DOI: 10.14515/monitoring.2026.2.3117

Р. А. Щербаков

ИНДИВИДУАЛЬНЫЕ ПРАКТИКИ КИБЕРБЕЗОПАСНОСТИ: СВЯЗЬ С СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМ СТАТУСОМ И ОПЫТОМ ПЕРЕЖИВАНИЯ РИСКОВ

Правильная ссылка на статью:
Щербаков Р. А. Индивидуальные практики кибербезопасности: связь с социально-экономическим статусом и опытом переживания рисков // Мониторинг общественного мнения: экономические и социальные перемены. 2026. № 2. С. 216—235. https://www.doi.org/10.14515/monitoring.2026.2.3117.

For citation:
Shcherbakov R. A. (2026) Individual Cybersecurity Practices: Relationship with Socioeconomic Status and Risk Experience of Risk Exposure. *Monitoring of Public Opinion: Economic and Social Changes.* No. 2. P. 216–235. https://www.doi.org/10.14515/monitoring.2026.2.3117. (In Russ.)

Получено: 02.10.2025. Принято к публикации: 18.02.2026.

DOI: 10.14515/monitoring.2026.2.3117

ИНДИВИДУАЛЬНЫЕ ПРАКТИКИ КИБЕРБЕЗОПАСНОСТИ: СВЯЗЬ С СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМ СТАТУСОМ И ОПЫТОМ ПЕРЕЖИВАНИЯ РИСКОВ

ЩЕРБАКОВ Роман Андреевич — аспирант, стажер-исследователь Лаборатории исследований науки и технологий, Институт статистических исследований и экономики знаний, Национальный исследовательский университет «Высшая школа экономики», Москва, Россия
E-MAIL: rashcherbakov@hse.ru
https://orcid.org/0000-0002-5054-3869

Аннотация. Цель исследования состояла в выявлении факторов, связанных с использованием россиянами практик кибербезопасности. В качестве факторов рассматривались социально-экономический статус (пол, возраст, наличие высшего образования, тип поселения и материальное положение), а также опыт столкновения с цифровыми рисками и связанная с ним обеспокоенность приватностью в сети. Эмпирической базой послужили данные Мониторинга цифровой трансформации экономики и общества Института статистических исследований и экономики знаний НИУ ВШЭ за 2024 г. ($N = 10\,038$). Практики кибербезопасности были разделены на две группы: инструментальные — простые действия, такие как установка паролей и использование биометрической идентификации, и стратегические — более сложные меры, включающие управление доступом к данным и настройку параметров безопасности. Анализ показал, что около пятой части населения вовсе не использует меры защиты, тогда как примерно половина сочетает инструментальные и стратегические практики. Социально-экономический статус в большей степени связан с использованием стратегических практик по сравнению с инструментальными. Кроме того, именно в отношении

INDIVIDUAL CYBERSECURITY PRACTICES: RELATIONSHIP WITH SOCIOECONOMIC STATUS AND RISK EXPERIENCE OF RISK EXPOSURE

Roman A. SHCHERBAKOV[1] *— Doctoral Student; Research Assistant, Laboratory for Science and Technology Studies, Institute for Statistical Studies and Economics of Knowledge*
E-MAIL: rashcherbakov@hse.ru
https://orcid.org/0000-0002-5054-3869

[1] HSE University, Moscow, Russia

Abstract. The aim of this study is to identify factors related to the use of cybersecurity practices among the Russian population. The author considers factors such as socioeconomic status (gender, age, higher education, type of settlement, and financial situation) and experience of exposure to digital risk (the fact of being exposed to risks and declared concerns about online privacy). The empirical basis of the study is data from the Monitoring of the Digital Transformation of the Economy and Society, 2024 ($N = 10\,038$) conducted by Institute for Statistical Studies and Economics of Knowledge (ISSEK) at HSE University. Cybersecurity practices were divided into two groups: instrumental — simple actions such as setting passwords and using biometric identification, and strategic — more complex actions such as managing access to data and adjusting security settings. The analysis showed that about one-fifth of the population does not use any protective practices at all, while about half combine simple and complex ones. At that, socioeconomic status has stronger relation to the choice of strategic practices in comparison with instrumental practices. In addition, concern about online privacy is significantly related only to complex practices. Experience of digital risks is a significant predictor of both simple and complex practices. The results sug-

DOI: 10.14515/monitoring.2026.2.3117

стратегических практик была зафиксирована положительная связь с обеспокоенностью приватностью в интернете. Опыт столкновения с киберрисками оказался значимым предиктором использования как инструментальных, так и стратегических практик. Полученные результаты позволяют предположить, что рефлексивное поведение в цифровой среде формируется на основе индивидуального опыта столкновения с рисками, тогда как выбор стратегий защиты зависит от объема материальных и культурных ресурсов. Таким образом, рефлексивность в отношении цифровых рисков может рассматриваться как одно из измерений социального неравенства.

Ключевые слова: риски цифровизации, кибербезопасность, практики противостояния рискам, цифровизация, цифровое неравенство, рефлексивное поведение

Благодарность. Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ (HSE-BR-2025-018).

gest that reflective behavior in the digital environment is formed by individual experiences of risk, while the choice of strategies for protection depends on the amount of material and cultural resources. Therefore, reflectivity towards digital risks can be considered as one of the dimensions of social inequality.

Keywords: digitalization risks, cybersecurity, risk mitigation practices, digitalization, digital divide, reflexive behavior

Acknowledgments. This article is an output of a research project HSE-BR-2025-018 implemented as part of the Basic Research Program at HSE University.

Введение

Цифровизация — это использование оцифрованной информации в различных процессах, а также трансформация социально-экономической среды под влиянием данного процесса [Gradillas, Thomas, 2025]. За последние десятилетия цифровизация охватила почти все сферы жизни, в результате чего цифровые технологии стали неотъемлемой частью быта большей части населения мира. Согласно данным Международного союза электросвязи (МСЭ), в 2025 г. более половины мирового населения (74%) пользовалась интернетом, владела мобильным телефоном (82%) или проживала в зоне покрытия высокоскоростного интернета (93%)[1].

Такое масштабное распространение цифровых технологий преобразовывает социальную реальность. С одной стороны, цифровые технологии дают пользователям много преимуществ — более быструю и гибкую коммуникацию, облегченный доступ к информации, больше возможностей для развлечений, образования и проч. С другой стороны, цифровизация связана и с определенными рисками для общества [Lupton, 2016]. К примерам такого воздействия можно отнести раз-

[1] Statistics // ITU. URL: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx (дата обращения: 08.04.2026).

DOI: 10.14515/monitoring.2026.2.3117

личные виды прямых рисков — интернет-зависимость и риски кибербезопасности, включая киберпреступления. При этом риски, связанные с цифровыми технологиями, могут быть непрямыми и иметь отложенные эффекты. К ним можно отнести цифровое неравенство, которое выражается в негативном изменении социального статуса из-за неравного доступа к технологиям или недостатка в навыках по их использованию.

Прямые риски, в частности риски кибербезопасности, оказываются одной из наиболее актуальных проблем в современном мире. Кибербезопасность — это защита индивида или организации, а также любых активов от угроз в киберпространстве, способных привести к несанкционированному доступу, утрате или неправомерному использованию информации [von Solms, van Niekerk, 2013]. Риски кибербезопасности включают в себя широкий спектр событий, которые могут нарушить безопасность в интернете, таких как заражение компьютерными вирусами, онлайн-мошенничество, кража личных данных. Эти риски все больше становятся частью повседневного опыта пользователей. По данным Росстата, с 2020 г. по 2024 г. доля интернет-пользователей от 15 лет и старше, столкнувшихся с проблемами кибербезопасности[2], выросла с 29 % до 48 %.

Противостояние рискам

Для защиты от цифровых угроз индивиды и организации адаптируют различные практики кибербезопасности. В литературе по исследованию рисков четко различаются коллективные, или институциональные, стратегии управления рисками и индивидуальные [Giritli Nygren, Olofsson, 2020]. Типичным примером первых стратегий является социальное страхование, когда организация берет на себя ответственность за управление и минимизацию рисков для определенной группы. Индивидуальные стратегии означают сознательные действия или модели поведения, которые используют люди для снижения риска в разных сферах. Например, для борьбы с игровой зависимостью некоторые игроки могут устанавливать самозапрет или лимиты на использование денежных средств [Drawson et al., 2017].

Когда речь идет о киберрисках, таких как утечка личных данных, онлайн-мошенничество и проч., институциональные решения включают в себя системы цифровой безопасности, созданные и внедренные техническими экспертами. Примерами таких решений могут служить системы аутентификации, антивирусные программы, шифрование данных и пр. на цифровых устройствах или в приложениях. Однако исследования в области кибербезопасности показывают, что реальное поведение людей часто не соответствует ожиданиям, заложенным в подобные решения, так как они не учитывают осведомленность пользователей о технологиях, их восприятие и умение ими пользоваться [Ng, Kankanhalli, Xu, 2009; Öğütçü, Testik, Chouseinoglou, 2016]. В результате эти технические решения сами по себе не всегда эффективны. Таким образом, кибербезопасность — это не только технологическая проблема, но и вопрос социального поведения.

В некоторых исследованиях рисков способность предотвращать или снижать риски, используя знания, описывается понятием рефлексивности. Эта идея про-

[2] Включая заражение вирусами, спам, получение мошеннических писем, кражу денежных средств, перенаправление на поддельные сайты, несанкционированный доступ к устройству и взлом учетных записей.

DOI: 10.14515/monitoring.2026.2.3117

исходит из теории общества риска, разработанной Энтони Гидденсом [Гидденс, 2011] и Ульрихом Беком [Бек, 2000]. Рефлексивность означает планирование жизни в условиях неопределенности с использованием знаний, произведенных в рамках различных экспертных систем [Гидденс, 2011]. Экспертные или абстрактные системы в понимании Гидденса означают системы профессиональной экспертизы или технического знания (например, медицина или право), на основе которых строится материальная или социальная сфера жизни [ibid.]. Рефлексивность помогает индивидам справляться с неопределенностью и рисками, вызванными модернизацией, и включает в себя общественное или индивидуальное осознание рисков, а также стратегии, то есть действия или практики по противостоянию им [Olofsson, Öhman, 2007].

В работах Гидденса и Бека рефлексивность рассматривается как характеристика поздней современности, связанная с возможностью индивидов (как и институтов) осмыслять и оценивать свои действия в условиях неопределенности. Однако рефлексивность не является универсальной чертой. Ряд авторов утверждают, что она неравномерно распределена в обществе и связана с социальной позицией индивида [Lash, 1997]. Рефлексивный индивид — это представитель социально и экономически привилегированных групп, имеющих материальные и культурные ресурсы для осознания рисков и адаптации стратегий для противостояния им [Lupton, 1999: 116]. Несмотря на то что разные социальные группы могут одинаково воспринимать риски, их способность отвечать на них может варьировать в зависимости от социальных условий и жизненных обстоятельств [Olofsson, Öhman, 2007].

Важным фактором принятия решений в отношении рисков оказывается также доверие экспертным системам, которое балансирует риск и обеспечивает индивидам опыт безопасности. В случае неудачного опыта взаимодействия с такими системами одна из реакций индивида может выражаться в попытке избегать контактов с ней и заполнить пробел самостоятельными действиями. Например, выходя в интернет, индивид принимает риски, связанные с этим, полагаясь на системы цифровой безопасности и предполагая, что вероятность столкнуться с утечкой данных или взломом аккаунта минимизирована. Нарушение цифровой безопасности в таком случае приводит к недоверию, то есть отрицательному или скептическому отношению к системе [Гидденс, 2011]. По мысли Гидденса, нарастая, недоверие превращается в беспокойство. Таким образом, недоверие и беспокойно из-за функционирования систем безопасности могут приводить к выработке индивидами практик по самостоятельной минимизации рисков.

Хотя риски цифровизации затрагивают значительную часть общества, остается недостаточно ясно, какие практики индивиды используют для самозащиты в цифровом пространстве и как это связано с социально-экономическим статусом. Одна из причин этого — редкое обращение исследователей к цифровизации как к источнику угроз. В связи с этим цель настоящей работы заключается в выявлении того, каким образом способность противостоять рискам цифровой безопасности соотносится с социально-экономическим статусом и опытом переживания рисков. Предполагается, что анализ практик кибербезопасности позволит сделать выводы о характере и распределении рефлексивности в условиях цифровизации.

DOI: 10.14515/monitoring.2026.2.3117

Методический подход к изучению практик кибербезопасности

Данные

Эмпирическая база исследования основана на материалах второй волны Мониторинга цифровой трансформации экономики и общества, реализованного Институтом статистических исследований и экономики знаний НИУ ВШЭ. Сбор данных проходил по месту жительства респондентов в формате личных интервью в апреле — мае 2024 г. Выборка включала население России из 64 регионов в возрасте от 14 лет и старше и формировалась с учетом пола, возраста, уровня образования и типа населенного пункта. В опросе приняли участие 10 038 человек, из которых 8404 (83 %) пользуются интернетом. Для обеспечения корректного представления генеральной совокупности применялось взвешивание по полу, возрасту, типу поселения, федеральному округу и региону. Так как работа фокусируется на противостоянии рискам цифровизации, в анализ включены только интернет-пользователи.

Анкета состояла из 14 тематических блоков, охватывающих широкий спектр вопросов — от доступа к интернету и использования устройств до цифровизации повседневных практик, онлайн-заработка и рисков.

Зависимая переменная. Практики кибербезопасности

Несмотря на большое разнообразие практик кибербезопасности, в исследовании охватывались только практики, доступные рядовым пользователям, тем самым не учитывались технически сложные инструменты, применяемые на уровне организаций,— криптографическое шифрование, системы обнаружения вторжений и пр. Набор практик кибербезопасности, о которых спрашивали респондентов, включает в себя: 1) использование пин-кода или пароля для разблокировки устройства, 2) использование отпечатка пальца или Face ID для разблокировки устройства, 3) сознательную замену паролей время от времени, 4) проверку безопасности сайта (например, наличие в адресе букв https, сертификата или логотипа безопасности и др.), 5) ознакомление с соглашением о конфиденциальности персональных данных при регистрации на сайтах и при установке приложений, 6) ограничение или отказ в доступе к местоположению при использовании приложений или сайтов, 7) ограничение доступа к профилю, контенту в соцсетях или облачных хранилищах (закрытие профиля, ограничение возможности просматривать страницу и др.), 8) отказ от разрешения использовать персональные данные в рекламных целях (например, отказ от рекламной рассылки по электронной почте и др.), 9) изменение настроек веб-браузера (например, Google Chrome, Яндекс. Браузер и др.) для блокировки сохранения файлов cookie на любом из устройств.

Практики с четвертой по девятую выделялись по методологии, используемой Евростатом, а с 2024 г.— Росстатом, для расчета цифровых навыков, в частности навыков безопасности. Практики с первой по третью были добавлены в опрос с целью измерить не только более продвинутый набор действий, но и базовый, включающий использование паролей и других средств защиты. Подобные вопросы, в частности, содержатся в методологическом гайде Международного союза электросвязи[3].

[3] Manual for Measuring ICT Access and Use by Households and Individual // International Telecommunication Union. 2020. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/manual/ITUManualHouseholds2020_E.pdf (дата обращения: 08.04.2026).

DOI: 10.14515/monitoring.2026.2.3117

Для измерения способности к рефлексивным действиям в области кибербезопасности все практики были разделены на две группы: инструментальные и стратегические. В группу инструментальных практик вошли практики 1—2, а во вторую — 3—9. Инструментальные практики включает в себя использование базовых функций цифровой безопасности, которые обычно встроены в устройства или приложения, например установку пароля или использование других форм идентификации [Steyaert, 2002]. Эти действия не требуют от пользователей особых технических знаний, а их эффективность во многом возлагается на организацию, которая их разработала. Стратегические практики, напротив, предполагают более продвинутое использование цифровых инструментов [van Deursen, van Dijk, 2009, 2010, 2011]. Они включают в себя такие действия, как ограничение поведения в сети и изменение настроек безопасности. Стратегические практики предполагают постоянный поиск и мониторинг информационной среды, которые выступают основой для действий. Чтобы применять эти практики, индивиду необходимо обладать некоторыми набором знаний о цифровой безопасности. Таким образом, инструментальные практики являются менее, а стратегические — более рефлексивными.

Независимые переменные

В качестве независимых переменных выступали основные социально-демографические характеристики, а также социально-экономической статус. В качестве социально-демографических переменных выступали: пол, возраст, наличие высшего образования и тип поселения. Тип поселения кодировался в три категории — село, города кроме Москвы и Санкт-Петербурга и Москва с Санкт-Петербургом.

В качестве индикатора социально-экономического статуса использовалась переменная материального положения домохозяйства. Материальное положение измерялось через субъективные оценки благосостояния домохозяйства индивида по шкале от 1 до 6, где 1 — «Мы едва сводим концы с концами. Денег не хватает даже на еду. Приходится сильно экономить», а 6 — «Можем позволить себе все, в том числе покупку квартиры или дачи». Чтобы обеспечить наполненность всех категорий, некоторые из них были объединены. В результате были получены четыре категории, закодированные от 0 до 3 — малообеспеченные, среднеобеспеченные, состоятельные и обеспеченные.

Кроме того, в модели были включены переменные, отражающие опыт столкновения с рисками информационной безопасности и степень беспокойства приватностью в интернете. Первая переменная позволяет выявить, сталкивался ли респондент ранее с проблемами информационной безопасности. Вторая переменная выражает доверие респондента абстрактной системе: чем выше беспокойство, тем ниже уровень доверия.

Для оценки опыта столкновения с рисками информационной безопасности респондентам предлагали выбрать из списка проблемы, с которыми они сталкивались за 12 месяцев до проведения опроса. В список включались следующие риски: 1) потеря из-за заражения вирусами файлов, фотографий и других данных на компьютере, на мобильном телефоне или другом устройстве, 2) получение мо-

DOI: 10.14515/monitoring.2026.2.3117

шеннических писем по электронной почте, телефонных звонков или смс, в том числе с просьбой указать персональные данные, 3) перенаправление на фальшивые сайты с просьбой указать персональные данные, 4) хищение денежных средств с банковской карты или счета, 5) утечка персональных данных, 6) взлом и использование неизвестными лицами профиля в социальных сетях, электронной почты и т. п., 7) вымогательство денежных средств, 8) другое. Переменная кодировалась как бинарная, где 1 — респондент сталкивался хотя бы с одним риском, 0 — респондент не сталкивался ни с одним риском.

В качестве переменной, отражающей уровень доверия к системам цифровой безопасности, использовался показатель беспокойства из-за приватности в интернете. Для его измерения респондентам предлагалось оценить степень беспокойства относительно следующих ситуаций: 1) порталы государственных и муниципальных услуг хранят все мои персональные данные, 2) другие люди могут найти в интернете личную информацию обо мне, 3) при регистрации на веб-сайтах и в приложениях требуется предоставлять персональную информацию, 4) информация о моих действиях в интернете может собираться и анализироваться в коммерческих целях, 5) моя личная информация может попасть в открытый доступ в результате взломов/утечек, 6) органы власти могут получить доступ к информации о моих действиях в интернете. Степень беспокойства измерялась по шкале от 0 до 3, где 0 — совсем не беспокоит, а 3 — очень беспокоит. Итоговая оценка для каждого респондента рассчитывалась как средняя оценка от всех ситуаций. Стоит отметить, что респондентов спрашивали преимущественно не про раскрытие информации другим людям, а про доверие организациям, которые собирают и обрабатывают персональные данные, поэтому переменная отражает институциональное доверие.

Анализ данных

Так как зависимая переменная имеет порядковый характер, для проведения анализа изначально предполагалось использовать порядковую логистическую регрессию. Однако при проверке допущений выяснилось, что не выполняется условие пропорциональности шансов. По этой причине выбор был сделал в пользу построения серии логистических регрессий, которые не требуют этого допущения. Всего было составлено две модели с отдельными зависимыми переменными. В модели 1 зависимая переменная выражалась как 0 — не используют практики (если респондент не отметил ни одной практики) и 1 — используют только инструментальные практики (если респондент отметил хотя бы одну инструментальную практику и ни одной стратегической). В модели 2 рассматривались две другие группы: 0 — используют только инструментальные и 1 — используют стратегические или комбинируют их с инструментальными (если респондент отметил хотя бы одну стратегическую или одну стратегическую и одну инструментальную практику).

Перед анализом данных была проведена проверка на наличие мультиколлинеарности между независимыми переменными. Результаты проверки показали варьирование коэффициента VIF от 1,3 до 3,7 для первой модели и 1,7 до 4,5 для второй. Такие значения указывают на отсутствие существенной мультиколлинеарности и считаются приемлемыми для социальных исследований.

DOI: 10.14515/monitoring.2026.2.3117

Результаты

Распространенность и социальная дифференциация практик кибербезопасности

Результаты анализа показывают, что практики кибербезопасности используют крайне неравномерно. Наиболее распространены самые простые практики — установка паролей (65 % интернет-пользователей 14 лет и старше) или разблокировка устройств с помощью биометрии — по отпечатку пальца или по лицу (37 %) (см. рис. 1). Меньшее распространение второго способа может быть связано с тем, что такие функции имеют более дорогие устройства, а значит, они доступны меньшей группе населения.

Рис. 1. Индивидуальные практики кибербезопасности
(в % от опрошенных пользователей интернета 14 лет и старше, *N* = 8404)

Стратегические практики применяются гораздо реже инструментальных, однако даже внутри этой группы можно наблюдать вариацию. Наиболее распространенная практика — сознательная периодическая смена паролей. Среди стратегических практик разные виды ограничительных действий (ограничение сбора данных о местоположении, отказ в использовании своих данных в рекламных целях, ограничение доступа к своему контенту в социальных сетях) применяются чаще, чем проверка и управление специфическими настройками безопасности (проверка безопасности сайта, изменение настройки браузера для блокировки файлов cookie).

DOI: 10.14515/monitoring.2026.2.3117

Заметная часть пользователей по-прежнему не применяет никаких практик кибербезопасности — таких оказалось 21% (см. табл. 1). Наиболее выражено это среди пожилых, малообеспеченных и жителей сел ($p < 0,05$). Пользователи, сталкивавшиеся с киберугрозами (21%), существенно реже игнорируют меры безопасности по сравнению с теми, у кого такого опыта не было (33%) ($p < 0,05$).

Более четверти опрошенных (29%) используют только инструментальные практики. Попарные тесты показали, что внутри этой группы значимые различия по основным социально-экономическим категориям минимальны. Это позволяет предположить, что принадлежность к группе слабо связана с социально-экономическим положением и может быть обусловлена другими факторами. Представителей этой группы больше среди мужчин, чем среди женщин, а также среди тех, кто не сталкивался с рисками информационной безопасности ($p < 0,05$).

Таблица 1. ***Использование практик кибербезопасности по типу практик (в % от опрошенных интернет-пользователей 14 лет и старше, N = 8404)***

	Не используют практики	Используют		
		Только инструментальные	Стратегические или инструментальные и стратегические	Только стратегические
Всего	21,4	28,9	49,8	8,2
Пол				
Мужчины	20,2	30,8	49,0	7,4
Женщины	22,3	27,4	50,3	8,9
Возраст				
Подростки (14—17 лет)	10,9	27,8	61,3	5,6
Молодые (18—44 года)	16,3	30,2	53,6	8,0
Средний возраст (45—59 лет)	25,4	30,0	44,6	11,0
Пожилые (60 лет и старше)	45,5	25,4	29,0	8,6
Высшее образование				
Без высшего обр.	22,4	30,0	47,6	7,9
С высшим обр.	19,0	26,3	54,7	9,0
Уровень материальной обеспеченности				
Малообеспеченные	34,4	30,2	35,4	7,4
Среднеобеспеченные	22,5	30,0	47,5	8,3
Состоятельные	16,2	26,4	57,4	8,8
Обеспеченные	16,1	31,0	52,9	6,1

DOI: 10.14515/monitoring.2026.2.3117

	Не используют практики	Используют		
		Только инструментальные	Стратегические или инструментальные и стратегические	Только стратегические
Тип поселения				
Село	25,5	31,8	42,6	6,6
Города кроме Москвы и Санкт-Петербурга	21,4	27,7	50,9	8,0
Москва и Санкт-Петербург	15,4	29,9	54,8	11,5
Опыт столкновения с рисками информационной безопасности				
Не сталкивались	27,7	32,8	39,5	6,4
Сталкивались	8,6	21,0	70,4	11,8
Обеспокоенность приватностью (среднее)	1,2	1,3	1,6	1,8

Источник: составлено автором на основе данных Мониторинга цифровой трансформации экономики и общества ИСИЭЗ НИУ ВШЭ.

Половина опрошенных (50%) используют стратегические практики, в том числе комбинируя их с инструментальными. Это преимущественно подростки (14—17) и молодые респонденты (18—44) ($p < 0,05$). Кроме того, для этого вида практик более выражена дифференциация по ряду социально-демографических характеристик и социально-экономическому положению — к стратегическим практикам чаще обращаются респонденты с высшим образованием, материально обеспеченные и проживающие в Москве или Санкт-Петербурге ($p < 0,05$). Подавляющее большинство респондентов, сталкивавшихся с рисками информационной безопасности, обращаются к стратегическим практикам ($p < 0,05$).

В ходе анализа также была выделена немногочисленная группа (8%) опрошенных, которые используют стратегические практики, но не используют инструментальные. Хотя эта группа и не выделялась для дальнейшего анализа, важно указать ее характерные особенности. Во-первых, ее представителей заметно больше в возрастной группе 45—59 лет. Во-вторых, только к стратегическим практикам обращаются чаще те, кто сталкивался с рисками (12%), чем те, кто не сталкивался с ними (6%). В-третьих, в этой группе заметно более высокий уровень беспокойства из-за приватности, чем в других. Малочисленность группы и недостаточность данных для ее изучения не позволили выделить ее для регрессионного анализа, хотя ее изучение может представлять интерес для дальнейших исследований.

Детерминанты использования инструментальных и стратегических практик кибербезопасности

Результаты регрессионного анализа показывают, что связь между социально-экономическим статусом и использованием практик кибербезопасности различа-

DOI: 10.14515/monitoring.2026.2.3117

ется в зависимости от вида практик. Так, при сопоставлении индивидов, не использующих практики и использующих только инструментальные, эта связь выражена слабее, чем при сравнении пользователей только инструментальных и стратегических практик. С возрастом шансы оказаться в группе, использующей только инструментальные практики, снижаются. Жители Москвы и Санкт-Петербурга по сравнению с жителями сельской местности имеют в 1,76 раза больше шансов попасть в группу использующих только инструментальные практики. Индивиды, сталкивавшиеся с рисками информационной безопасности, имеют больше шансов на использование только инструментальных практик. Этот предиктор демонстрирует самый высокий коэффициент — 2,422. Кроме того, по мере роста беспокойства приватностью в интернете повышаются шансы попасть в группу использующих только инструментальные практики. Остальные факторы — наличие высшего образование и материальное положение домохозяйства — не показали значимой связи.

Таблица 2. ***Результаты регрессионного анализа: отношения шансов***

	Модель 1	**Модель 2**
	Не используют практики = 0, Используют только инструментальные практики = 1	**Используют только инструментальные практики = 0, Используют оба вида практик = 1**
Константа	4,463** [3,09, 6,44]	1,133 [0,84, 1,53]
Пол: 1 = Мужской	1,183 [0,99, 1,41]	0,844* [0,73, 0,97]
Возраст	0,965** [0,96, 0,97]	0,981** [0,98, 0,99]
Тип поселения (референс — село)		
Города кроме Москвы и Санкт-Петербурга	1,102 [0,90, 1,35]	1,287** [1,08, 1,54]
Москва и Санкт-Петербург	1,762** [1,30, 2,39]	1,194 [0,94, 1,52]
Наличие высшего образования	1,117 [0,91, 1,37]	1,225** [1,04, 1,44]
Материальное положение	0,954 [0,88, 1,04]	1,136** [1,05, 1,23]
Опыт столкновения с киберрисками	2,422** [1,91, 3,07]	2,693** [2,31, 3,14]
Беспокойство приватностью	1,070 [0,98, 1,17]	1,387** [1,28, 1,50]
N	4084	6458
Pseudo R2	0,097	0,089

* p-value < 0,01, ** p-value < 0,001.
Источник: составлено автором на основе данных Мониторинга цифровой трансформации экономики и общества ИСИЭЗ НИУ ВШЭ.

DOI: 10.14515/monitoring.2026.2.3117

Результаты второй модели показали, что вероятность попасть в группу использующих стратегические практики выше среди женщин. Как и в предыдущей модели, с возрастом вероятность попасть в группу использующих стратегические практики снижается. Также вероятность прибегнуть к стратегическим практикам выше у жителей городов, кроме Москвы и Санкт-Петербурга, чем у жителей сел. Наличие высшего образования увеличивает шансы использования стратегических практик примерно в 1,2 раза. С ростом материального благосостояния шансы использовать стратегические практики увеличиваются в 1,14 раза. Как и в первой модели, опыт столкновения с рисками информационной безопасности продемонстрировал самый высокий коэффициент (2,693) и значимую положительную связь. По мере роста уровня беспокойства возрастают и шансы использования стратегических практик.

Дискуссия

Результаты анализа показали, что применение практик кибербезопасности связано с социально-демографическими характеристиками пользователей интернета. В то же время именно на уровне стратегических практик отчетливо проявляется влияние факторов, определяющих социально-экономическое положение. Таким образом, социально-экономическое неравенство выражается в различиях использования сложных стратегических практик, требующих от пользователей не только определенных знаний, но и более высокой степени вовлеченности в управление цифровой безопасностью.

Использование простых практик кибербезопасности характерно для более молодых пользователей, а также для жителей Москвы и Санкт-Петербурга. Ранее исследования показывали, что представители разных возрастных категорий по-разному воспринимают приватность в интернете и относятся к защитным практикам [Elueze, Quan-Haase, 2018; Quan-Haase, Ho, 2020]. Пожилые пользователи по сравнению с молодыми уделяют меньше внимания вопросам собственной приватности и проявляют бóльшую готовность к обмену информацией. Личную информацию они чаще считают менее ценной и, следовательно, менее требующей защиты. Это может быть связано как с ограниченным использованием интернета, так и с меньшей осведомленностью о сопутствующих рисках [Blackwood-Brown, Levy, D'Arcy, 2021]. В то же время в анализ включались и более новые технологии, в частности биометрические методы идентификации. В одном из исследований показано, что среди старших пользователей наблюдается настороженное отношение к биометрической идентификации, что объясняется низким доверием к новым технологиям и трудностями их освоения [Kumalasari et al., 2024]. Значимая связь с проживанием в крупных мегаполисах может быть обусловлена именно включением в анализ использования биометрических методов. Жители Москвы и Санкт-Петербурга чаще имеют доступ к более дорогим и технологически продвинутым устройствам, поддерживающим биометрическую идентификацию, чем жители сельской местности.

Обращает на себя внимание отсутствие значимых связей с факторами, считающимися «классическими» предикторами цифрового неравенства (за исключением возраста), в частности уровня образования. Использование простых ме-

DOI: 10.14515/monitoring.2026.2.3117

тодов цифровой защиты не формируется напрямую социально-экономическим статусом. Вероятно, это связано с преодолением «первого» цифрового разрыва, то есть разрыва в доступе к технологиям, который обуславливался в первую очередь возрастом и образованием. Установка паролей доступна на большинстве современных устройств, как и сами эти устройства (смартфоны или мобильные телефоны). Например, среди россиян в 2024 г. 87 % владели смартфонами [4]. Вероятно, этот разрыв перешел на уровень различий в восприятии приватности и необходимости защищать свою цифровую информацию.

При сравнении использования только простых и более сложных стратегических практик использование вторых более тесно связано с социально-экономическим положением. К стратегическим практикам чаще прибегают женщины, молодые пользователи, люди с более высоким уровнем дохода и с высшим образованием. Эти результаты согласуются с выводами предыдущих исследований, показавших связь между социально-экономическим положением и выбором стратегий безопасного поведения в интернете, которая объясняется феноменом цифрового неравенства [Dodel, Mesch, 2018; Dodel, Kaiser, Mesch, 2020]. Традиционные различия по возрасту, уровню образования и доходу определяли неравенство в доступе к технологиям (интернету и цифровым устройствам), а доступ, в свою очередь, влиял на формирование цифровых навыков. Пользователи с более высоким уровнем таких навыков, успешно прошедшие «социализацию» в интернете, лучше осознают потенциальные риски его использования и обладают более широким набором средств для самозащиты. Подобная дифференциация между более активными и более пассивными стратегиями адаптации к рискам наблюдалась и вне цифровой сферы: российские исследования показывают, что активные стратегии адаптации чаще выбирают более молодые и более образованные группы. Последнее позволяет предположить сходство механизмов адаптации к рискам различной природы [Мозговая, Шлыкова, 2014; Мозговая, 2021].

Некоторые результаты выглядят несколько противоречивыми. В частности, выяснилось, что женщины имеют больше шансов использовать стратегические практики защиты. Это не согласуется с выводами других исследователей, утверждающих, что мужчины демонстрируют более высокий уровень цифровых навыков и склонны быть более технологически подкованными, а значит, должны иметь более широкое представление о рисках и способах защиты [Hargittai, 2010]. Вероятно, в этом случае играет роль различие в восприятии рисков, которое фиксируется и на гендерном уровне. Женщины демонстрируют более выраженное беспокойство и страх стать жертвами киберпреступлений [Henson, Reyns, Fisher, 2013]. Это может способствовать более осторожному поведению в интернете и адаптации более продвинутых практик киберзащиты.

Помимо социально-экономических факторов, значимая связь выявлена и с опытом столкновения с киберрисками. При этом обеспокоенность вопросами приватности оказалась релевантной лишь на уровне продвинутых практик. Вероятно, это связано с тем, что базовые действия, такие как использование паролей или биометрии, направлены преимущественно на защиту устройства, а не персо-

[4] Кузина Л. С., Полякова В. В. Что россияне делают со старыми гаджетами? // ИСИЭЗ НИУ ВШЭ. 2024. 5 декабря. URL: https://issek.hse.ru/news/993901856.html (дата обращения: 08.04.2026).

DOI: 10.14515/monitoring.2026.2.3117

нальных данных напрямую, тогда как стратегические практики ориентированы именно на защиту информации. Поскольку обеспокоенность приватностью выступает индикатором недоверия к системам безопасности, полученные результаты подтверждают предположение, что уровень доверия влияет на адаптацию практик. Можно заключить, что недоверие к способам сбора, хранения и управления пользовательскими данными стимулирует самостоятельные усилия по их защите. Эти выводы согласуются с рядом исследований, фиксирующих прямую зависимость между доверием к цифровым системам и готовностью делиться персональной информацией или, напротив, ограничивать доступ к ней [Wang, Yu, 2015; Kumar, Kumar, Bhasker, 2018].

Наконец, опыт столкновения с цифровыми рисками оказался значимым предиктором не только для базовых, но и для продвинутых практик, причем в обоих случаях самым сильным. То есть переживание киберрисков связано с формированием защитного поведения. Можно предположить, что нанесенный ущерб усиливает чувство тревожности и стимулирует адаптацию как инструментальных, так и стратегических защитных стратегий. Само столкновение с риском нередко интерпретируется пользователями как свидетельство ненадежности цифровых систем, что порождает недоверие и усиливает беспокойство. Ряд исследований также показали, что связь между киберрисками и формированием защитных практик опосредуется их субъективным восприятием: опыт кибервиктимности повышает чувствительность к угрозам, что, в свою очередь, способствует как избеганию рисков, так и переходу к более сложным стратегиям защиты [Henson, Reyns, Fisher, 2013; Ngo et al., 2020].

Такой механизм может быть связан с особенностями самих цифровых рисков. Исследования в рамках психометрической парадигмы в социологии рисков показали, что восприятие цифровых рисков несколько отличается от восприятия более традиционных рисков (например, глобальное потепление, курение, преступность и пр.). Цифровые риски являются частью повседневного опыта, взаимодействие с ними стало традиционной практикой для населения [Гаврилов, Бутынко, 2021]. Одновременно с этим они не воспринимается как катастрофичные по своим последствиям, вызывая только умеренный страх. По этой причине именно личный опыт переживания рисков влияет на уровень беспокойства.

Результаты работы позволили взглянуть на рефлексивность с точки зрения неравно распределенного качества. В исследованиях риска неравномерное распределение рефлексивности объясняется через концепцию габитуса П. Бурдьё [Lewis, 2006; Threadgold, Nilan, 2009]: управление рисками структурируется как личным опытом, так и материальными и культурными ресурсами индивида. Перенося эту идею на киберриски, можно предположить, что управление индивидуальной кибербезопасностью формируется личным опытом столкновения с рисками, но выбор стратегий и их адаптация зависят от объема располагаемых ресурсов. Неолиберальная, то есть индивидуализированная, модель управления цифровыми рисками ориентирована на материально и культурно привилегированные слои общества, в то время как другие вынуждены выбирать более простые методы или полагаться на те способы защиты, которые предлагают цифровые системы.

DOI: 10.14515/monitoring.2026.2.3117

Заключение

Исследование показало, что практики кибербезопасности среди интернет-пользователей в России распределены неравномерно. Наибольшее распространение получили самые простые меры — установка паролей и использование биометрической идентификации на цифровых устройствах. Более сложные практики, такие как управление доступом к личным данным, требующие определенной технической осведомленности и готовности к принятию решений, применяются значительно реже. При этом, несмотря на то что заметная часть россиян по-прежнему не использует никаких средств защиты, для большинства характерно комбинирование простых и сложных практик.

Кроме того, было установлено, что шансы использовать сложные и продвинутые практики определяются в большей степени социально-экономическими характеристиками индивидов, тогда как обращение к простейшим мерам защиты по сравнению с полным их отсутствием связано лишь с частью этих факторов. Тем самым подтверждаются выводы исследований цифрового неравенства о воспроизводстве традиционного социального неравенства на цифровом уровне.

В то же время выявлено, что способность противостоять цифровым рискам обусловлена не только социально-экономическим положением, но и опытом их непосредственного переживания. Опыт измерялся через факт столкновения с проблемами информационной безопасности и через уровень обеспокоенности вопросами приватности в интернете. Анализ показал, что если сам опыт столкновения с рисками связан как с простыми, так и со сложными практиками, то обеспокоенность приватностью играет значимую роль только на уровне сложных практик. Поскольку данный показатель рассматривался как индикатор недоверия к системам цифровой безопасности, полученные результаты подтверждают предположения теории общества риска: недоверие к абстрактным системам побуждает индивидов предпринимать самостоятельные действия по защите от угроз.

Таким образом, личный опыт переживания рисков и их восприятие, — в частности доверие к системам, призванным обеспечивать цифровую безопасность, — способны стимулировать защитные реакции. Однако выбор практик зависит от объема и качества материальных и культурных ресурсов индивида. В этом смысле рефлексивность, понимаемая как способность самостоятельно отвечать на риски, выступает еще одним измерением социального неравенства.

Ряд ограничений исследования связан с особенностями сбора данных. Во-первых, перечень практик, предложенных респондентам, был ограничен и не предусматривал возможность указать вариант «другое», что сужает спектр зафиксированных практик. Во-вторых, в вопросе о киберрисках фиксировался только факт их переживания, без оценки величины полученного ущерба или субъективного восприятия последствий. Кроме того, данная переменная не позволяет учитывать частоту столкновения с рисками. В будущих исследованиях стоит уделить больше внимания взаимосвязи между адаптацией практик кибербезопасности и восприятием цифровых угроз. Наконец, субъективная оценка материального положения домохозяйства может рассматриваться как общая характеристика социально-экономического положения индивида, не отражая влияния отдельных его аспектов — положения в хозяйственной иерархии, наличия различных видов активов и проч.

DOI: 10.14515/monitoring.2026.2.3117

Исходя из полученных результатов меры по противодействию угрозам цифровой безопасности следует фокусировать на развитие технической осведомленности и цифровых навыков населения. Такая осведомленность предполагает не только информирование о существующих рисках, но и распространение знаний о доступных средствах защиты — настройках безопасности, управлении доступом к персональным данным, регулярной смене паролей и других практиках. Особое внимание при этом целесообразно уделять группам с ограниченным опытом социализации в интернете, прежде всего пожилым пользователям.

Список литературы (References)

1. Бек У. Общество риска. На пути у другому модерну / пер. с нем. В. Седельникова, Н. Федорова, М.: Прогресс-Традиция, 2000.
Beck U. (2000) Risikogesellschaft. Auf dem Weg in eine andere Moderne. Moscow: Progress-Tradition. (In Russ.)

2. Гаврилов К., Бутынко М. Восприятие традиционных рисков и киберрисков: опыт использования «психометрической парадигмы» // Социологический журнал. 2021. Т. 27. № 4. С. 146—168.https://doi.org/10.19181/socjour.2021.27.4.8649.
Gavrilov K. A., Butynko M. V. (2021) The Perception of Cyber and Traditional Risks: Experience of Using the Psychometric Paradigm Approach. *Sociological Journal*. Vol. 27. No. 4. P. 146—168. https://doi.org/10.19181/socjour.2021.27.4.8649. (In Russ.)

3. Гидденс Э. Последствия современности / пер. с англ. Г. К. Ольховикова; Д. А. Кибальчича. М.: Праксис, 2011.
Giddens A. (2011) The Consequences of Modernity. Moscow: Praxis. (In Russ.)

4. Мозговая А. Адаптация к средовым изменениям: риски социальных и технологических нововведений // Социологический журнал. 2021. Т. 27. № 3. С. 60—77. https://doi.org/10.19181/socjour.2021.27.3.8424.
Mozgovaya A. V. (2021) Adapting to Environmental Changes: The Risks of Social and Technological Innovations. *Sociological Journal*. Vol. 27. No. 3. P. 60—77. https://doi.org/10.19181/socjour.2021.27.3.8424. (In Russ.)

5. Мозговая А., Шлыкова Е. Социальные ресурсы и адаптация к риску: выбор Стратегии (на примере Социальной общности в Ситуации конкретного риска) // Социологическая наука и социальные практики. 2014. Т. 8. № 4. С. 25—49. URL: https://www.socnp.ru/index.php/snsp/article/view/3089 (дата обращения: 30.04.2026).
Mozgovaya A. V., Shlykova E. V. (2014) Social Resources and Adaptation to Risk: The Choice of Strategy (by the Example The Social Community in the Situation of Particular Risk). *Sociological Science and Social Practice*. Vol. 8. No. 4. P. 25—49. URL: https://www.socnp.ru/index.php/snsp/article/view/3089 (date of access: 30.04.2026). (In Russ.)

6. Blackwood-Brown C., Levy Y., D'Arcy J. (2021) Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems*. Vol. 61. No. 3. P. 195—206. https://doi.org/10.1080/08874417.2019.1579076.

7. Dodel M., Mesch G. (2018) Inequality in Digital Skills and the Adoption of Online Safety Behaviors. *Information, Communication & Society*. Vol. 21. No. 5. P. 712—728. https://doi.org/10.1080/1369118X.2018.1428652.

8. Dodel M., Kaiser D., Mesch G. (2020) Determinants of Cyber-Safety Behaviors in a Developing Economy: The Role of Socioeconomic Inequalities, Digital Skills and Perception of Cyber-Threats. *First Monday*. Vol. 25 No. 7. https://doi.org/10.5210/fm.v25i7.10830.

9. Drawson A. S., Tanner J., Mushquash C. J., Aislin R. M., Dwight M. (2017) The Use of Protective Behavioural Strategies in Gambling: a Systematic Review. *International Journal of Mental Health and Addiction*. Vol. 15. No. 6. P. 1302—1319. https://doi.org/10.1007/s11469-017-9754-y.

10. Elueze I. and Quan-Haase A. (2018) Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited. *American Behavioral Scientist*. Vol. 62. No. 10. P. 1372—1391. https://doi.org/10.1177/0002764218787026.

11. Giritli Nygren K., Olofsson A. (2020) Managing the COVID-19 Pandemic Through Individual Responsibility: The Consequences of a World Risk Society and Enhanced Ethopolitics. *Journal of Risk Research*. Vol. 23. No. 7—8. P. 1031—1035. https://doi.org/10.1080/13669877.2020.1756382.

12. Gradillas M., Thomas L. D.W. (2025) Distinguishing Digitization and Digitalization: A Systematic Review and Conceptual Framework. *Journal of Product Innovation Management*. Vol. 42. No. 1. P. 112—143. https://doi.org/10.1111/jpim.12690.

13. Hargittai E. (2010) Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the 'Net Generation.' *Sociological Inquiry*. Vol. 80. No. 1. P. 92—113. https://doi.org/10.1111/j.1475-682X.2009.00317.x.

14. Henson B., Reyns B. W., Fisher B. S. (2013) Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice*. Vol. 29. No. 4. P. 475—497. https://doi.org/10.1177/1043986213507403.

15. Kumalasari R. A.D., Rahardjo K., Kusumawati A., Sunarti S. (2024) Biometric-Based Self-Service Technology Adoption by Older Adult: Empirical Evidence from Pension Fund Sector in Indonesia. *Cogent Business & Management*, Vol. 11. No. 1. Art. 232543. https://doi.org/10.1080/23311975.2024.2325543.

16. Kumar S., Kumar P., Bhasker B. (2018) Interplay Between Trust, Information Privacy Concerns and Behavioural Intention of Users on Online Social Networks. *Behaviour & Information Technology*. Vol. 37. No. 6. P. 622—633. https://doi.org/10.1080/0144929X.2018.1470671.

17. Lash S. (1997) La ReflexivIdad y sus Dobles: Estructura, Estética, Comunidad. En: Beck U., Giddens A., Lash S. (eds.) Modernización reflexive: Política, tradición y estética en el orden social modern. Madrid: Alianza Editorial, S. A. P. 137—209.

18. Lewis T. (2006) DIY selves? Reflexivity and Habitus in Young People's Use of the Internet for Health Information. *European Journal of Cultural Studies*. Vol. 9. No. 4. P. 461—479. https://doi.org/10.1177/1367549406069068.

19. Lupton D. (1999) Risk. New York, NY: Routledge. https://doi.org/10.4324/9781003316299.

20. Lupton D. (2016) Digital Risk Society. In: Burgess A., Alemanno A., Zinn J. (eds.) *Routledge Handbook of Risk Studies*. New York, NY: Routledge. P. 301—309. https://doi.org/10.4324/9781315776835.

21. Ng B.-Y., Kankanhalli A. and Xu Y. (Calvin) (2009) Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*. 46. No. 4. P. 815—825. https://doi.org/10.1016/j.dss.2008.11.010.

22. Ngo F. T., Piquero A.R, LaPrade J., Duong B. (2020) Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? *Criminal Justice Review*. Vol. 45. No. 4. P. 430—451. https://doi.org/10.1177/0734016820934175.

23. Öğütçü G., Testik Ö. M., Chouseinoglou O. (2016) Analysis of Personal Information Security Behavior and Awareness. *Computers & Security*. No. 56. P. 83—93. https://doi.org/10.1016/j.cose.2015.10.002.

24. Olofsson A., Öhman S. (2007) Views of Risk in Sweden: Global Fatalism and Local Control — An Empirical Investigation of Ulrich Beck's Theory of New Risks. *Journal of Risk Research*. Vol. 10. No. 2. P. 177—196. https://doi.org/10.1080/13669870601122451.

25. Quan-Haase A., Ho D. (2020) Online Privacy Concerns and Privacy Protection Strategies Among Older Adults in East York, Canada. *Journal of the Association for Information Science and Technology*. Vol. 71. No. 9. P. 1089—1102. https://doi.org/10.1002/asi.24364.

26. Steyaert J. (2002) Inequality and the Digital Divide: Myths and Realities. In: Hick S., McNutt J. (eds.) *Advocacy, Activism and The Internet*. Chicago, IL: Lyceum Press. P. 199—211.

27. Threadgold S., Nilan P. (2009) Reflexivity of Contemporary Youth, Risk and Cultural Capital. *Current Sociology*. Vol. 57. No. 1. P. 47—68. https://doi.org/10.1177/0011392108097452.

28. Van Deursen A. J.A.M., van Dijk J. A.G.M. (2009) Using the Internet: Skill Related Problems in Users' Online Behavior. *Interacting with Computers*. Vol. 21. No. 5—6. P. 393—402. https://doi.org/10.1016/j.intcom.2009.06.005.

DOI: 10.14515/monitoring.2026.2.3117

29. Van Deursen A. J.A.M.V., van Dijk J. A.G.M. (2010) Measuring Internet Skills. *International Journal of Human-Computer Interaction*. Vol. 26. No. 10. P. 891—916. https://doi.org/10.1080/10447318.2010.496338.

30. Van Deursen A., van Dijk J. (2011) Internet Skills and the Digital Divide. *New Media and Society*. Vol. 13. No. 6. P. 893—911. https://doi.org/10.1177/1461444810386774.

31. Von Solms R., van Niekerk J. (2013) From Information Security to Cyber Security. *Computers & Security*. No. 38. P. 97—102. https://doi.org/10.1016/j.cose.2013.04.004.

32. Wang Z., Yu Q. (2015) Privacy Trust Crisis of Personal Data in China in the Era of Big Data: The Survey and Countermeasures. *Computer Law & Security Review*. Vol. 31. No. 6. P. 782—792. https://doi.org/10.1016/j.clsr.2015.08.006.