном пространстве накапливается достаточно большой объем фейковой информации, тиражирование которой сложно ограничить, что существенно снижает уровень социального доверия к государству и процессам, происходящим в нем.

2. Реализация информационных прав индивида. Современный человек практически не ограничен в праве генерирования информации вне зависимости от ее природы и отраслевого характера. В современном информационном пространстве индивид имеет право формировать свою позицию относительно общественно-политических и социально-экономических процессов, транслируя ее через комментарии, собственные интерпретации зачастую без привязки к официальным данным и аргументам, определяющим ее достоверность и содержательность. Отсутствие критического мышления и культуры фактчекинга приводит иногда к неосознанному формированию фейков или использованию данного фактора в качестве ключевого для развития вирусности и социально-психологического влияния недостоверной информации в среде массового общественного обсуждения.

3. Субъективность формирования информационного пространства. Наращивание субъективного основания в деятельности индивида в информационном пространстве привело к растворению его в информационной среде, где зачастую он стремится к созданию «идеального» собственного информационного образа, подменяя факты, избегая реальность, конструируя мнимые образы, оторванные от действительности, теряющие смыслы. Это формирует его уязвимость в информационной среде, неспособность осваивать и применять знания и, как следствие, массовое поверхностное восприятие информации. Подобное упрощенное восприятие информации на окружающую действительность способствует проникновению транслируемых конструируемых моделей поведения и достижению целей в политической и экономической среде, которые преследуют создатели и распространители недостоверного контента.

4. Разнообразность подходов к конструированию и распространению недостоверной информации. Результативность воздействия фейковой информации определяется интенсивностью информационного потока ее распространяющего. Первоначальная стадия социального восприятия сконструированной недостоверной информации — это психоэмоциональная реакция, способствующая включенности граждан в поглощение информационного контента, формированию устойчивого образа и соответствующего ему поведения. На фоне высокой скорости и массовости распространения, всепогло-

щающего восприятия фейковой информации политика опровержения, реализуемая со стороны органов государственной власти, не является эффективной.

Таким образом, в современных условиях цифровизации главной целью негативного информационного воздействия является трансформация массового и индивидуального сознания в интересах определенных лиц, организаций государств, что существенным образом подрывает безопасность государства и его граждан. Включенность в информационное пространство всех аспектов жизнедеятельности человека приводит к усложнению государственной политики обеспечения информационной безопасности и ограниченности ее реализации в отдельных направлениях, связанных с личностно-субъективным поведением индивида в информационном пространстве. Постоянная трансформация технологий конструирования информации, ее передачи и распространения не позволяет на сегодняшний день выработать эффективную политику предотвращения ее социально-психологического воздействия на население. Все это используется заинтересованными сторонами для дестабилизации функционирования основных социальных систем через воздействие на личности. Фейковая информация становится неотъемлемой частью информационного пространства, конструирование которой основывается на приемах социальной инженерии, накопленных данных, изменениях структуры информации, способствующих возникновению эффектов массовости распространения, социально-психологической деформации поведения, инертности восприятия официальной информации, снижению функциональной роли государства в конструировании информационного пространства.

Выводы

В трансформационных процессах общественного развития информация приобрела стратегическое значение, определяющее специфику социальных процессов, поведение индивида и социальных групп, развитие государства и его системы управления.

Цифровизация и развитие всесторонних коммуникативных связей привело к тому, что конструирование информационного пространства стало ограниченно регулируемым процессом со стороны органов государственной власти, и в результате в его формирование оказались включены различные заинтересованные субъекты, деятельность которых зачастую направлена на дестабилизацию внутриполитических процессов в России и активное воздействие на массовое сознание граждан.

В этих условиях на протяжении последних десятилетий органами государственной власти РФ ведется поиск эффективных механизмов реализации политики обеспечения информационной безопасности, которая на сегодняшний день включает в себя два основных блока. Первый блок направлен на развитие информационно-технологической независимости управленческих систем различных уровней от возможных киберугроз, нарушений нормального функционирования и способности обработки и передачи данных, снижения рисков их утечки и потери. И это возможно при реализации комплекса мер, направленных на достижение информационно-технологического суверенитета, которые в настоящее время реализуются в Российской Федерации. Второй блок направлен на предотвращение деструктивного воздействия

фейковой информации на общество, социальные группы и личности, которое вызвано активным распространением недостоверной, специально сформированной информации, преследующей цель дестабилизировать социальные процессы в российском обществе. В связи с постоянными изменениями технологий конструирования недостоверного контента меры, предпринимаемые государством, не являются достаточно эффективными и постоянно трансформируются.

Политика обеспечения информационной безопасности имеет стратегическое значение и является одной из ключевых подсистем национальной безопасности государства. Комплекс нормативно-правовых документов, принятых в России, сформировал системный подход к правовому обеспечению национальной безопасности.

Список источников

1. Интерактивная карта киберугроз. – URL: https://cybermap.kaspersky.com/ru/stats (дата обращения: 18.01.2024). – Текст : электронный.

2. Черноусов, И. Фишинговая прямая : число мошеннических сайтов в 2023 году выросло на 86 %. С чем связано увеличение количества таких порталов и почему преступники переносят их за границу / И. Черноусов. – Текст : электронный // Известия : сайт. – 2023. – 27 дек. – URL: https://iz.ru/1625951/ivan-chernousov/ fishingovaia-priamaia-chislo-moshennicheskikh-saitov-v-2023-godu-vyroslo-na-86 (дата обращения: 18.01.2024).

3. МВД РФ сообщило, что мошенники стали применять элементы ИИ при атаках на граждан. – Текст : электронный // Интерфакс : сайт. – 2024. – 15 фев. – URL: https://www.interfax.ru/russia/946188.

4. В России определили главные фейки 2023 года. – Текст : электронный // Регнум : сайт. – 2023. – 22 нояб. – URL: https://regnum.ru/news/3847932 (дата обращения: 11.01.2024).

5. Доктрина информационной безопасности РФ 2000 г. – Текст : электронный // Гарант : сайт. – URL: https://base.garant.ru/182535/?ysclid= lt44vzlhdt965536224 (дата обращения: 13.01.2024).

6. Доктрина информационной безопасности Российской Федерации 2016 г. – Текст : электронный // Гарант : сайт. – URL: https://base.garant.ru/71556224/?ysclid=lt44sifgv346243997 (дата обращения: 13.01.2024).

7. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 2 июля 2021 г. № 400. – Москва, 2021. – URL: https://base.garant.ru/401425792/?ysclid=lt450uou35234098396 (дата обращения: 16.01.2024). – Текст : электронный.

8. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – Москва, 2006. – URL: https://base.garant.ru/12148555/?ysclid= lt4582gmxn515844527 (дата обращения: 16.01.2024) – Текст: электронный.

9. Указ Президента Российской Федерации «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» от 12.04.2021 № 213. – Москва, 2021. – URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 16.01.2024). – Текст: электронный.

10. Абрамов, К. Информационная безопасность россиян в условиях внешних цифровых угроз / К. Абрамов. – Текст : электронный. – URL: https://profi.wciom.ru/fileadmin/file/nauka/prof_conversation/strategii-kiberoborony/2022_04_07_Abramov_kiberbezopasnost.pdf (дата обращения: 05.01.2024).

11. Стратегии кибероборoны : как обеспечить информационную безопасность граждан. – Текст : электронный // ВЦИОМ : сайт. – URL: https://profi.wciom.ru/strategii-kiberoborony/ (дата обращения: 18.01.2024).

12. Число уникальных фейков в сети в 2023 году может достичь 4 тыс. – Текст : электронный // ТАСС : сайт. – 2023. – 22 нояб. – URL: https://tass.ru/obschestvo/19351319?ysclid=lt46h7fzun5629775 (дата обращения: 11.01.2024).

13. Кравченко, Л. А. Государственная политика информационной безопасности / Л. А. Кравченко, Д. В. Субоч. – Текст : непосредственный // Проблемы информационной безопасности социально-экономических систем : Труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 года / Под редакцией О. В. Бойченко. – Симферополь : Крымский федеральный университет им. В. И. Вернадского, 2023. – С. 40–41.

14. Global Business Data Platform Statista – URL: www.statista.com/statistics/631151/wordwide-data-cjllected-by-smart-buildings/и (дата обращения: 17.01.2024). – Текст : электронный.

15. Медиапотребление V2.0. – Текст : электронный // Диалог : сайт. – 2023. – 17 окт. – URL: https://dialog.info/mediapotreblenie-v2-0/ (дата обращения: 25.12.2023).

16. Почепцов, Г. Г. Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях / Г. Г. Почепцов. – Москва : OMIKO, 2019. – 390 с. – (Современные технологии). – Текст : непосредственный.

17. Манойло, А. В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления / А. В. Манойло. – Текст : непосредственный // Вестник Московского университета. Серия 12. Политические науки. – 2019. – № 2. – С. 37–45.

18. Напсо, М. Б. К вопросу о социально-психологических последствиях оборота недостоверной информации в условиях цифровизации / М. Б. Напсо. – DOI 10.25629/HC.2024.01.19. – Текст : непосредственный // Человеческий капитал. – 2024. – № 1 (181). – С. 181–191.

References

1. Interaktivnaya karta kiberugroz. (In Russian). Available at: https://cybermap.kaspersky.com/ru/stats

2. Chernousov, I. (2023). Fishingovaya pryamaya: chislo moshennicheskikh saytov v 2023 godu vyroslo na 86 %. S chem svyazano uvelichenie kolichestva takikh portalov i pochemu prestupniki perenosyat ikh za granitsu. (In Russian). Available at: https://iz.ru/1625951/ivan-chernousov/fishingovaia-priamaia-chislo-moshennicheskikh-saitov-v-2023-godu-vyroslo-na-86

3. MVD RF soobshchilo, chto moshenniki stali primenyat' elementy II pri atakakh na grazhdan. (2024). (In Russian). Available at: https://www.interfax.ru/russia/946188

4. V Rossii opredelili glavnye feyki 2023 goda. (2023). (In Russian). Available at: https://regnum.ru/news/3847932

5. Doktrina informatsionnoy bezopasnosti RF 2000 g. (In Russian). Available at: https://base.garant.ru/182535/?ysclid=lt44vzlhdt965536224

6. Doktrina informatsionnoy bezopasnosti RF 2016 g. (In Russian). Available at: https://base.garant.ru/71556224/?ysclid=lt44sifgv346243997

7. Ukaz Prezidenta RF "O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii" ot 2 iyulya 2021 g. No 400. (In Russian). Available at: https:// base .garant.ru/401425792/?ysclid=lt450uou35234098396

8. Rossiyskaya Federatsiya. Zakony. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: Federal'nyy zakon No 149-FZ. (In Russian). Available at: https://base.garant.ru/12148555/?ysclid=lt4582gmxn515844527

9. Ukaz Prezidenta Rossiyskoy Federatsii "Ob utverzhdenii Osnov gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti" ot 12.04.2021 No 213. (In Russian). Available at: https://base.garant.ru/ 12148555/?ysclid=lt4582gmxn515844527 (In Russian).

10. Abramov, K. Informatsionnaya bezopasnost' rossiyan v usloviyakh vneshnikh tsifrovykh ugroz. (In Russian). Available at: https://profi.wciom.ru/fileadmin/file /nauka/prof_conversation/strategii-kiberoborony/2022_04_07_Abramov_kiberbezopasnost.pdf

11. Strategii kiberoborony: kak obespechit' informatsionnuyu bezopasnost' grazhdan. (In Russian). Available at: https://profi.wciom.ru/strategii-kiberoborony

12. Chislo unikal'nykh feykov v seti v 2023 godu mozhet dostich' 4 tys. (2023). (In Russian). Available at: https://tass.ru/obschestvo/19351319?ysclid=lt46h7fzun5629775

13. Kravchenko, L. A., & Suboch, D. V. (2023). Gosudarstvennaya politika informatsionnoy bezopasnosti. Problemy informatsionnoy bezopasnosti sotsial'no-ekonomicheskikh system. Simferopol, V. I. Vernadsky Crimean Federal University Publ., pp. 40-41. (In Russian).

14. Global Business Data Platform Statista (In English). Available at: www.statista.com/statistics/631151/wordwide-data-cjllected-by-smart-buildings/и

15. Mediapotreblenie V2.0. (2023). (In Russian). Available at: https://dialog.info/mediapotreblenie-v2-0/

16. Pocheptsov, G. G. (2019) Kognitivnye voyny v sotsmedia, massovoy kul'ture i massovykh kommunikatsiyakh. Moscow, OMIKO Publ., 390 p. (In Russian).

17. Manoylo, A. V. (2019). Fake news as a threat to national security and as a tool information management. Moscow University Bulletin, Series 12. Political Sciences, (2), pp. 37-45. (In Russian).

18. Napso, M. B. (2024). On the issue of the socio-psychological consequences of the circulation of unreliable information in the conditions of digitalization. Chelovecheskiy capital, (1(181)), pp.181-191. (In Russian). DOI: 10.25629/HC.2024.01.19

Информация об авторах / Information about the authors

Попкова Алена Анатольевна, кандидат социологических наук, доцент кафедры маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень, popkovaaa@tyuiu.ru, ORCID: https://orcid.org/ 0000-0002-8507-8151

Парфенов Константин Владимирович, аспирант кафедры маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень

Alena A. Popkova, Candidate of Sociology, Associate Professor at the Department of Marketing and Government Administration, Industrial University of Tyumen, popkovaaa@tyuiu.ru, ORCID: https://orcid.org/0000-0002-8507-8151

Konstantin V. Parfenov, Postgraduate at the Department of Marketing and Government Administration, Industrial University of Tyumen

Статья поступила в редакцию 28.02.2024; одобрена после рецензирования 05.03.2024; принята к публикации 18.03.2024.

The article was submitted 28.02.2024; approved after reviewing 05.03.2024; accepted for publication 18.03.2024.