А.П. БОЧАРОВА*

НОВЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ: УСТАНОВКИ ГРАЖДАН ПО ВОПРОСУ ИНФОРМАЦИОННОГО РЕГУЛИРОВАНИЯ В РОССИИ[1]

Аннотация. Эффективность государственной политики по обеспечению кибербезопасности и информационной безопасности напрямую зависит от того, насколько успешно такие меры будут соблюдаться гражданами на национальном уровне. В рамках данного исследования рассматривается влияние когнитивно-рациональных, ценностно-аффективных и социально-демографических факторов на поддержку респондентами проводимой государством политики в сфере информационного регулирования на примере выбранных кейсов регулирования социальных сетей и введения обязательной системы распознавания лиц в общественном транспорте. В ходе исследования применялся факторный опрос (N=395) с использованием виньеток, позволяющих рассмотреть эффекты фреймирования на восприятие респондентами предлагаемых мер. Анализ результатов эксперимента в данном исследовании показал, что фреймирование новостей путем убеждения населения оказать поддержку предложенным мерам в краткосрочном периоде не приводит к росту поддержки мер, в то время как факторы, оказывающие влияние на общественное восприятие, имеют менее изменчивый во времени характер и включают в себя гражданскую идентичность, доверие политической системе и оценку опасности киберугроз. Результаты исследования позволяют нам подтвер-

* **Бочарова Александра Павловна**, аспирант, младший научный сотрудник Международной лаборатории исследований мирового порядка и нового регионализма, Национальный исследовательский университет «Высшая школа экономики» (Москва, Россия), e-mail: apbocharova@hse.ru

[1] Статья подготовлена в рамках консорциума МГИМО МИД России и НИУ ВШЭ из средств гранта на реализацию программы стратегического академического лидерства «Приоритет-2030».

 DOI: 10.31249/poln/2024.02.15

дить гипотезу о прямой связи гражданской идентичности и поддержки рестриктивных мер, а также частично подтвердить предположение о том, что политическое доверие граждан и специфика восприятия киберугроз положительно влияют на поддержку введения мер. Кроме того, был получен интересный результат, связанный с неоднородностью поддержки государственных мер на различных уровнях политического доверия респондентов, что позволяет обозначить дальнейший потенциал исследований общественного восприятия таких мер с учетом доверия политической системе и отдельным политическим акторам (правительству, спецслужбам, армии и т.д.) в России.

Ключевые слова: информационное регулирование; политическая поддержка; информационная безопасность; меры рестриктивного регулирования; дилемма «безопасность или приватность»; восприятие киберугроз.

Для цитирования: Бочарова А.П. Новые аспекты безопасности: установки граждан по вопросу информационного регулирования в России // Политическая наука. – 2024. – № 2. – С. 326–347. – DOI: http://www.doi.org/10.31249/poln/2024.02.15

Введение

Трансформация мирового порядка, связанная с отходом все большего числа международных акторов от принципов глобального либерализма, неизменно ведет к росту сторонников государственно-ориентированного подхода в изучении внешней политики государств и концепции *Realpolitik* [Саймонс, 2023]. В этом контексте особенно важным остается обеспечение безопасности государства и защита его национальных интересов в условиях внешнеполитических кризисов, а также вызовов, которые порождаются нетрадиционными типами угроз. Угрозы государственной безопасности и национальным интересам в киберпространстве остаются особенно острыми и требующими своевременного прогнозирования и противостояния. При этом если всего двадцать лет назад в экспертном поле преобладали мнения «киберлибертарианцев» – сторонников позиционирования киберпространства как *terra nullius*, или сферы, которая не находится под суверенитетом какого-либо государства и которая не должна регулироваться какими-либо международными или внутренними нормами [Khanna, 2018; Chadwick, Howard, 2008], то в настоящее время преобладает позиция о признании распространения государственного суверенитета на эту сферу [Demchak, Dombrowski, 2011; Gomez, Whyte, 2022]. Принцип территориальности в данном случае подразумевает, что государства имеют право регулировать передачу информации

через свои границы и использовать такую информацию на своей территории. В частности, контроль над критической инфраструктурой, защита аппаратного и программного обеспечения, передачи и хранения данных, входящие в сферу кибербезопасности, а также регулирование политического контента в социальных сетях и на интернет-сайтах с целью противостояния терроризму (информационное регулирование) являются непосредственными мерами повышения государственной безопасности и предупреждения информационных угроз и киберугроз.

При этом эффективность государственной политики по обеспечению кибербезопасности и информационной безопасности напрямую зависит от того, насколько успешно такие меры будут соблюдаться гражданами на национальном уровне. Поскольку меры, принимаемые государством в сфере информационной безопасности, в той или иной степени ограничивают свободу граждан, политическая поддержка принимаемых государством ограничительных мер является фактором легитимации информационной политики правительства со стороны населения, а следовательно, важнейшим индикатором эффективности такой политики. При этом гражданин в контексте реализации такой государственной политики напрямую сталкивается с дилеммой «безопасность или приватность»: в данном случае ему предлагается отказаться от части своих свобод и права на приватность в обмен на обеспечение личной и общественной безопасности со стороны государства.

Почему государство заинтересовано в обеспечении политической поддержки подобных ограничительных мер со стороны граждан, если вопрос идет об обеспечении национальных интересов в информационном пространстве? Успех политики по предупреждению внутренних и внешних информационных угроз, в том числе путем введения определенных ограничений на публикацию и хранение данных, отслеживание действий пользователей и т.д., непосредственным образом зависит от того, насколько успешно граждане будут обеспечивать поддержку правительства [McLaren, 2015] и выполнять предписанные меры. Это случается не всегда: так, попытки российского правительства в 2018–2020 гг. блокировать мессенджер Telegram и аналогичные меры иранского правительства по ограничению доступа пользователей к мессенджеру в связи с изначальным отказом П. Дурова предоставлять ключи шифрования службам безопасности, а также информационная

кампания в СМИ и соцсетях против использования мессенджера не увенчались успехом[1] – аудитория в России продолжала активно использовать Telegram, пока в 2020 г. не было принято компромиссное решение снять блокировку Telegram в обмен на выборочное предоставление ключей шифрования по запросу спецслужб [Akbari, Abdulhakov, 2019]. В свою очередь правительство пересмотрело отношение к Telegram с позиции «Не можешь победить – возглавь», вследствие чего к 2022 г. 60% главных политических каналов в Telegram составляли представители власти и проправительственные авторы[2]. Продолжается активное неприятие населением сбора биометрических данных – согласно результатам исследования ВЦИОМа за 2020 г., почти 60% опрошенных россиян выступают против их сбора и хранения[3].

Таким образом, основной вопрос, с которым сталкиваются исследователи при изучении политики национального регулирования информационного пространства в условиях кризисных ситуаций, заключается в следующем: какие факторы оказывают влияние на общественную поддержку государственных мер в сфере информационной безопасности? Иными словами, что в контексте выбора индивида между приватностью своих личных данных, с одной стороны, и личной и общественной безопасностью – с другой, способствует отказу от первого в пользу последнего? В рамках данного исследования будет рассмотрено, как различные когнитивно-рациональные, ценностно-аффективные и социально-демографические факторы влияют на поддержку респондентами проводимой государством политики в сфере информационного регулирования на примере выбранных кейсов.

---

[1] История блокировки Telegram в России // ТАСС. – 2020. – Режим доступа: https://tass.ru/info/8761201 (дата посещения: 15.12.2023).

[2] Токарева М. Meta* с возу — «телеге» легче: как государство приходило в Telegram // РСМД. – 2023. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/meta-s-vozu-telege-legche-kak-gosudarstvo-prikhodilo-v-telegram/ (дата посещения: 15.12.2023).

[3] Персональные данные в Интернете: угроза утечки и как с ней бороться // ВЦИОМ. – 2020. – Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/personalnye-dannye-v-internete-ugroza-utechki-i-kak-s-nei-borotsja (дата посещения: 15.12.2023).

Теоретическая рамка исследования

В каких условиях граждане добровольно отказываются от своей свободы и приватности в пользу безопасности? Исследователи отмечают, что в кризисные периоды люди более склонны добровольно отказываться от части своих фундаментальных прав и свобод в пользу безопасности, которую им призвано обеспечить государство [Davis, Silver, 2004]. На склонность индивида согласиться с ограничительной мерой государства в пользу своей безопасности оказывают влияние как психоэмоциональные факторы, такие как страх, чувство беспомощности [van Der Does et al., 2021], так и когнитивные, направленные на минимизацию рисков путем максимизации собственной безопасности [Theiss-Morse, Barton, 2018]. Учитывая этот факт, государство может формировать определенный дискурс в социальных сетях и СМИ, создающий картину потенциальных угроз государству и обществу в случае непринятия ограничительных мер и направленный на получение политической поддержки со стороны граждан.

Дилемма «свобода или безопасность» является характерной чертой общественного восприятия информационного регулирования, когда граждане становятся перед выбором ограничения определенной части свобод в информационном пространстве для обеспечения государственной безопасности или отказа от политической поддержки подобных мер. Ввиду характера угроз в информационном пространстве для государственного регулирования в этой сфере характерны сложность прогнозирования будущих угроз, а также отсутствие доступа граждан к информации об угрозах вне информации, опубликованной СМИ, что позволяет государству выступать и в роли информанта аудитории, и в роли основного защитника граждан [Snider et al., 2021]. В то же время граждане, решая поддержать ли определенные меры, предпринимаемые правительством с целью обеспечения информационной безопасности, встают перед выбором – так ли высока опасность той или иной угрозы, чтобы пожертвовать частью своей свободы, или нет. Ведь меры, направленные на предотвращение преступности в информационном пространстве, снижают уровень анонимности и уровень доступа к альтернативным источникам информации, а также обеспечивают расширение доступа государства к личным данным пользователей.

Описание выбранных кейсов и гипотезы

В качестве примеров, репрезентирующих общественное восприятие государственной политики информационного регулирования, в данной работе были выбраны два кейса: регулирование контента в социальных сетях, а также введение системы распознавания лиц (*facial recognition system*). Согласно статье 15.1-1 Федерального закона РФ «Об информации, информационных технологиях и о защите информации»[1], в сети «Интернет» должна удаляться информация, «выражающая в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации». В исследовании ВЦИОМ, проведенном в 2021 г., вопрос блокировки аккаунтов в социальных сетях, распространяющих недостоверную или оскорбительную информацию, получил противоречивую оценку: так, половина опрошенных посчитала блокировку недопустимой, в то время как остальные 40% респондентов – прежде всего представители старшего возраста и жители небольших городов – поддержали введение подобной меры[2]. Сбор биометрических данных граждан и их использование в общественном транспорте и при обеспечении общественной безопасности вызывает еще более отрицательную оценку – при крайне низком уровне осведомленности о системе более половины опрошенных россиян настроены нейтрально-отрицательно[3]. Анализ отношения респондентов к введению подобных мер, таким образом, отражает актуальную картину принятых или принимаемых государством мер, направленных на обес-

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации» // Консультант Плюс. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/079aac275ffc6cea954b19c5b177a547b94f3c48/ (дата посещения: 15.12.2023).

[2] Социальные сети и цензура: за и против // ВЦИОМ. – 16 марта. – 2021. – Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-cenzura-za-i-protiv (дата посещения: 15.12.2023).

[3] Делиться биометрическими данными: выгоды и риски // ВЦИОМ. – 4 июля – 2023. – Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/delitsja-biometricheskimi-dannymi-vygody-i-riski (дата посещения: 15.12.2023).

печение общественной и национальной безопасности как в информационном пространстве, так и в традиционных сферах обеспечения безопасности.

Авторы исследований, посвященных восприятию гражданами угроз, сходятся во мнении, что с ростом тяжести угрозы растет политическая поддержка гражданами государственных ограничительных мер. Так, Снайдер и его соавторы в работе «Киберопасности и киберугрозы» [Snider et al., 2021] разделяли киберугрозы на летальные и нелетальные; в ряде работ учитывается срок действия ограничительной меры как фактор согласия или несогласия индивида с предложенной мерой (например: [Chmel et al., 2021; Brouard et al., 2018]). В рамках данной работы мы предлагаем рассмотреть реакцию респондентов на предложенные правительством ограничительные меры на основе разделения всех информационных угроз на угрозы личной безопасности (безопасности самого респондента, его друзей и близких) и угрозы национальной безопасности (безопасности общества, правительства, государства). Эти примеры угроз являются важной частью российского медиадискурса, причем оба сюжета редко встречаются в одном и том же тексте[1].

При анализе влияния политического доверия граждан на политическую поддержку тех или иных действий государства / правительства исследователи выделяют фактор национальной идентичности в качестве одной из ключевых детерминант позитивного отношения респондентов к экономической и политической системе государства. Основными составляющими национальной идентичности являются гражданская идентичность (идентификация индивида с какой-либо страной по признаку гражданства) и этническая идентичность (идентификация на основе этнического родства с другими проживающими на территории страны людьми) (см., например: [Lenard, Miller, 2018]). В фокусе исследований

[1] Примеры такого дискурса можно встретить в статьях: *Катасонов В.* Цифровое зомбирование // Царьград. – 22 декабря. – 2018. – Режим доступа: https://tsargrad.tv/articles/cifrovoe-zombirovanie_175547 (дата посещения: 15.12.2023); Россиянам рассказали о мошеннических схемах в приложениях для знакомств // Лента.ру. – 4 августа. – 2023. – Режим доступа: https://lenta.ru/news/2023/08/04/mshnnk/ (дата посещения: 15.12.2023); *Громова В.* Минцифры объяснило появление на «Госуслугах» данных о месте проживания // РБК. – 4 августа. – 2023. – Режим доступа: https://www.rbc.ru/technology_and_media/04/08/2023/64ccd9379a7947450c9d2186 (дата посещения: 15.12.2023).

восприятия россиянами ограничительной политики в информационном пространстве находится именно гражданская идентичность, поскольку основной дискурс описания информационных угроз конструируется вокруг понятия «россияне»[1]. Идентификация себя с группой по признаку гражданственности становится важным индикатором ассоциации индивида с группой в условиях международного или внутреннего политического противостояния.

Исходя из пункта о влиянии гражданской идентичности на доверие и, как следствие, поддержку государственных мер в сфере информационного регулирования, мы сформулировали следующие гипотезы:

H1. Респонденты с высоким уровнем гражданской идентичности с большей вероятностью поддержат ограничительные меры, чем респонденты с низким уровнем идентичности.

Также мы предполагаем, что, поскольку гражданская идентичность и поддержка правительственных мер имеют прямую корреляцию, респонденты, ощущающие себя россиянами, будут склонны воспринимать угрозы национальной безопасности как наиболее серьезные, чем респонденты с менее выраженной гражданской идентичностью. Это обосновано логикой максимизации собственных рисков при принятии решения о поддержке правительства: респондент, имеющий сильную связь с группой (страной), будет склонен воспринимать угрозы стране такими же опасными, как угрозы личного характера; с другой стороны, респондента с низкой гражданской идентификацией не будет волновать национальный характер угроз, поскольку он будет заинтересован только в обеспечении личной безопасности.

H2. Среди респондентов со слабой гражданской идентичностью, респонденты, получившие информацию об угрозе личной безопасности, с большей вероятностью поддержат государственные рестриктивные меры, чем респонденты, получившие информацию об угрозе национальной безопасности.

---

[1] См., например: Россиян предупредили о мошенничестве с использованием нейросетей» // Lenta.ru. – 8 августа – 2023. – Режим доступа: https://lenta.ru/news/2023/08/08/nrst/(дата посещения: 15.12.2023); Эксперты рассказали о волне кибератак против российских компаний в июле // РБК. – 4 августа. – 2023. – Режим доступа: https://www.rbc.ru/technology_and_media/04/08/2023/64cb9d769a79470a4303c954 (дата посещения: 15.12.2023).

Наконец, когнитивно-рациональный подход к оценке индивидами ограничительных мер государства подразумевает, что если граждане в целом доверяют правительству и, кроме того, воспринимают стоящую на кону проблему как чрезвычайно важную, то они склонны принять более высокий риск – путем предоставления своих личных данных государству – для достижения политической цели, приносящей личную и коллективную выгоду. Высокое доверие приводит к решению сотрудничать с государством, что приводит к политическим выгодам. Однако эта связь всегда зависит от условий: доверяющий должен верить в положительные намерения доверенного лица (т.е. государства) и быть готовым к более высокому риску только в случае, если ожидаемые выгоды высоки. При формулировании четвертой гипотезы мы опираемся на предположение, выдвинутое в исследовании [Trein, Varone, 2023], о том, что:

H3. Респонденты, имеющие высокий уровень политического доверия и считающие киберугрозы наиболее опасными, с большей вероятностью поддержат предложенные меры, чем другие респонденты.

В таблице 1 представлены, таким образом, все выдвинутые гипотезы, а также переменные, находящиеся в фокусе внимания в рамках данной работы.

Таблица 1

Обзор независимых переменных и гипотез

Независимые переменные	**Формулировка гипотез**
H1: Гражданская идентичность	Респонденты с высоким уровнем гражданской идентичностью с большей вероятностью поддержат ограничительные меры, чем респонденты с низким уровнем идентичности.
H2: Эффект взаимодействия (гражданская идентичность и принадлежность к группе)	Среди респондентов со слабой гражданской идентичностью респонденты, получившие информацию об угрозе личной безопасности, с большей вероятностью поддержат государственные рестриктивные меры, чем респонденты, получившие информацию об угрозе национальной безопасности.
H3: Эффект взаимодействия (политическое доверие и оценка киберугроз)	Респонденты, имеющие высокий уровень политического доверия и считающие киберугрозы наиболее опасными, с большей вероятностью поддержат предложенные меры, чем другие респонденты.

Методология и сбор данных

Для проведения исследования в рамках данной работы был выбран экспериментальный метод факторного опроса с использованием виньеток (3*3) (таблица 2). Данный подход обладает рядом преимуществ: во-первых, он позволяет измерить устойчивость доверия респондентов политической системе в условиях получения различной информации об информационных угрозах, что позволяет оценить влияние каждого фактора на зависимую переменную. Во-вторых, явным преимуществом факторного опроса является меньшая подверженность социальной желательности[1] по сравнению с классическими опросными методами, что позволяет частично снять проблему смещения результатов исследования [Григорян, Горинова, 2016]. Наконец, факторный экспериментальный дизайн позволяет воссоздать реальный процесс формирования суждения респондента с учетом различных комбинаций изначально предлагаемой информации [Auspurg, Hintz, 2014].

В рамках данного исследования были собраны опросные данные респондентов с помощью интернет-платформы Яндекс.Толока в количестве 395 наблюдений. Вопросы формально делятся на три группы: первая группа вопросов, включавшая базовые социально-демографические показатели, группа вопросов об осведомленности граждан о рисках в сфере кибербезопасности, вопросы об уровне доверия респондентов политической системе, а также уровне гражданской идентичности, были одинаковыми для всех групп респондентов. Анкета с вопросами представлена в приложении (Приложение 1).

Таблица 2

Матрица дизайна эксперимента

Группа	Чистый эффект	Вмешательство 1	Вмешательство 2
Контрольная группа	Описание введения меры	–	–
Группа 1	Описание введения меры	Описание угрозы личной безопасности	–
Группа 2	Описание введения меры	–	Описание угрозы национальной безопасности

[1] Под эффектом социальной желательности подразумевается поведение респондентов, направленное на желание дать социально одобряемые ответы.

В таблице 3 представлены две виньетки, описывающие меры государственного регулирования с целью минимизации рисков в сфере кибербезопасности – регулирования социальных сетей и введения системы распознавания лиц в общественном транспорте. Так, все группы респондентов получают информацию о планируемой государственной политике по реализации определенной меры в сфере обеспечения кибербезопасности (вводное предложение). Далее группа 1 получает информацию о том, что в случае, если данная мера не будет введена, пострадает личная безопасность граждан; группа 2 получает аналогичную информацию с описанием угрозы национальной безопасности в России. Кроме того, обе экспериментальные группы получают информацию с обоснованием вводимой меры: введение предложенной меры позволит правительству защитить граждан от описанных выше угроз.

Таблица 3

Тексты, предлагаемые респондентам для ознакомления в рамках эксперимента

Вариант 1. **Вводное предложение (всем респондентам):** *В 2024 году в России предлагают ввести блокировку аккаунтов пользователей социальных сетей, распространяющих ложную информацию, оскорбляющую государство и общество.* **Вмешательство 1: описание угрозы личной безопасности** *Эксперты считают, что эта мера необходима для того, чтобы не допустить дезинформации граждан о последних политических и экономических событиях в России и за рубежом.* **Вмешательство 2: описание угрозы национальной безопасности** *Эксперты считают, что такую информацию в социальных сетях зачастую распространяют спецслужбы недружественных стран для подрыва национальной безопасности России.* **Обоснование вводимой меры (всем респондентам):** *Введение предложенной меры позволит правительству защитить граждан от описанных выше угроз.* *Источники:* Сайт Государственной Думы, Lenta.ru[1]

[1] Порочащая информация о гражданах в интернете будет оперативно блокироваться // Сайт Государственной Думы Федерального Собрания Российской Федерации. – 2021. – 24 марта. – Режим доступа: http://duma.gov.ru/news/51054/ (дата посещения: 19.02.2024); *Кадочникова С.* «Никто за нас в интернете не отвечает, кроме нас самих»: в России соцсети обязали блокировать незаконную информацию. Как это отразится на жизни людей? // Lenta.ru. – 2020. – 26 декабря. – Режим доступа: https://lenta.ru/articles/2020/12/26/social_media/ (дата посещения: 19.02.2024).

Продолжение таблицы 3

Вариант 2. **Вводное предложение (всем респондентам):** *В 2024 году в крупных российских городах предлагают ввести оплату проезда в общественном транспорте с помощью функции распознавания лица.* **Вмешательство 1: описание угрозы личной безопасности** *Эксперты крупных российских и международных IT-компаний утверждают, что эта мера необходима для того, чтобы облегчить борьбу с мелким мошенничеством в транспорте, а также быстрее находить находящихся в розыске преступников.* **Вмешательство 2: описание угрозы национальной безопасности** *Эксперты крупных российских и международных IT-компаний утверждают, что отсутствие системы слежения за перемещениями граждан может привести к росту террористических актов в общественном транспорт из-за невозможности отслеживания подозрительных лиц.* **Обоснование вводимой меры (всем респондентам):** *Введение предложенной меры позволит правительству защитить граждан от описанных выше угроз.* (Источник: Царьград[1])	
Вопрос после виньеток	
Поддерживаете ли Вы введение данной меры?	1. абсолютно поддерживаю 2. скорее поддерживаю 3. скорее не поддерживаю 4. абсолютно не поддерживаю 5. затрудняюсь ответить

Результаты

Подробное описание используемых переменных в исследовании представлено в приложении 2. Зависимые переменные – поддержка введения блокировки аккаунтов в социальных сетях и введение функции распознавания лиц в общественном транспорте – измерялись по шкале от −2 до 2, где −2 – «абсолютно не поддерживаю» введение меры, −1 – «скорее не поддерживаю», 1 – «скорее поддерживаю», 2 – «абсолютно поддерживаю», 0 – «затрудняюсь ответить». Описательная статистика зависимых переменных представлена в таблице 4.

Из представленных в таблице данных видно, что распределение мнений респондентов по выбранным темам неодинаково: так, более 60% респондентов полностью или частично поддержали блокировку аккаунтов пользователей социальных сетей, распространяющих ложную информацию, оскорбляющую государство и

[1] *Ильин И.* Недалекое будущее: вход в московское метро по FACE ID // Царьград. – 2019. – Режим доступа: https://tsargrad.tv/articles/nedalekoe-budushheevhod-v-moskovskoe-metro-po-face-id_194707 (дата посещения: 25.01.2024).

общество. При этом почти вдвое меньший процент респондентов – около 38% – полностью или частично поддержали предложение ввести функцию распознавания лиц в общественном транспорте. Вдвое выше и процент тех, кто абсолютно против введения последней меры – 22,3% против 11,6% в случае блокировок соцсетей. В целом полученная картина позволяет подтвердить противоречивость восприятия политики по сбору и использованию биометрических данных среди россиян – в отличие от ряда других мер, направленных на обеспечение общественной безопасности и тем или иным способом ограничивающих анонимность граждан, использование функций распознаваний лица продолжает не приниматься значительной частью общества.

Таблица 4

Отношение респондентов к введению предложенных мер по обеспечению безопасности

Блокировка аккаунтов в социальных сетях	Абсолютно поддерживаю	36,4%
	Скорее поддерживаю	29,1%
	Скорее не поддерживаю	14,4%
	Абсолютно не поддерживаю	11,6%
	Затрудняюсь ответить	8,5%
Введение функции распознавания лиц в общественном транспорте	Абсолютно поддерживаю	12,4%
	Скорее поддерживаю	25,8%
	Скорее не поддерживаю	27,6%
	Абсолютно не поддерживаю	22,3%
	Затрудняюсь ответить	11,9%

В таблице 5 представлены результаты регрессионного анализа для проверки обозначенных в теоретической части исследования гипотез. Модели 1 и 2, показывающие влияние фактора гражданской идентичности на уровень поддержки мер по регулированию социальных сетей (SM) и использованию функции распознавания лиц в общественном транспорте (FR), позволяют на основе представленных данных подтвердить гипотезу о сильном положительном эффекте фактора гражданской идентичности на уровень поддержки мер: так, коэффициент переменной в модели 1 равен 0,835, в модели 2 равен 0,509. Таким образом, мы можем подтвердить, что в предложенных кейсах высокий показатель ощущения респондентом принадлежности к России действительно оказывает влияние на высокую поддержку рестриктивных мер, что

подтверждает более ранние исследования авторов информационной политики в других странах [Mužík, Šerek, 2021; Sekerdej, Kossowska, 2011].

Таблица 5

Факторы политической поддержки государственных мер регулирования информационного пространства: результаты регрессионного анализа

	Модель 1_SM	**Модель 2_FR**	**Model3_SM**	**Model 4_FR**
Переменные				
Индекс гражданской идентичности	**0,835*** (0,007)**	**0,509*** (0,077)**		
Уровень политического доверия			**0,695*** (0,078)**	**0,499*** (0,084)**
Уровень восприятия киберугроз			**0,495** (0,19)**	**0,5* (0,205)**
Уровень политического доверия / уровень восприятия киберугроз			**−0,134* (0,054)**	**−0,138* (0,058)**
Описание угрозы личной безопасности	−0,154 (0,151)	0,216 (0,166)	−0,116 (0,156)	0,252 (0,167)
Описание угрозы национальной безопасности	−0,124 (0,155)	0,057 (0,17)	0,006 (0,158)	0,167 (0,17)
Пол (м)	**−0,243* (0,12)**	−0,1 (0,132)	−0,156 (0,124)	−0,053 (0,133)
Возраст	**0,016** (0,005)**	0,00 (0,006)	**0,028*** (0,005)**	0,009 (0,006)
Уровень образования	**−0,13* (0,053)**	**−0,16** (0,059)**	**−0,116* (0,055)**	**−0,15* (0,06)**
Уровень дохода	**0,161* (0,065)**	**0,167* (0,171)**	**0,147* (0,067)**	**0,158* (0,072)**
Городское население	0,074 (0,233)	0,145 (0,257)	0,136 (0,24)	0,203 (0,258)
Константа	−0,539	−0,756	−2,849	−2,484
Количество наблюдений	395	395	395	395

Стандартные ошибки в скобках
*** $p < 0,01$, ** $p < 0,05$, * $p < 0,1$*

При этом можно заметить, что во всех приведенных выше моделях коэффициенты принадлежности к экспериментальным группам, получившим информацию об угрозах личного и национального характера, остаются статистически незначимыми. Незначимость эффекта фреймирования в эксперименте с виньетками в различных группах позволяет нам сделать важное предположение о том, что политические установки респондентов по вопросам под-

держки таких мер, как регулирование социальных сетей или распознавание лиц в общественных местах, являются устойчивыми и не меняющимися в краткосрочном периоде. Мы не можем, таким образом, на основании собранных данных подтвердить гипотезу 2, но делаем вывод о том, что позиция респондентов носит когнитивно-рациональный характер, она не ситуативна, а достаточно устойчива, и для изменения мнений индивидов по таким вопросам необходимо работать с относительно постоянными факторами гражданской идентичности, обеспокоенности по поводу хранения и передачи данных (*privacy concerns*) и доверия политической системе в целом и отдельным политическим институтам.

Наконец, обращаясь к гипотезе 3, мы предполагали, что в моделях будет наблюдаться положительные и статистически значимые коэффициенты переменных политического доверия (общий) и восприятия киберугроз. Кроме того, мы ожидали, что респонденты, имеющие высокий уровень политического доверия и считающие киберугрозы наиболее опасными, с большей вероятностью поддержат предложенные меры, чем другие респонденты (то есть коэффициент перед переменной взаимодействия политического доверия и оценки киберугроз также будет положительным и статистически значимым). Результаты регрессионного анализа позволяют частично подтвердить наши предположения: так, коэффициенты перед переменной политического доверия положительны и статистически значимы в моделях 3 и 4 (0,695 и 0,499, соответственно); коэффициенты перед переменной уровня восприятия киберугроз также положительны и статистически значимы (0,495 и 0,5 в моделях 3 и 4). При этом коэффициент перед переменной взаимодействия политического доверия и восприятия киберугроз имеет статистическую значимость, но является отрицательным также в обеих моделях (−0,134 и −0,138, соответственно).

На рис. 1 изображены графики предсказанной вероятности поддержки государственных мер в зависимости от оценки киберугроз на различных уровнях политического доверия респондентов. На левой части двух графиков показана устойчивая тенденция к росту уровня поддержки мер индивидов с низкими и средними показателями политического доверия при увеличении оценки серьезности киберугроз. Мы опираемся на ранее высказанное предположение о том, что, сталкиваясь с угрозой, которая, по мнению респондента, может нанести непоправимый вред личной или

общественной безопасности, индивид приходит к выводу о том, что в текущей ситуации логичнее и безопаснее довериться государству как «наименьшему из двух зол»: страх перед взломом или утечкой данных, например, велик настолько, что безопаснее доверить противостояние этим угрозам государству, что подтверждает предыдущие исследования дилеммы «безопасность или приватность» [Guo, Habich-Sobiegalla, Kostka, 2023]. Интересная закономерность сохраняется при анализе предсказанной поддержки мер среди респондентов с высоким уровнем политического доверия: в отличие от наших изначальных предположений о росте поддержки мер среди респондентов, доверяющих государству и считающих киберугрозы серьезными и опасными, прогнозируемая поддержка мер с ростом оценки серьезности угроз падает. Мы предполагаем, что это может быть связано с аффективной оценкой респондентами киберугроз в связи с предыдущим опытом восприятия фреймирования угроз в СМИ: возможно, логика восприятия строится на установке о том, что киберугрозы представляют опасность для индивида и общества, но государство и так справляется с ними достаточно успешно, чтобы вводить новые меры по предупреждению и ликвидации рисков. Дальнейшее более углубленное изучение предыдущего опыта граждан по столкновению с угрозами в информационном пространстве, их восприятие и интерпретация, позволят точнее интерпретировать данный феномен.

Таким образом, результаты исследования позволяют нам подтвердить гипотезу о прямой связи гражданской идентичности и поддержки рестриктивных мер, а также частично подтвердить предположение о том, что политическое доверие граждан и специфика восприятия киберугроз положительно влияют на поддержку введения мер. При этом в рамках данного эксперимента не удалось подтвердить гипотезу 2 о влиянии различных типов фреймирования угроз на поддержку граждан, так как установки респондентов оказались устойчивы к изменению вмешательств в ходе эксперимента. Кроме того, был получен интересный результат, связанный с неоднородностью поддержки государственных мер на различных уровнях политического доверия респондентов, что позволяет обозначить дальнейший потенциал исследований общественного восприятия таких мер с учетом доверия политической системе и отдельным политическим акторам (правительству, спецслужбам, армии и т.д.) в России.

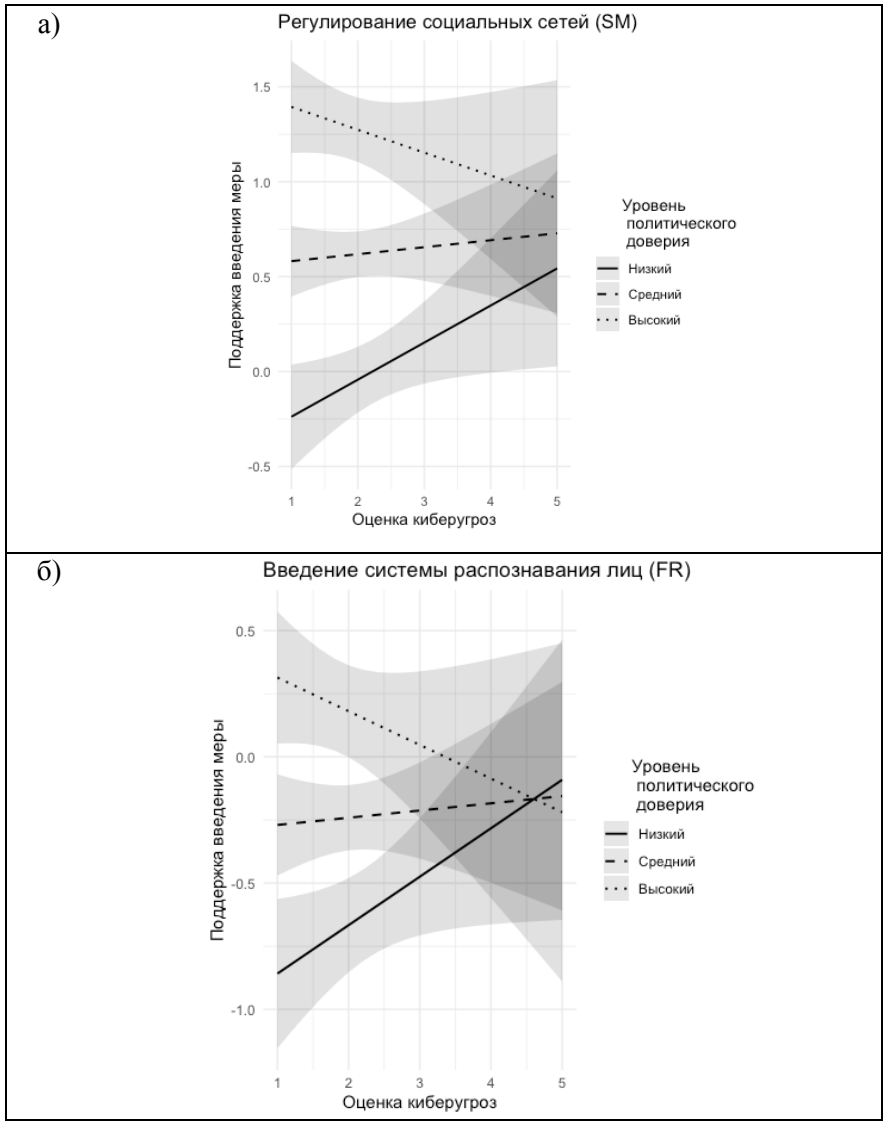

Рис. 1 а), б)

Графики предсказанной вероятности поддержки государственных мер в зависимости от оценки киберугроз на различных уровнях политического доверия респондентов

Заключение

Современные дискуссии об изменениях мирового порядка, трансформации роли государственных акторов и национальной безопасности неизменно связаны с такими темами, как развитие информационной безопасности и обеспечение национальной безопасности в кибер- и информационном пространстве [Bordachev, 2021]. При растущем числе региональных и глобальных конфликтов, в том числе военного характера, неизбежно возникают риски и угрозы для суверенитета государств в информационном пространстве. Россия, Китай, другие страны, не согласные с восприятием информационного пространства как единой системы с отсутствием государственных барьеров и минимизацией регулирования среды, все больше стремятся оградить собственное информационное пространство от внешнего вмешательства, обеспечив национальную безопасность.

При этом при обеспечении национальной безопасности решающим фактором остается уровень эффективности соблюдения мер по обеспечению кибер- и информационной безопасности гражданами. Эта проблема характерна и для России: высокий уровень непринятия предлагаемых мер со стороны граждан, вкупе с недостаточно четко прописанной процедурой правоприменения рестриктивных мер, в том числе блокировки контента в социальных сетях и сбора биометрических данных, вынуждают власти использовать либо инструменты фреймирования, направленные на убеждение аудитории через СМИ о необходимости соблюдения таких мер ради личной и общественной безопасности, либо отменять обязательность введения меры с целью минимизации протестов со стороны граждан[1]. Важной причиной несогласия граждан предоставлять свои личные данные является крайне низкий уровень защиты данных компаниями и банками – так, за 2022–2023 годы количество утечек данных российских компаний увеличилось в разы, в том числе популярных платформ «Яндекс.Еда», СДЭК, Delivery Club, что говорит не только об увеличении угроз в российском информационном пространстве,

[1] Собирать биометрию без согласия не будут // Минцифры России. – 9 августа 2022. – Режим доступа: https://digital.gov.ru/ru/events/41802/?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата посещения: 15.12.2023).

но и халатности компаний по защите личных данных пользователей, особенно учитывая минимальные штрафы в десятки тысяч рублей, из-за которых компании легче выплатить штраф, чем увеличивать затраты на защиту данных[12].

Анализ результатов эксперимента в данном исследовании показал, что фреймирование новостей путем убеждения населения оказать поддержку предложенным мерам в краткосрочном периоде не приводит к росту поддержки, так как факторы, оказывающие влияние на общественное восприятие мер, имеют менее изменчивый во времени характер и включают в себя гражданскую идентичность, доверие политической системе и оценку опасности киберугроз. Мы полагаем, что государственные меры, направленные на обеспечение защиты данных граждан и ужесточение ответственности за утечки данных, а также более точно прописанный процесс правоприменения в контексте регулирования политического контента, могут повлиять на общественное восприятие мер информационного регулирования, а значит, на эффективность обеспечения информационной политики в целом.

[1] Количество утечек в крупных компаниях выросло в 1,5 раза // Ведомости. – 12 мая 2023. – Режим доступа: https://www.vedomosti.ru/technology/articles/2023/05/12/974660-kolichestvo-utechek-dannih-v-krupnih-kompaniyah-viroslo (дата посещения: 15.12.2023).

[2] Сервис «Туту» оштрафован за утечку данных пользователей // Tadviser. – 2023. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A8%D1%82%D1%80%D0%B0%D1%84%D1%8B_%D0%B7%D0%B0_%D1%83%D1%82%D0%B5%D1%87%D0%BA%D1%83_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#.D0.A1.D0.B5.D1.80.D0.B2.D0.B8.D1.81_.C2.AB.D0.A2.D1.83.D0.A2.D1.83.C2.BB_.D0.BE.D1.88.D1.82.D1.80.D0.B0.D1.84.D0.BE.D0.B2.D0.B0.D0.BD_.D0.B7.D0.B0_.D1.83.D1.82.D0.B5.D1.87.D0.BA.D1.83_.D0.B4.D0.B0.D0.BD.D0.BD.D1.8B.D1.85_.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D1.82.D0.B5.D0.BB.D0.B5.D0.B9 (дата посещения: 15.12.2023).

A.P. Bocharova*

New aspects of security: citizens' attitudes towards the issue of information regulation in Russia[1]

Abstract. The effectiveness of government policies to ensure cyber- and information security directly depends on how successfully such measures are followed by citizens at the national level. The author considers the influence of cognitive-rational, value-affective, and socio-demographic factors on respondents' support for government policy in the field of information regulation through selected cases of regulating social networks and introducing a mandatory face recognition system in public transport. In the course of the study, a factorial survey (N=395) was conducted using vignettes to examine the effects of framing on respondents' perception of the measures proposed. The analysis of the experimental results in this study shows that news framing to persuade the population to support the proposed measures does not lead in the short term to an increase in support for the measures. However, certain factors influencing public perception, such as civic identity, trust in the political system, and assessment of cyber threats danger, show less variability over time. The results of the study allow us to confirm the hypothesis of a direct connection between civic identity and support for restrictive measures, as well as partially confirm the assumption that the political trust of citizens and the specifics of perception of cyber threats positively influence support for the introduction of measures. In addition, the heterogeneity of support for government measures at various levels of political trust of respondents was revealed, therefore we can identify the further potential of research on public perception of such measures taking into account trust in the political system and individual political actors (government, special services, army, etc.) in Russia.

Keywords: information regulation; political support; information security; restrictive regulation measures; "security vs privacy" dilemma; perception of cyber threats.

For citation: Bocharova A.P. New aspects of security: citizens' attitudes on the issue of information regulation in Russia. *Political science (RU).* 2024, N 2, P. 326–347. DOI: http://www.doi.org/10.31249/poln/2024.02.15

References

Akbari A., Gabdulhakov R. Platform surveillance and resistance in Iran and Russia: the case of Telegram. *Surveillance & Society*. 2019, N 17 (1/2), P. 223–231. DOI: https://doi.org/10.24908/ss.v17i1/2.12928

* **Bocharova Alexandra,** HSE University (Moscow, Russia), e-mail: apbocharova@hse.ru

[1] The article was prepared within the consortium of MGIMO University and HSE University and funded by the grant for the implementation of the Priority 2030 Strategic Academic Leadership Program

Auspurg K., Hinz T. *Factorial survey experiments*. Los Angeles: Sage Publications, Inc., 2014, 168 p. DOI: https://doi.org/10.4135/9781483398075

Bordachev, T. *Europe, Russia and the liberal world order: international relations after the cold war*. London, New York: Routledge, 2021, 209 p.

Brouard S., Vasilopoulos P., Foucault M. How terrorism affects political attitudes: France in the aftermath of the 2015–2016 attacks. *West European politics*. 2018, N 41 (5), P. 1073–1099. DOI: https://doi.org/10.1080/01402382.2018.1429752

Chadwick A., Howard P. *Routledge handbook of internet politics.* London: Routledge, 2009, 487 p. DOI: https://doi.org/10.4324/9780203962541-30

Chmel K., Marques II I., Mironyuk M., Rosenberg D., Turobov A. *Privacy versus security in trying times: evidence from Russian public opinion*. Higher School of Economics. Series WP BRP 82/PS/2021 "Higher School of Economics Research Paper". 2021. DOI: https://doi.org/10.2139/ssrn.3975380

Davis D.W., Silver B.D. Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American journal of political science*. 2004, Vol. 48, № 1, P. 28–46. DOI: https://doi.org/10.2307/1519895

Demchak C., Dombrowski P. Rise of a cybered Westphalian age. *Strategic studies quarterly*. 2011, Vol. 5, N 1, P. 32–61. DOI: https://doi.org/10.1007/978-3-642-55007-2_5

Gomez M.A., Whyte C. Unpacking strategic behavior in cyberspace: a schema-driven approach. *Journal of cybersecurity*. 2022, Vol. 8, N 1. DOI: https://doi.org/10.1093/cybsec/tyac005

Grigoryan L.K., Gorinova E.V. Factor survey: advantages, scope of application, practical recommendations. *Social psychology and society*. 2016, N 7(2), P. 142–157. (In Russ.)

Guo D., Habich-Sobiegalla S., Kostka G. Emotions, crisis, and institutions: Explaining compliance with COVID-19 regulations. *Regulation & Governance*. 2023. DOI: https://doi.org/10.1111/rego.12509

Khanna P. State sovereignty and self-defence in cyberspace. *BRICS Law journal.* 2018, N 5 (4), P. 139–154. DOI: https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Lenard P.T., Miller D. Trust and National Identity. In: Uslaner E.M. (ed.). *The Oxford handbook of social and political trust*. Oxford university press, 2018. DOI: https://doi.org/10.1093/oxfordhb/9780190274801.013.36

McLaren L. *Immigration and perceptions of national political systems in Europe*. Oxford: Oxford university press, 2015. DOI: https://doi.org/10.1093/acprof:oso/9780198739463.001.0001

Mužík M., Šerek J. What reduces support for civil liberties: Authoritarianism, national identity, and perceived threat. *Analyses of social issues and public policy.* 2021, N 21 (1), P. 734–760. DOI: https://doi.org/10.1111/asap.12241

Sekerdej M., Kossowska M. Motherland under attack! Nationalism, terrorist threat, and support for the restriction of civil liberties. *Polish psychological bulletin*. 2011, N 42 (1), P. 11–19. DOI: https://doi.org/10.2478/v10059-011-0003-0

Simons G. A turn towards realism. *Russia in global affairs*. 2023. Mode of access: https://globalaffairs.ru/articles/povorot-k-realizmu/ (accessed: 15.12.2023) (In Russ.)

Snider K.L., Shandler R., Zandani S., Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of cybersecurity*. 2021, N 7, P. 1–11. DOI: https://doi.org/10.1093/cybsec/tyab019

Theiss-Morse E., Barton D.-G. Emotion, cognition, and political trust. In: Zmerli S., Van der Meer T. W. (eds.). *Handbook on political trust*. UK: Edward Elgar Publishing, 2007, P. 160–175. DOI: https://doi.org/10.4337/9781782545118.00021

Trein P., Varone F. Citizens' agreement to share personal data for public policies: trust and issue importance. *Journal of European public policy*. 2023, P. 1–26. DOI: https://doi.org/10.1080/13501763.2023.2205434

van Der Does R., Kantorowicz J., Kuipers S., Liem M. Does terrorism dominate citizens' hearts or minds? The relationship between fear of terrorism and trust in government. *Terrorism and Political Violence*. 2021, Vol.33, № 6, P. 1276–1294. DOI: https://doi.org/10.1080/09546553.2019.1608951

Литература на русском языке

Григорян Л.К., Горинова Е.В. Факторный опрос: преимущества, область применения, практические рекомендации // Социальная психология и общество. – 2016. – № 7(2). – С. 142–157.

Саймонс Г. Поворот к реализму // Россия в глобальной политике. – 2023. – Режим доступа: https://globalaffairs.ru/articles/povorot-k-realizmu/ (дата посещения: 15.12.2023).

ПРИЛОЖЕНИЯ

Приложение 1

Анкета для проведения опросного эксперимента. – Режим доступа: https://doi.org/10.7910/DVN/GSB75E (дата посещения: 25.01.2024).

Приложение 2

Описание переменных, используемых в исследовании. – Режим доступа: https://doi.org/10.7910/DVN/GSB75E (дата посещения: 25.01.2024).