Электронный журнал
«Современная зарубежная психология»
2024. Том 13. № 4. С. 163—171.
DOI: https://doi.org/10.17759/jmfp.2024130415
ISSN: 2304-4977 (online)

E-journal
“Journal of Modern Foreign Psychology”
2024, vol. 13, no. 4, pp. 163—171.
DOI: https://doi.org/10.17759/jmfp.2024130415
ISSN: 2304-4977 (online)

ЮРИДИЧЕСКАЯ ПСИХОЛОГИЯ И ПСИХОЛОГИЯ БЕЗОПАСНОСТИ
LEGAL PSYCHOLOGY AND PSYCHOLOGY OF SAFETY

Психологические факторы кибербезопасности и доверие к ложным новостям в интернет-коммуникации: обзор современных зарубежных исследований

Фабрикант М.С.
Национальный исследовательский университет «Высшая школа экономики» (ФГАОУ ВО «НИУ ВШЭ»), г. Москва, Российская Федерация;
Белорусский государственный университет (БГУ), г. Минск, Республика Беларусь
ORCID: https://orcid.org/0000-0001-5707-2943, e-mail: marharyta.fabrykant@gmail.com

Представлен систематический обзор современных зарубежных исследований психологических факторов кибербезопасности и доверия к ложным новостям. Проведен анализ теоретических разработок и эмпирических исследований психологических сторон кибербезопасности в рамках концепций психологии личности, поведенческой психологии и социальной психологии. Несмотря на то, что общие психологические закономерности и теоретические модели этих разделов психологии находят применение в изучении кибербезопасности, имеющиеся результаты исследовательской работы этого направления все еще не позволяют сформировать целостную картину психологических факторов кибербезопасного поведения. При этом факторы личностных характеристик и поведения киберпреступников представляются лучше изученными и более понятными, чем факторы соблюдения и нарушения правил кибербезопасного поведения «обычными» пользователями. Далее в статье проводится обзор эмпирических исследований причин доверия интернет-пользователей к ложным новостям и способов его преодоления. Показано, что общая осведомленность о наличии проблемы распространения ложных новостей не способствует уменьшению доверия к ним, а использование неэффективных стратегий их распознавания часто дает противоположный эффект. Более сложная стратегия, основанная на знании конкретных приемов, посредством которых создаются ложные новости, напротив, позволяет более эффективно снижать риск доверия к ложным новостям. Автор приходит к выводу о целесообразности мер, содействующих кибербезопасному поведению интернет-пользователей, направленных не на стимулирование бдительности, а на повышение доверия к картине мира, в которую феномены угроз кибербезопасности и ложных новостей встроены в качестве знакомой и понятной составляющей.

Ключевые слова: кибербезопасность, киберпреступность, кибербезопасное поведение, Интернет, социальные медиа, ложные новости, информационный пузырь, доверие.

Финансирование. Исследование выполнено в рамках Программы фундаментальных исследований НИУ ВШЭ.

Для цитаты: *Фабрикант М.С.* Психологические факторы кибербезопасности и доверие к ложным новостям в интернет-коммуникации: обзор современных зарубежных исследований [Электронный ресурс] // Современная зарубежная психология. 2024. Том 13. № 4. С. 163—171. DOI: https://doi.org/10.17759/jmfp.2024130415

Psychological Factors of Cybersecurity and Trust in Fake News in Internet Communication: Review of Contemporary Foreign Studies

Marharyta S. Fabrykant
HSE University, Moscow, Russia; Belarusian State University, Minsk, Belarus
ORCID: https://orcid.org/0000-0001-5707-2943, e-mail: marharyta.fabrykant@gmail.com

The paper presents a systematic review of contemporary foreign research on psychological factors of cybersecurity and trust in fake news. It contains an analysis of theoretical developments and empirical studies of the psychological aspects of cybersecurity within the framework of the concepts of personality psychology, behavioral psychology and social psychology. Despite the fact that general psychological patterns and theoretical models of these

branches of psychology are used in the study of cybersecurity, the available results of research in this area still do not form a holistic picture of the psychological factors of cybersecurity behavior. At the same time, the factors of personal characteristics and behavior of cybercriminals seem to be better studied and more understandable than the factors of compliance and violation of the rules of cybersecurity behavior by "ordinary" users. The article then presents a review of empirical studies on the reasons why Internet users trust fake news and how to overcome it. General awareness of the problem of the spread of fake news is shown to offer little help in reducing trust in fake news, and the use of ineffective strategies for recognizing fake news often has the opposite effect. A more sophisticated strategy based on knowledge of the specific techniques by which fake news is created, on the contrary, can more effectively reduce the risk of trust in fake news. The author comes to the conclusion that measures promoting cybersecurity behavior of Internet users are advisable if aimed not at stimulating vigilance, but at increasing confidence in the picture of the world, in which the phenomena of cybersecurity threats and fake news are built in as a familiar and understandable component.

Keywords: cybersecurity, cybercrime, cybersecurity behavior, Internet, social media, fake news, information bubble, trust.

Funding. This work is an output of a research project implemented as part of the Basic Research Program at the HSE University.

For citation: Fabrykant M.S. Psychological Factors of Cybersecurity and Trust in Fake News in Internet Communication: Review of Contemporary Foreign Studies [Electronic resource]. *Sovremennaya zarubezhnaya psikhologiya = Journal of Modern Foreign Psychology*, 2024. Vol. 13, no. 4, pp. 163—171. DOI: https://doi.org/10.17759/jmfp. 2024130415 (In Russ.).

Введение

Проблема кибербезопасности становится все более актуальной по мере цифровизации различных сфер жизни. В связи с распространением посредством социальных сетей феномена кибермошенничества в его разнообразных формах и, соответственно, ложной информации (иногда с серьезными негативными последствиями) углубляется понимание того, что задача обеспечения кибербезопасности *как организаций, так и частной жизни людей* не является исключительно технологической. Ее решение во многом зависит от поведения людей как субъектов кибербезопасности, причем не только экспертов, но и всех, кто вовлечен в использование цифровых ресурсов. Более того, жертвами киберпреступников и нарушителями правил кибербезопасного поведения становятся в том числе люди, в целом хорошо осведомленные о киберпреступности и ее внешних проявлениях, однако по каким-либо причинам не всегда способные использовать эту информацию в конкретных ситуациях, когда она оказывается необходимой. С проблемой доверия интернет-пользователей кибермошенникам связана другая проблема — доверие массово тиражируемым в социальных медиа ложным новостям, что может приводит к не столь очевидным, но не менее опасным последствиям.

На этом фоне все более осознанной становится необходимость изучения психологических факторов безопасного поведения в Интернете. Цель данной статьи — систематический обзор проведенных к настоящему времени эмпирических исследований личностных и ситуативных факторов кибербезопасного поведения и доверия к ложным новостям. В наши задачи входит показать, что известно в современной эмпирической социальной психологии, поведенческой психологии и психологии личности о личностных чертах людей, склонных к соблюдению или, напротив, нарушению правил кибербезопасного поведения, а также самих киберпреступников, каковы факторы, обусловливающие доверие интернет-пользователей к ложным новостям, и на основании проанализированных результатов обозначить пути решения проблемы обеспечения безопасного поведения интернет-пользователей.

Психологические подходы к изучению кибербезопасности

Лейтмотив многих публикаций о психологических факторах кибербезопасности — указание на их относительную неизученность и недооцененость. Изначально и довольно долго проблема кибербезопасности рассматривалась как *сугубо* техническая и соответственно она решалась техническими средствами [15]. Лишь впоследствии (и, возможно, как раз вследствие этой неизученности) человеческий фактор был признан наиболее слабым звеном в программах повышения кибербезопасности. Стали предприниматься попытки изучить этот человеческий фактор — в формате приложения отдельных теоретических подходов к практическим вопросам, проведения эмпирических исследований, вплоть до построения общих моделей — с позиций различных разделов общей и специальной психологии. Рассмотрим в*и*дение психологического аспекта кибербезопасности с позиции классических концепций психологии личности, поведенческой психологии и социальной психологии.

Недавние исследования кибербезопасности применительно к теории и практике психологии личности предсказуемо представляют собой попытки выявить, какие личностные черты и каким образом значимо влияют на кибербезопасное поведение. Так, Шерри,

Доусон и Дебб [22] обнаружили, что степень соблюдения норм и правил кибербезопасного поведения положительно связана с тремя из пяти составляющих «Большой пятерки» личностных черт — прежде всего с добросовестностью, затем доброжелательностью и открытостью опыту.

Можно интерпретировать результаты этих авторов таким образом, что кибербезопасному поведению способствуют не только добросовестное отношение к своим обязательствам и правилам кибербезопасного поведения как норма поведения в целом, но и просоциальная ориентация. Иными словами, кибербезопасность оценивается субъектом как серьезный риск, когда осознается угроза не только себе, но и окружающим, а также как восприимчивость к новым идеям (либо благодаря способности представить себе все разнообразные вариации киберугроз и их вероятные последствия, либо более высокая общая информированность о цифровой сфере как следствие более высокого интереса к новым технологиям в целом).

Вместе с тем Кеннисон и Чан-Тин [14] выявили значимую связь кибербезопасного поведения лишь с одной чертой личности, наиболее очевидной из личностных характеристик пятифакторной модели, — добросовестностью. Такой результат может быть связан с тем, что в этом исследовании кибербезопасное поведение операционализировалось не как соблюдение правил, а, напротив, как их нарушение — рискованное поведение.

Обращает на себя внимание тот факт, что в обоих исследованиях не было выявлено значимой связи между кибербезопасным поведением и нейротизмом, хотя, казалось бы, причиной нарушения правил кибербезопасности должна быть низкая эмоциональная стабильность. Представляется, что многие формы киберугроз не выглядят как явные ситуации опасности, но, напротив, они мимикрируют под стандартные ситуации (таковы, например, фишинг, имитирующий стандартную процедуру запроса данных, или фейковые сайты известных интернет-магазинов, имитирующие привычную операцию оформления покупки онлайн). В результате запускается стандартное, наиболее привычное человеку, поведение, и именно оно в нестандартных ситуациях приводит к опасным последствиям, выполняя роль триггера.

Еще один подход к проблеме кибербезопасности в рамках психологии личности ориентирован на смену полюсов объекта изучения психологических особенностей субъекта кибербезопасности: на изучение не потенциальных жертв кибератак (то есть, по сути, всех добросовестных пользователей цифровых технологий), а тех, кто планирует и осуществляет эти атаки. Так, Чань, Лу, Кумар и Яу [13], предлагая достаточно эклектичную по своим основаниям классификацию хакеров, включающую в себя 13 типов («новички»; «киберпанки»; «инсайдеры»; «старая гвардия»; «профессионалы»; «хактивисты»; «национальные государства»; «студенты»; «мелкие воришки»; «цифровые пираты»; онлайн преступники, совершающие преступления сексуального характера; «краудсорсеры», содействующие киберпреступности), составили для каждого из этих типов мотивационный профиль, акцентируя внимание на наличии либо отсутствии каждого из следующих мотивов: любопытство, материальная выгода, слава, месть, досуг, идеология, сексуальные импульсы.

Показано, что наиболее частыми мотивами, которые встречаются у семи из тринадцати типов, включенных в классификацию, являются материальная выгода и месть. При этом у пяти типов хакеров — киберпанков, инсайдеров, профессионалов, национальных государств и мелких воришек — сочетаются оба этих мотива.

Таким образом, в мотивации хакеров сочетаются узкопрагматические и эмоционально-личностные мотивы, что должно сильно затруднять профайлинг.

Эта проблема профайлинга хакеров решается сегодня в подходе к кибербезопасности с позиций теории и практики в русле еще одного раздела психологии — поведенческой психологии — посредством переноса фокуса внимания исследователя с причин хакерской активности на ее практические последствия, особенно на оценку серьезности последствий и их охвата.

В наиболее фундаментальном на сегодняшний день труде по психологии кибербезопасности за авторством Паттерсона и Уинстон-Простора [20] предлагается схема профайлинга хакеров на основании двух основных критериев — уровня технических компетенций и способности к стратегическому планированию (категории A, B, C, D).

Хакеры категории A представляют собой достаточно хорошо организованные группы, владеющие знанием сложных технологий и большими материальными ресурсами, заинтересованные только в масштабных целях и способные к тщательному планированию. Категорию B составляют хакеры, обладающие продвинутыми знаниями технологий при ограниченных ресурсах и способные к ограниченному планированию. В категорию C входят хакеры, обладающие некоторыми ограниченными знаниями и ресурсами, но не склонные к планированию. Наконец, к категории D относятся хакеры, для которых совершение киберпреступлений является в терминологии К. Левина полевым повелением — те, кто не обладают ни специальными знаниями, ни ресурсами, действуют только тогда, когда видят легкую возможность, и реализуют свои идеи немедленно без какого-либо предварительного планирования.

Основное ограничение этой модели — ее опора на субъективный, пусть и обширный, опыт без научно-доказательной основы, которая позволила бы объяснить, почему эта модель включает в себя именно четыре категории. Она обобщает имеющиеся знания, но не объясняет поведения киберпреступников и может препятствовать обнаружению новых категорий, допустим, сочетающих высокий уровень технических компетенций с невниманием к стратегическому планированию.

Еще один вариант реализации поведенческого подхода к кибербезопасности — использование инструментария математической теории игр. Под игрой в данном случае понимается стратегическое взаимодействие двух и более лиц (игроков), преследующих строго определенные цели; при этом степень достижения своей цели каждым игроком зависит не только от его собственных действий, но и от действий других игроков [18]. Это требует в принятии решения ставить себя на место других игроков и просчитывать их действия.

По мнению инициаторов применения теории игр к анализу психологических факторов кибербезопасности, в данной области знания речь идет об играх с двумя игроками и с нулевой суммой, т. е. о таких играх, где больший размер выигрыша одного из участников возможен исключительно за счет меньшего выигрыша второго.

Конкретно, речь идет о стратегическом взаимодействии между киберпреступником, который намеревается совершить кибератаку, и киберэкспертом, который намеревается ее предотвратить.

Использование теории игр предположительно должно быть особенно эффективным при определении того, кто из круга подозреваемых может стоять за конкретным киберпреступлением [20]. Достоинством теории игр является ее высокая степень алгоритмизируемости и прозрачность обоснования выводов. Вместе с тем у этого инструмента, на наш взгляд, есть два серьезных ограничения. Первое — презумпция абсолютной рациональности всех игроков: предполагается, что участники взаимодействия не только руководствуются исключительно соотношением выгод и потерь (экономическая логика максимизации полезности), но и идеально верно просчитывают это соотношение для каждого из возможных сценариев. Кроме этого общего ограничения, которым обусловлено весьма ограниченное применение теории игр в психологии по сравнению с экономической наукой, следует отметить еще одно обстоятельство, связанное непосредственно со сферой кибербезопасности.

Учитывая изначальную асимметрию позиций киберпреступника и киберэксперта и направленность модели на идентификацию с последним, для моделирования логики принятия решений киберэксперту нужно первоначально, еще до начала использования инструментария теории игр, оценить, что является выигрышем для различных категорий киберпреступников (очевидно, что это не то же самое, что выигрыш для киберэксперта). Соответственно, применимость теории игр зависит от наличия и достоверности большого объема знаний, полученных иными, неалгоритмизируемыми и зачастую неотрефлексированными путями.

Как следствие, применение теории игр в данном случае, особенно при расследовании киберпреступлений, может давать мало новой информации, а порой и цементировать уже существовавшие предубеждения, предоставляя им дополнительную необоснованную легитимацию.

Социально-психологические исследования кибербезопасности преимущественно сводятся к экстраполяции общих закономерностей на сферу цифрового взаимодействия. Так, исследование децентрализованной распределенной цифровой группы хакеров Anonymous [16] позволило выявить, что в этой, настолько нетипичной социальной группе происходят основные групповые процессы. Осуществляется контроль над поведением членов группы при помощи неформальных механизмов — конформности, повышения престижа группы и членства в ней, создания и поддержания ролевых моделей и внутригрупповых норм. Кроме того, представители этой группы тщательно отслеживают отношение к их действиям извне и целенаправленно занимаются поддержанием своего имиджа, используя известные приемы управления впечатлениями.

Тему макросоциального и социального контекстов кибербезопасности оригинально раскрывает исследование, опубликованное в одном из журналов группы Nature [11]. Авторы исследования использовали для изучения социально-перцептивной стороны кибербезопасности технику окна Джохари.

Отправным пунктом исследования стало предположение о том, что в восприятии кибербезопасности существует некое «слепое пятно» — то, чего не осознают ни сами пользователи, ни эксперты, которые пытаются побудить пользователей к более последовательному соблюдению правил кибербезопасного поведения. В результате анализа серии специально проведенных интервью выяснилось, что таким «слепым пятном» является негативное отношение к кибербезопаности как таковой. У многих участников исследования кибербезопасность как социальный феномен в различных ее проявлениях вызывает плохо осознаваемые негативные эмоции, естественным следствием которых является желание избегать этой темы, а не осваивать новые техники защиты от кибератак. Эта эмоциональная реакция зачастую не учитывается экспертами, которые рассматривают кибербезопасность как решение проблемы, а не как феномен, вызывающий ассоциации с самой проблемой и напоминающий об угрозах, о которых пользователи предпочитают не задумываться до тех пор, пока не сталкиваются с их непосредственными последствиями.

Несмотря на предметную и методологическую разрозненность рассмотренных здесь исследований, их объединяет одна общая характеристика: все они представляют собой попытки рассмотрения того, как в сфере кибербезопасности проявляются общие явления и закономерности из различных специальных разделов психологии, будь то теории личности, модели поведения или процессы групповой динамики.

Параллельно с этим направлением существует иная категория исследований, которые направлены на изучение того, какие психологические закономерности скрываются за другим феноменом, связанным со злоупотреблением доверием интернет-пользователей, — принятием и участием в распространении ложных новостей.

Рассмотрим основные наработки в рамках этого направления.

Доверие к ложным новостям в Интернете

Проблема так называемых ложных (или фейковых) новостей в последние годы активно обсуждается и как одна из характерных особенностей современной социальной реальности, и как важный фактор социальных изменений [3]. Основной проблемой применительно к «ложным новостям» является не сам факт появления в Интернете ложных сведений, а массовость их тиражирования [1]. Соответственно, ключевой вопрос применительно к «ложным новостям» — это вопрос о причинах массовой склонности доверять явно недостоверной информации.

Различным сторонам его решения посвящен ряд эмпирических исследований, результаты которых были опубликованы в последние годы. Так, Ванг, Панг и Павлоу изучили эффективность верификации идентичности пользователей социальных медиа как средства противодействия распространению ложных новостей посредством стимулирования более ответственного поведения [25]. Было выявлено, что пользователи социальных медиа, прошедшие верификацию идентичности, действительно реже распространяют ложные новости. Более ответственное поведение применительно к тиражированию информации означает именно более последовательное и менее спонтанное принятие решений, в то время как доверие, напротив, выступает как способ экономии когнитивных усилий.

Баракат, Дарбус и Тархини [8] изучили влияние ряда факторов, влияющих на правильность распознавания ложных новостей в социальных медиа. Им удалось подтвердить, что доверие к социальным медиа как источнику информации отрицательно влияет на качество идентификации ложных новостей. Кроме того, доверие к социальным медиа имеет и опосредующий эффект, ослабляя влияние осведомленности: даже те пользователи, которые хорошо ориентируются в механизмах функционирования социальных медиа и обучены специальным навыкам проверки подлинности информации, реже используют эти компетенции по назначению, если склонны доверять источнику получаемой ими информации.

Мюллер и Шульц [17] изучили, каким образом поведение, направленное на проверку подлинности информации, получаемой из социальных медиа, связано с отношением к этим социальным медиа и осведомленностью о самой проблеме ложных новостей. Как выяснилось, связи более специфичны, чем это можно предположить. Так, общая осведомленность о проблеме и оценка объема ложных новостей, с которыми участники исследования, согласно их представлениям, вынуждены сталкиваться в своей повседневной жизни, сами по себе не связаны с отношением к конкретным социальным медиа. С этим отношением значимо связаны представления о том, насколько высока вероятность встретить «ложные новости» именно в этих социальных медиа (отрицательная связь) и в так называемых традиционных медиа (положительная связь).

Венцель [26], использовав метод фокус-групп, выяснил, что их участники осознают проблему ложных новостей и используют для ее решения ограниченный набор стратегий — фактчекинг, уход от проблемы путем ограничения объема потребляемых интернет-ресурсов, особенно информационных (эта стратегия была выявлена в исследовании отечественных психологов Фролова и Чернова в условиях потребления большого объема негативных новостей [6]), и ограничение источников информации теми, по отношению к которым интернет-пользователь испытывает доверие и априорно переносит это доверие на любую информацию, поступающую из этих источников, т. е. путем формирования «информационного пузыря» [9; 19].

Розенбек и ван дер Линден [21] предложили иную стратегию работы с ложными новостями, основанную на понимании того, как эти новости создаются. Участникам исследования предлагалось в форме онлайн-игры освоить шесть приемов создания «ложных новостей» (поляризацию, стимулирование эмоций, распространение конспирологических теорий, троллинг, переключение вины и использование фейковых аккаунтов). Апробация этой игры показала, ее эффективность: вместо диффузного недоверия к информации, поступающей из интернет-источников, у участников исследования формировалось более избирательное недоверие, основанное на освоенных ими признаках ложных новостей.

Карраско-Фарре также задался вопросом по поводу отличительных особенностей «ложных новостей», однако, в отличие от предыдущего исследования, изучил не отличительные особенности приемов их создания, а отличия по степени психологического воздействия на целевую аудиторию [10]. Согласно полученным им результатам, ложные новости отличаются большей простотой для восприятия и большей эмоциональной насыщенностью, особенно в отношении отрицательных эмоций. Опасность «ложных новостей» состоит не только в том, что они насыщают информационное пространство ложной информацией, но и тем, что они зачастую вызывают большое доверие, вероятно, не в последнюю очередь потому, что создаются намеренно с целью манипулятивного воздействия и их авторы отслеживают это воздействие на аудиторию более осознанно, чем те, кто просто делится своими взглядами.

Проблема обучения распознаванию «ложных новостей» находится в центре внимания в исследовании Аслетта с соавторами [23]. Серия проведенных ими экспериментов показала, что парадоксальным образом те участники исследования, которые уделяли больше внимания проверке достоверности и надежности информации, в итоге чаще начинали доверять «ложным новостям», чем те, кто принимал решение без дополнительных усилий. Это объясняется тем, что в качестве способа проверки достоверности и надежности использовался онлайн-поиск и сопоставление информации, найденной в дополнительных источни-

ках, с исходным материалом — объектом оценки. Как выяснилось, во многих случаях бо́льшая, если не основная часть источников, получаемых в результате такого поиска, сами являются «ложными новостями», поскольку по многим темам надежные источники отсутствуют. Это согласуется с рекомендациями отечественных авторов Кочетовой и Климаковой, которые считают предоставление большего объема достоверной информации по актуальным вопросам эффективным средством борьбы с ложной информацией, даже без прямого разоблачения последней [2].

Еще одно направление изучение восприятия и поведения в отношении «ложных новостей» — изучение того, какие стимулы могут побудить интернет-пользователей осуществлять самостоятельный контроль над распространением ложных новостей. Гимпель с соавторами [24] изучили, каким образом формируется нормативное регулирование поведения, направленного на активное противодействие распространению «ложных новостей». Результаты исследования показали, что воздействие прескриптивных сообщений о социальных нормах значимо способствовало увеличению частоты желаемого поведения, т. е. уведомления о «ложных новостях», в то время как дескриптивные сообщения сами по себе не имели статистически значимого эффекта (вопреки тому, что можно было бы ожидать исходя из теории социального научения через подражание), однако в сочетании с ними прескриптивные сообщения оказывали более интенсивное воздействие, чем без них. Таким образом, прямое указание на желаемую модель поведения ослабляет пассивное доверие к «ложным новостям». Вместе с тем Гвебу с соавторами [12] изучили эффективность прямых предупреждений о ложных новостях и обнаружили, что более высокий уровень доверия и большая готовность трансформировать его в поведение несмотря на предупреждения наблюдались в том случае, когда содержание ложных новостей подтверждало уже имевшиеся у пользователя взгляды и убеждения. Это означает, что помимо эффекта «информационной пустоты» из-за преобладания «ложных новостей» среди результатов интернет-поиска на заданную тему может играть свою роль также готовность прекратить поиск быстрее, чем в случае, когда первые, относительно легко найденные источники опровергают исходное сообщения, а не подтверждают его. Таким образом, наибольшим доверием, как следует из результатов рассмотренных исследований, будут пользоваться, во-первых, сообщения на остро актуальную тему: во-вторых, сообщения, содержащие положительно оцениваемую субъектом доверия информацию, подтверждающую уже сформированные у него взгляды; в-третьих, прескриптивные сообщения, содержащие не только описание ситуации, но и прямое указание к действию.

Выводы

Проведенный обзор исследований позволяет считать, что в изучении закономерностей кибербезопасного поведения и его обеспечения продолжают доминировать технологические подходы, а психологические исследования остаются фрагментарными как по тематическому охвату, так и по конкретным результатам. Можно ожидать, что по мере исчерпания ресурсов чисто технологических программ обеспечения кибербезопасности при неизменной или даже растущей актуальности проблемы на первый план выйдет «человеческий фактор», а на смену констатациям его недостаточной изученности придет рост количества психологических исследований и обретение ими системного характера.

Судя по рассмотренным публикациям, личностные и иные психологические характеристики хакеров и иных киберпреступников, создающих угрозу кибербезопасности, несмотря на их экзотическую деятельность, мотивацию и опыт, представляются не только более изученными, но и более понятными, чем психологические особенности обычных пользователей. Это объясняется тем, что поведение киберпреступников интенционально, осознанно и основано на экспертном знании, в то время как поведение обычных пользователей, в том числе создающее угрозы кибербезопасности, намного более хаотично и, по-видимому, представляет собой сочетание импульсивных реакций, поведенческих стереотипов, когнитивных эвристик и более или менее удачных попыток последовательной обработки информации на фоне характерной для цифровой эпохи постоянной информационной перегрузки.

В исследования доверия к ложным новостям, напротив, основное внимание уделяется именно психологическим факторам, причем в большей мере ситуативным и социально-когнитивным, чем личностно-психологическим; последние в большей степени рассмотрены в работах отечественных психологов [4; 5; 7]. Склонность доверять ложным новостям предстает в качестве универсальной проблемы, а не следствием конкретных личностных черт. В ряде рассмотренных публикаций показано, что общая осведомленность как о проблеме ложных новостей, так и об угрозах кибербезопасности сама по себе не является решением проблемы. Более того, на фоне общего сниженного доверия к информационной составляющей интернет-среды эти попытки дополнительно его снизить могут в качестве непреднамеренных последствий приводить к росту общего эмоционального напряжения и, как следствие, к повышению вероятности наиболее простых импульсивных реакций — т. е. поведения, прямо противоположного кибербезопасному.

Более эффективной альтернативой, основанной на запросе на надежность и обоснованное доверие, может стать рутинизация кибербезопасности. Ее целью должно стать не просто формирование отдельных привычек кибербезопасного поведения (таких как регулярное обновление паролей) и распознавание отдельных угроз, но восприятие этих угроз и ложных новостей как чего-то знакомого и закономерного — не как загадочных явлений, нарушающих привычную картину мира, а, напротив, как органичной ее части.

Литература

1. *Казун А.Д.* Так ли страшен фейк? Ложные новости и их роль в современном мире // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 4(158). С. 162—175. DOI:10.14515/monitoring.2020.4.791

2. *Кочетова Ю.А., Климакова М.В.* Зарубежный опыт профилактики стресса, связанного с пандемией COVID-19 // Современная зарубежная психология. 2023. Том 12. № 2. С. 84—93. DOI:10.17759/jmfp.2023120208

3. *Марочкина С.С., Круглова М.С., Круглова Л.Э.* Медиабезопасность аудитории СМИ в современном информационном пространстве // Вопросы безопасности. 2023. № 1. С. 42—50. DOI:10.25136/2409-7543.2023.1.39836

4. *Михеев Е.А.* Психологические механизмы продвижения недостоверной информации в сети Интернет // Психопедагогика в правоохранительных органах. 2021. Том 26. № 4(87). С. 423—434. DOI:10.24412/1999-6241-2021-4-87-423-434

5. *Михеев Е.А., Нестик Т.А.* Психологические механизмы инфодемии и отношение личности к дезинформации о COVID-19 в социальных сетях // Институт психологии Российской академии наук. Социальная и экономическая психология. 2021. Том 6. № 1(21). С. 37—64. DOI:10.38098/ipran.sep.2021.21.1.002

6. *Фролов И.С., Чернов А.Ю.* Психологические аспекты восприятия негативных новостей в сети Интернет // Вектор науки Тольяттинского государственного университета. Серия: Педагогика, психология. 2023. № 3(54). С. 76—82. DOI:10.18323/2221-5662-2023-3-76-82

7. *Яновский М.И., Малишевская Е.В.* Личностные свойства, способствующие нераспознаванию лжи // Психология и психотехника. 2023. № 4. С. 72—85. DOI:10.7256/2454-0722.2023.4.68728

8. *Aoun Barakat K., Dabbous A., Tarhini A.* An empirical approach to understanding users' fake news identification on social media // Online Information Review. 2021. Vol. 45. № 6. P. 1080—1096. DOI:10.1108/OIR-08-2020-0333

9. *Bruns A.* Are filter bubbles real? Cambridge: Polity Press, 2019. 160 p.

10. *Carrasco-Farr C.* The fingerprints of misinformation: how deceptive content differs from reliable sources in terms of cognitive effort and appeal to emotions // Humanities and Social Sciences Communications. 2022. Vol. 9. № 1. Article ID 162. 18 p. DOI:10.1057/s41599-022-01174-9

11. Exploring cybersecurity-related emotions and finding that they are challenging to measure / K. Renaud, V. Zimmermann, T. Schrmann, C. Bhm // Humanities and Social Sciences Communications. 2021. Vol. 8. Article ID 75. 17 p. DOI:10.1057/s41599-021-00746-5

12. *Gwebu K.L., Wang J., Zifla E.* Can warnings curb the spread of fake news? The interplay between warning, trust and confirmation bias // Behaviour & Information Technology. 2022. Vol. 41. № 16. P. 3552—3573. DOI:10.1080/0144929X.2021.2002932

13. Hacker types, motivations and strategies: A comprehensive framework / S. Chng, H.Y. Lu, A. Kumar, D. Yau // Computers in Human Behavior Reports. 2022. Vol. 5. Article ID 100167. 8 p. DOI:10.1016/j.chbr.2022.100167

14. *Kennison S.M., Chan-Tin E.* Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors // Frontiers in Psychology. 2020. Vol. 11. Article ID 546546. 9 p. DOI:10.3389/fpsyg.2020.546546

15. *McAlaney J., Benson V.* Chapter 1 — Cybersecurity as a social phenomenon // Cyber influence and cognitive threats / Eds. V. Benson, J. McAlaney. New York: Academic Press, 2020. P. 1—8. DOI:10.1016/B978-0-12-819204-7.00001-4

16. *McAlaney J., Taylor J., Faily S.* The social psychology of cybersecurity [Электронный ресурс] // The social psychology of cybersecurity: In Proceedings of the 1st International conference on cyber security for sustainable society: g. Coventry, 26—27 February 2015. London: Sustainable Society Network, 2015. 14 p. URL: https://rgu-repository.worktribe.com/output/1427756/the-social-psychology-of-cybersecurity (дата обращения: 25.10.2024).

17. *Müller P., Schulz A.* Facebook or Fakebook? How users' perceptions of 'fake news' are related to their evaluation and verification of news on Facebook // Studies in Communication and Media. 2019. Vol. 8. № 4. P. 547—559. DOI:10.5771/2192-4007-2019-4-547

18. *Owen G.* Game theory. Bingley: Emerald Group Publishing, 2013. 500 p.

19. *Pariser E.* The filter bubble: How the new personalized web is changing what we read and how we think. New York: Penguin Press, 2011. 375 p.

20. *Patterson W., Winston-Proctor C.E.* Behavioral cybersecurity: Applications of personality psychology and computer science. Boca Raton: CRC Press, 2019. 47 p. DOI:10.1201/9780429461484

21. *Roozenbeek J., Van der Linden S.* The fake news game: actively inoculating against the risk of misinformation // Journal of risk research. 2019. Vol. 22. № 5. P. 570—580. DOI:10.1080/13669877.2018.1443491

22. *Shappie A.T., Dawson C.A., Debb S.M.* Personality as a predictor of cybersecurity behavior // Psychology of Popular Media. 2020. Vol. 9. № 4. P. 475—480. DOI:10.1037/ppm0000247

23. Testing the Effect of Information on Discerning the Veracity of News in Real Time / K. Aslett, Z. Sanderson, W. Godel, N. Persily, J. Nagler, R. Bonneau, J.A. Tucker // Journal of Experimental Political Science. 2023. Vol. 11. № 3. P. 262—276. DOI:10.1017/XPS.2023.20

24. The effectiveness of social norms in fighting fake news on social media / H. Gimpel, S. Heger, C. Olenberger, L. Utz // Journal of Management Information Systems. 2021. Vol. 38. № 1. P. 196—221. DOI:10.1080/07421222.2021.1870389
25. *Wang S.A., Pang M.S., Pavlou P.A.* Seeing is believing? How including a video in fake news influences users' reporting of the fake news to social media platforms // MIS Quarterly. 2022. Vol. 46. № 3. P. 1323—1354. DOI:10.2139/ssrn.3909942
26. *Wenzel A.* To verify or to disengage: Coping with "fake news" and ambiguity [Электронный ресурс] // International Journal of Communication. 2019. Vol. 13. P. 1977—1995. URL: https://ijoc.org/index.php/ijoc/article/viewFile/10025/2636 (дата обращения: 25.10.2024).

References

1. Kazun A.D. Tak li strashen feik? Lozhnye novosti i ikh rol' v sovremennom mire [Are Fakes Really Dangerous? Fake News and Their Role in the Modern World]. *Monitoring obshchestvennogo mneniya: ekonomicheskie i sotsial'nye peremeny = Monitoring of Public Opinion: Economic and Social Changes*, 2020, no. 4(158), pp. 162—175. DOI:10.14515/monitoring.2020.4.791 (In Russ.).
2. Kochetova Y.A., Klimakova M.V. Zarubezhnyi opyt profilaktiki stressa, svyazannogo s pandemiei COVID-19 [Foreign Experience in the Prevention of the COVID-19 Pandemic Stress]. *Sovremennaya zarubezhnaya psikhologiya = Journal of Modern Foreign Psychology*, 2023. Vol. 12, no. 2, pp. 84—93. DOI:10.17759/jmfp.2023120208 (In Russ.).
3. Marochkina S.S., Kruglova M.S., Kruglova L.E. Security of the Media Audience in the Modern Information Space [Mediabezopasnost' auditorii SMI v sovremennom informatsionnom prostranstve]. *Voprosy bezopasnosti = Security Issues*, 2023, no. 1, pp. 42—50. DOI:10.25136/2409-7543.2023.1.39836 (In Russ.).
4. Mikheev E.A. Psikhologicheskie mekhanizmy prodvizheniya nedostovernoi informatsii v seti Internet [Psychological Mechanisms of Promoting False Information on the Internet]. *Psikhopedagogika v pravookhranitel'nykh organakh = Psychopedagogics in Law Enforcement*, 2021. Vol. 26, no. 4(87), pp. 423—434. DOI:10.24412/1999-6241-2021-4-87-423-434 (In Russ.).
5. Mikheev E.A., Nestik T.A. Psikhologicheskie mekhanizmy infodemii i otnoshenie lichnosti k dezinformatsii o COVID-19 v sotsial'nykh setyakh [Psychological Mechanisms of Infodemic and Personal Attitudes to Disinformation About Covid-19 in Social Media]. Institut psikhologii Rossiiskoi akademii nauk. *Sotsial'naya i ekonomicheskaya psikhologiya = Institute of Psychology Russian Academy of Sciences. Social and Economic Psychology*, 2021. Vol. 6, no. 1(21), pp. 37—64. DOI:10.38098/ipran.sep.2021.21.1.002 (In Russ.).
6. Frolov I.S., Chernov A.Yu. Psikhologicheskie aspekty vospriyatiya negativnykh novostei v seti Internet [Psychological Aspects of Perception of Negative News on the Internet]. *Vektor nauki Tol'yattinskogo gosudarstvennogo universiteta. Seriya: Pedagogika, psikhologiya = Science Vector of Togliatti State University. Series: Pedagogy, Psychology*, 2023, no. 3(54), pp. 76—82. DOI:10.18323/2221-5662-2023-3-76-82 (In Russ.).
7. Yanovsky M.I., Malishevskaya E.V. Lichnostnye svoistva, sposobstvuyushchie neraspoznavaniyu lzhi [Personality Traits That Contribute to the Non-Recognition of Lies]. *Psikhologiya i psikhotekhnika = Psychology and Psychotechnics*, 2023, no. 4, pp. 72—85. DOI:10.7256/2454-0722.2023.4.68728 (In Russ.).
8. Aoun Barakat K., Dabbous A., Tarhini A. An empirical approach to understanding users' fake news identification on social media. *Online Information Review*, 2021. Vol. 45, no. 6, pp. 1080—1096. DOI:10.1108/OIR-08-2020-0333
9. Bruns A. Are filter bubbles real? Cambridge: Polity Press, 2019. 160 p.
10. Carrasco-Farr C. The fingerprints of misinformation: how deceptive content differs from reliable sources in terms of cognitive effort and appeal to emotions. *Humanities and Social Sciences Communications*, 2022. Vol. 9, no. 1, article ID 162. 18 p. DOI:10.1057/s41599-022-01174-9
11. Renaud K., Zimmermann V., Schrmann T., Bhm C. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 2021. Vol. 8, article ID 75. 17 p. DOI:10.1057/s41599-021-00746-5
12. Gwebu K.L., Wang J., Zifla E. Can warnings curb the spread of fake news? The interplay between warning, trust and confirmation bias. *Behaviour & Information Technology*, 2022. Vol. 41, no. 16, pp. 3552—3573. DOI:10.1080/0144929X.2021.2002932
13. Chng S., Lu H.Y., Kumar A., Yau D. Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, 2022. Vol. 5, article ID 100167. 8 p. DOI:10.1016/j.chbr.2022.100167
14. Kennison S.M., Chan-Tin E. Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, 2020. Vol. 11, article ID 546546. 9 p. DOI:10.3389/fpsyg.2020.546546
15. McAlaney J., Benson V. Chapter 1 — Cybersecurity as a social phenomenon. In Benson V., McAlaney J. (eds.), *Cyber influence and cognitive threats*. New York: Academic Press, 2020. P. 1—8. DOI:10.1016/B978-0-12-819204-7.00001-4
16. McAlaney J., Taylor J., Faily S. The social psychology of cybersecurity [Electronic resource]. The social psychology of cybersecurity: In *Proceedings of the 1st International conference on cyber security for sustainable society: g. Coventry, 26—27 February 2015*. London: Sustainable Society Network, 2015. 14 p. URL: https://rgu-repository.worktribe.com/output/1427756/the-social-psychology-of-cybersecurity (Accessed 25.10.2024).

17. Müller P., Schulz A. Facebook or Fakebook? How users' perceptions of 'fake news' are related to their evaluation and verification of news on Facebook. *Studies in Communication and Media*, 2019. Vol. 8, no. 4, pp. 547—559. DOI:10.5771/2192-4007-2019-4-547
18. Owen G. Game theory. Bingley: Emerald Group Publishing, 2013. 500 p.
19. Pariser E. The filter bubble: How the new personalized web is changing what we read and how we think. New York: Penguin Press, 2011. 375 p.
20. Patterson W., Winston-Proctor C.E. Behavioral cybersecurity: Applications of personality psychology and computer science. Boca Raton: CRC Press, 2019. 47 p. DOI:10.1201/9780429461484
21. Roozenbeek J., Van der Linden S. The fake news game: actively inoculating against the risk of misinformation. *Journal of risk research*, 2019. Vol. 22, no. 5, pp. 570—580. DOI:10.1080/13669877.2018.1443491
22. Shappie A.T., Dawson C.A., Debb S.M. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 2020. Vol. 9, no. 4, pp. 475—480. DOI:10.1037/ppm0000247
23. Aslett K., Sanderson Z., Godel W., Persily N., Nagler J., Bonneau R., Tucker J.A. Testing the Effect of Information on Discerning the Veracity of News in Real Time. *Journal of Experimental Political Science*. Vol. 11, no. 3, pp. 262—276. DOI:10.1017/XPS.2023.20
24. Gimpel H., Heger S., Olenberger C., Utz L. The effectiveness of social norms in fighting fake news on social media. *Journal of Management Information Systems*, 2021. Vol. 38, no. 1, pp. 196—221. DOI:10.1080/07421222.2021.1870389
25. Wang S.A., Pang M.S., Pavlou P.A. Seeing is believing? How including a video in fake news influences users' reporting of the fake news to social media platforms. *MIS Quarterly*, 2022. Vol. 46, no. 3, pp. 1323—1354. DOI:10.2139/ssrn.3909942
26. Wenzel A. To verify or to disengage: Coping with "fake news" and ambiguity [Electronic resource]. *International Journal of Communication*, 2019. Vol. 13, pp. 1977—1995. URL: https://ijoc.org/index.php/ijoc/article/viewFile/10025/2636 (Accessed 25.10.2024).

Информация об авторах
Фабрикант Маргарита Сауловна, кандидат психологических наук, кандидат социологических наук, ведущий научный сотрудник лаборатории сравнительных исследований массового сознания Экспертного института, Национальный исследовательский университет «Высшая школа экономики» (ФГАОУ ВО «НИУ ВШЭ»), г. Москва, Российская Федерация; доцент кафедры социальной и организационной психологии факультета философии и социальных наук, Белорусский государственный университет (БГУ), г. Минск, Республика Беларусь, ORCID: https://orcid.org/0000-0001-5707-2943, e-mail: marharyta.fabrykant@gmail.com

Information about the authors
Marharyta S. Fabrykant, PhD in Psychology, PhD in Sociology, Leading Research Fellow, Laboratory for Comparative Studies in Mass Consciousness, Expert Institute, HSE University, Moscow, Russia; Associate Professor, Chair of Social and Organizational Psychology, Faculty of Philosophy and Social Sciences, Belarusian State University, Minsk, Belarus, ORCID: https://orcid.org/0000-0001-5707-2943, e-mail: marharyta.fabrykant@gmail.com

Получена 01.07.2023
Принята в печать 30.09.2024

Received 01.07.2023
Accepted 30.09.2024