Экономические и социально-гуманитарные исследования. 2024. № 3 (43). С. 196—204.
Economic and Social Research. 2024. No. 3 (43). P. 196—204.
Научная статья

УДК 004.77: 004.056+159.9+37+613.8
doi: 10.24151/2409-1073-2024-3-196-204
https://elibrary.ru/ccihvd

Обеспечение безопасности в сети Интернет: психолого-педагогические аспекты

В. Л. Мрочко[1], Т. М. Рощина[2], М. Д. Тарасов[3]

[1] ООО «Центр Специальных Проектов Консалтинг», Москва, Россия
[2, 3] Московский гуманитарный университет, Москва, Россия

[1] dr.discussion@yandex.ru
[2] reklama.vo.mosgu@mail.ru
[3] MKStarasoff@yandex.ru

Аннотация. Рассматриваются информационные риски психофизиологическому здоровью пользователей в сети Интернет. Выявляются факторы, способствующие кибербуллингу, анализируются последствия цифрового преследования, домогательства и запугивания, побуждения к противоправным и аморальным действиям. Обозначаются основные направления правоохранительной деятельности по осуществлению мер конфиденциальности и безопасности, способы защиты молодежи от сталкинга и газлайтинга. Раскрываются психолого-педагогические методы укрепления морально-нравственного здоровья личности и особенности современной программы образования в решении проблемы социальной и коммуникативной подготовки личности, адаптированной к киберугрозам.

Ключевые слова: информационные риски, психофизиологическое здоровье, безопасность личности, морально-нравственное здоровье, цифровое преследование, кибербуллинг, сталкинг, газлайтинг, психолого-педагогические методы, защита от киберугроз

Для цитирования: Мрочко В. Л., Рощина Т. М., Тарасов М. Д. Обеспечение безопасности в сети Интернет: психолого-педагогические аспекты // Экономические и социально-гуманитарные исследования. 2024. № 3 (43). С. 196—204. https://doi.org/10.24151/2409-1073-2024-3-196-204 EDN: CCIHVD.

Original article

Safety ensuring on the Internet: psychological and pedagogical aspects

V. L. Mrochko[1], T. M. Roshchina[2], M. D. Tarasov[3]

[1] OOO “Center for Special Projects Consulting”, Moscow, Russia
[2, 3] Moscow State University for the Humanities, Moscow, Russia

[1] dr.discussion@yandex.ru
[2] reklama.vo.mosgu@mail.ru
[3] MKStarasoff@yandex.ru

Abstract. Information risks to the psychophysiological health of users on the Internet are considered. Factors contributing to cyberbullying are identified; the authors analyze the effects of digital harassment, victimization and intimidation, and inducement to illegal and immoral actions. The main directions of law enforcement activity on implementation of confidentiality and security measures, methods of protection of youth from stalking and gaslighting are outlined. Psychological and pedagogical methods of promoting the moral health of the individual and peculiarities of modern education program in solving the problem of social and communicative training of an individual adapted to cyber threats have been disclosed.

Keywords: information risks, psychophysiological health, personal safety, moral health, digital harassment, cyberbullying, stalking, gaslighting, psychological and pedagogical methods, cyberthreats protection

For citation: Mrochko V. L., Roshchina T. M., Tarasov M. D. “Safety Ensuring on the Internet: Psychological and Pedagogical Aspects”. *Economic and Social Research* 3 (43) (2024): 196—204. (In Russian). https://doi.org/10.24151/2409-1073-2024-3-196-204 EDN: CCIHVD.

Специалисты в последние годы фиксируют в российском сегменте цифрового пространства сети Интернет значительное увеличение количества негативного контента. Роскомнадзор ежегодно блокирует тысячи сайтов, содержащих недостоверную информацию, с элементами экстремистского характера. По данным Роскомнадзора, в период с начала 2022 г. по конец 2023 г. было выявлено и заблокировано 30 тыс. призывов к массовым беспорядкам, 190 тыс. материалов с недостоверной информацией, 85 тыс. материалов с элементами экстремистского контента. В первое полугодие 2023 г. объем негативного контента в Интернете вырос более чем на 16 % по сравнению с аналогичным периодом 2022 г. Руководитель мониторингового центра «Безопасность 2.0» Елена Сутормина сообщила, что «сотрудники центра за шесть месяцев 2023 года выявили около 20 тыс. таких материалов» [9]. Таким образом, сеть Интернет сегодня содержит информационные угрозы и риски как для психофизиологического здоровья человека, так и для морально-нравственного здоровья общества в целом.

Психологическая безопасность личности в цифровой среде — это совокупность сложившихся объективных условий и субъективных факторов, которые дают человеку возможность и право самостоятельно и сознательно формировать свои идеи, регулировать собственное морально-нравственное состояние и эмоциональное поведение вне зависимости от явного или скрытого внешнего информационного воздействия [12]. Законодательство РФ определяет формы информационно-психологического воздействия, регламентирует противодействие им и борьбу с ними [9]. Так, запрещены публичные выступления и публикации, содержащие порнографию, насилие и жестокость, пропагандирующие нетрадиционные сексуальные отношения, педофилию, смену пола и др. Однако число аморальных и экстремистских идеологий множится. Обратим внимание на идеологию чайлдфри (англ. *child-free*). Наряду с другими аморальными и экстремистскими идеями ЛГБТ-сообществ, эта идея отказа от рождения детей активно пропагандируется среди населения западных стран и насаждается сегодня российской молодежи через СМИ.

На сессии «Семья: сохранить, нельзя потерять» в рамках Петербургского международного юридического форума [13], состоявшегося в июне 2024 г., было заявлено, что в России разрабатывается законопроект, запрещающий идеологию чайлдфри. Наиболее распространена сегодня в России такая

информационная угроза психофизиологическому здоровью, как кибербуллинг. Сложность этой проблемы в том, что кибербуллинг использует цифровые платформы для нанесения вреда, запугивания или преследования людей. Через текстовые сообщения, комментарии в социальных сетях, на форумах и даже в онлайн-играх осуществляется «киберзапугивание». Оно может быть направлено на людей любого возраста, но особенно распространено среди детей и подростков.

Перечислим факторы, способствующие оказанию вредоносного психологического воздействия кибербуллинга через сеть Интернет:

1. Анонимность, обеспечиваемая Интернетом, позволяет киберхулиганам скрывать свою личность, что облегчает им совершение вредоносного поведения без непосредственных последствий для них.

2. Обезличенность цифрового нападения и отсутствие прямого контакта с киберхулиганом может подтолкнуть человека к аморальным и противоправным действиям.

3. Идеологически опасные сообщения, изображения или видео быстро распространяются и достигают большой аудитории.

4. Длительное сохранение провокационной информации приводит к эмоциональному расстройству жертвы.

5. Цифровая природа онлайн-контента усиливает негативное воздействие кибербуллинга, поскольку адресация контента регулярно повторяется, что нивелирует возможность избежать информационного преследования.

6. Круглосуточная доступность Интернета, а значит, непрекращающийся характер воздействия [2; 3].

Психологические последствия кибербуллинга: непрерывный стресс, тревога, депрессия и снижение самооценки, постоянный страх и унижение, которые могут привести к социальной замкнутости, изоляции и даже суицидальным мыслям, нарушить режим сна, повлиять на успеваемость в учебе и успешность в работе. Психологический эффект киберзапугивания выходит далеко за рамки непосредственного воздействия: жертвы продолжают страдать от психологической травмы, помимо недоверия к сетевому взаимодействию испытывают трудности в формировании новых отношений и проблемы с восстановлением уверенности в себе [4].

Сообщить о случаях кибербуллинга зачастую непросто, поскольку нет рекламы, подсказывающей, к кому обращаться за помощью и как действовать в подобных ситуациях. Важно, чтобы жертвы имели доступ к ресурсам и системам поддержки, как онлайн, так и офлайн, включая телефоны доверия, специалистов по психическому здоровью и специализированные организации по борьбе с киберзапугиванием [10]. Поэтому следует разработать систему мер поддержки пострадавших от кибербуллинга. Перечислим основные направления этой правоохранительной деятельности.

Во-первых, следует проконсультировать родителей, школьных педагогов-психологов, мотивировать к необходимости максимального внимания к детям и подросткам, в поведении которых начали проявляться психологические отклонения.

Во-вторых, борьба с киберзапугиванием требует коллективных усилий, целенаправленной деятельности сообществ, образовательных учреждений и государственных онлайн-платформ в продвижении цифровой грамотности, воспитании сопереживания.

Обратим внимание на информационно-психологические риски и угрозы морально-нравственному здоровью личности в Интернете. Прежде всего такие риски и угрозы порождены преследованием в Интернете — преднамеренным и неоднократным использованием цифровых платформ для запугивания людей и домогательства. Оно может

включать отправку оскорбительных или угрожающих сообщений, распространение ложных сведений (слухов) или публичный позор. Преследование подразумевает сбор личной информации, наблюдение за деятельностью и попытки контроля. В июне 2024 г. на круглом столе, посвященном противодействию навязчивому преследованию, представители общественности обсуждали новый вариант законопроекта о сталкинге [8].

Интернет обеспечивает определенную степень анонимности и дистанции, что способствует созданию фальшивых профилей или анонимных аккаунтов с целью усложнить задачу идентификации преследователей и противостояния противоправным действиям, создать у жертвы ощущение беспомощности и страха.

Обозначим психологические последствия домогательства и преследования. Это доведение стресса до третьей стадии — от тревоги и страха за свою безопасность до снижения сопротивления. Тактика постоянного вторжения в личную жизнь жертвы за счет использования цифровых данных направлена на потерю приватности и приводит к ощущению слежки, нарушению сна, социальной замкнутости и ухудшению общего самочувствия.

Домогатели и преследователи часто меняют тактику эмоционального манипулирования своими жертвами, используют технику газлайтинга, чтобы заставить жертву сомневаться в собственном восприятии и опыте. Цель газлайтера — исказить ситуацию так, чтобы обесценить чувства и мысли жертвы и получить возможность управлять реальностью жертвы. Специалисты советуют: во-первых, сохранять электронные документы, чтобы предъявить их в качестве доказательства; во-вторых, определить триггеры, которые провоцируют манипулятора на совершение нападения, например: деньги, наследство, власть, полномочия; в-третьих, оценить, какая эмоция ранит в большей степени, и контролировать себя с помощью рефлексии.

В более широком масштабе газлайтеры создают клеветнические кампании в Интернете или распространяют ложную информацию, чтобы нанести ущерб репутации жертвы. Последствия противоправных и аморальных действий в цифровой среде охватывают и социальную, и личную жизнь жертвы. С одной стороны, потеря доверия к другим людям приводит к напряженным личным отношениям. С другой стороны, изменение поведения в социальных сетях и онлайн-платформах — ограничение общения в электронных ресурсах — еще более изолирует жертву, в частности от сообществ и сетей поддержки.

Риски усугубляются за счет транснационального характера Интернета и трудностей с идентификацией преступников [7]. Законы и нормативные акты, касающиеся преследования и домогательств в Интернете, различаются в разных юрисдикциях, поэтому жертвы могут столкнуться с препятствиями при обращении в суд.

Кроме того, огромный объем контента Интернета в открытом доступе содержит откровенные, насильственные или тревожные материалы. Случайное или преднамеренное воздействие такого контента может вызвать дистресс, тревогу и другие психологические травмы, особенно у детей и уязвимых лиц, которые более восприимчивы к негативной информации. Например, это доступ к широкому информационному материалу откровенно сексуального содержания, включая порнографию, который возможен при просмотре веб-страниц с недостоверными ссылками. Порнографическая информация в раннем возрасте искажает представление о сексуальности и потенциально провоцирует психические расстройства [6].

Особую опасность представляют видео и графические изображения, демонстрирующие насилие, несчастные случаи, жестокость

в реальной жизни. Такой контент вызывает чувство страха, тревоги и беспомощности у людей любого возраста. Неожиданность получения агрессивной информации, когда таким контентом делятся без предупреждения или надлежащего контекста, провоцирует психическую травму.

Для несовершеннолетних представляют опасность онлайн-конкурсы, побуждающие к экстремальным физическим нагрузкам или рискованному поведению. Подростки чувствуют давление, заставляющее их участвовать в конкурсе, что приводит к потенциальному физическому и психическому ущербу [11]. Ряд онлайн-платформ используют язык вражды, экстремистские идеологии или радикализирующий контент. Воздействие такого контента направлено на развитие негативных убеждений, предрассудков и нетерпимости, может привести к чувству гнева, тревоги и дистрессу.

В-третьих, образование и информационная культура развивают навыки, необходимые для ответственной навигации в сетевом мире и защиты своего психологического благополучия [17].

В 2023 г. в Российской академии народного хозяйства при Президенте РФ начата подготовка киберполицейских, специализация обучения включает расследование правонарушений в отношении граждан (кибербуллинг), юридических лиц (пиратство) или государства (экстремизм). Завкафедрой медиаобеспечения государственных интересов и национальной безопасности ИПНБ РАНХиГС Лидия Малыгина напомнила, что медиабезопасность — это комплекс мер по защите государства, общества и человека в медиапространстве: «В задачи “медиабезопасников” входит борьба с пропагандой терроризма, идеологии криминальной культуры, суицидов среди подростков, оскорбления чувств верующих. <...> Программа реализуется при поддержке Национального антитеррористического комитета» [9]. Комплексная программа направлена на повышение осведомленности пользователей о различных видах психологических угроз в Интернете. Благодаря примерам конкретных ситуаций, программа помогает пользователям понять риски, связанные с киберзапугиванием, преследованием, кражей личных данных, просмотром откровенного или тревожного контента, а также мошенничеством и обманом в Интернете, дает знания о тактиках, используемых злоумышленниками, о попытках фишинга, поддельных веб-сайтах и подозрительных ссылках. Эти знания призваны научить осторожности в предоставлении личной информации в Интернете или в общении, особенно с незнакомыми пользователями [15].

Кроме того, современное образование направлено на развитие навыков критического мышления, способности оценить онлайн-контент на предмет достоверности и потенциальных рисков, отличить надежный источник информации от ложного. Педагоги подчеркивают необходимость ответственного поведения в Интернете и соблюдения этических норм. Студентов учат относиться к другим пользователям с уважением и сочувствием, что способствует формированию цифровой культуры цивилизованного общества. Первоочередная цель современного образования — формирование профессиональных качеств личности, социально адаптированной к изменениям внешней среды, в связи с этим задачи программы воспитания направлены на умение ориентироваться в контентах Интернета, распознавать опасную информацию, использовать проверенные, государственные ресурсы, иметь чувство ответственности и сострадания к другим и контролировать свои личные данные в цифровой сфере.

Меры по обеспечению конфиденциальности и безопасности призваны защитить от психологических угроз в Интернете и снизить риск несанкционированного доступа

к личной информации или неправомерного ее использования [14].

1. Прежде всего цифровая безопасность обеспечивается созданием надежных паролей для каждой из собственных учетных записей в Интернете. Надежный пароль отличается уникальной комбинацией букв, цифр и специальных символов.

2. Основополагающим в защите от вредоносного ПО является регулярное обновление программного обеспечения, операционных систем и антивирусных программ, включая поиск и исправление лакун в системе безопасности, что помогает снизить риск несанкционированного доступа к персональным устройствам.

3. Осторожность при передаче конфиденциальных данных в Интернете предполагает использование надежных веб-сайтов, а именно с защищенным соединением HTTPS, и предоставление личной информации исключительно по электронной почте, поскольку фишинг часто маскируется под дизайн сайтов законных организаций.

4. Снизить риск кражи личных данных позволяет настройка параметров конфиденциальности на платформах социальных сетей. Эта мера защиты основана на функциях контроля видимости своих сообщений и ограничении объема личной информации, доступной другим.

5. Необходимо отслеживание вредоносных ссылок или вложений, которые могут содержать вредоносные программы или открывать фишинговые веб-сайты.

6. При доступе к общественным сетям Wi-Fi такие технологии шифрования, как виртуальные частные сети (VPN), обеспечивают дополнительный уровень безопасности. VPN шифруют данные, передаваемые между устройствами и онлайн-сервисами, что затрудняет хакерам доступ к конфиденциальной информации.

Перечисленные меры по обеспечению конфиденциальности способствуют созданию более безопасной онлайн-среды. Далее обратим внимание на меры по достижению психологического благополучия в цифровой сфере.

1. Ответственное поведение в цифровой среде обеспечивается внимательным отношением к передаваемой информации, осторожностью хранения личных данных, таких как полное имя, адрес, номер телефона, и финансовой информации.

2. Важно формировать критическое мышление для контроля взаимодействия с физическими и юридическими лицами в Интернете. Это не только осмотрительность. Критический принцип мышления означает умение опровергать ложные высказывания, обязывает проверять на прочность любую альтернативу, разрушать спекулятивную аргументацию, активно защищать истину, разрушать стереотипы в мышлении, не допускать распространения ложных мнений. Критика и самокритика в современной образовательной программе относится к коммуникативной компетентности. *Коммуникативная компетентность* — это умение передавать информацию собеседнику в соответствии с правилами коммуникации, презентовать себя в качестве субъекта общения, адекватно воспринимать и расшифровывать вербальные и невербальные послания собеседника, взаимодействовать в процессе общения, руководствуясь принципами сотрудничества, толерантности, фасилитации. Дидактические задачи развития критического мышления в образовательной программе решает метод раскрытия противоречий, его значение — в исключении ошибок в суждениях, предотвращении провалов в доказательствах, он ограждает от заблуждений и необоснованных выводов, исключает слепую веру.

3. В обеспечении онлайн-безопасности и психологического благополучия детей и уязвимых лиц играют жизненно важную роль инструменты родительского контроля

и контент-фильтры, они позволяют ограничить доступ к контенту веб-сайтов, не соответствующему возрасту. Родители и опекуны имеют возможность активно управлять использованием детьми Интернета — устанавливать ограничения, например, блокировать определенные сайты или отфильтровывать откровенные материалы, обеспечивая защиту детей от потенциально вредного или тревожного контента [16]. Регулярный контроль за деятельностью детей в Интернете имеет большое значение. Зная, какие сайты посещают их дети, какими приложениями пользуются и с кем взаимодействуют, родители могут выявить любые потенциальные риски или признаки преследования и киберзапугивания. Более того, доверительное общение между родителями и детьми на тему опыта пребывания в Интернете является необходимым условием кибербезопасности: только так можно своевременно оказать ребенку помощь и поддержку. Ознакомление детей с правилами пользования Интернетом, установление ограничения времени пользования (фильтр работы с экраном) — меры безопасности, которые помогают выработать у ребенка здоровые привычки пользования Интернетом и сохранить психологическое благополучие в семье.

4. Обучение молодежи вопросам безопасности в Интернете должно включать знания об ответственном поведении, о важности защиты личной информации от фишинга, цифровую грамотность и навыки критического мышления как возможность принимать взвешенные решения и защищать себя от фишинговых психологических атак [1; 5].

Способы обеспечения психологического здоровья общества в интернет-навигации сегодня направлены на контроль за использованием Интернета детьми, на обучение подростков мерам компьютерной безопасности и на предупреждение террористического манипулирования сознанием молодежи. Кроме того, модернизация современного образования сосредоточена на развитии полноценной личности, профессионально устойчивой и адаптированной к изменениям социальной и информационной среды. Этому способствуют дидактические принципы дискуссионного метода обучения, в частности обучение критическому мышлению, и интериоризация компетенций — коммуникативной, социальной, философско-мировоззренческой, правовой и др. — в целях умения ориентироваться в окружающей реальности. Однако этих мер для защиты от психологических угроз и рисков в цифровой среде сегодня уже явно недостаточно, поэтому представляется целесообразным включить изучение основ кибербезопасности в образовательные школьную и вузовскую программы.

Список литературы и источников

1. ***Бикамова З. И., Гимазетдинова Ю. Р., Иксанов Р. А.*** Информационная безопасность ребенка в сети Интернет // Аллея науки. 2018. Т. 2. № 4 (20). С. 145—149. EDN: XOHOXR.
2. ***Буханцева А. С., Леонтьева В. Л.*** Влияние информационного поля на поведение интернет-пользователей // Неделя науки СПбПУ: материалы науч.-практ. конф. с междунар. участием (С.-Петербург, 19—24 нояб. 2018). Ч. 1. СПб.: С.-Петерб. политехн. ун-т Петра Великого, 2019. С. 277—279. EDN: ZAEMGT.
3. ***Денисов Д. В.*** Безопасность в Интернете: защита от внешних угроз // Прикладная информатика. 2016. Т. 11. № 2 (62). С. 57—64. EDN: VVERTR.
4. ***Заболоцкая А. В., Ткачева Е. Г.*** Психологическая безопасность личности в Интернете // Автономия личности. 2022. № 1 (27). С. 91—97. EDN: PUXMVM.
5. ***Клячева А. В., Анашкина О. М.*** Информационно-психологическая безопасность подростков в сети Интернет // Актуальные проблемы безопасности жизнедеятельности в образовании: материалы Всерос. науч.-практ. конф. (Саратов, 8 февр. 2022). Саратов: Саратовский источник, 2022. С. 76—81. EDN: KWOUGT.
6. ***Лучинкина А. И., Юдеева Т. В., Ушакова В. Р.*** Информационно-психологическая безопас-

ность личности в интернет-пространстве: учеб. пособ. Симферополь: ДИАЙПИ, 2015. 151 с. EDN: VNTFSX.
7. ***Лызь Н. А., Веселов Г. Е., Лызь А. Е.*** Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Известия ЮФУ. Технические науки. 2014. № 8 (157). С. 58—66. EDN: STQREF.
8. ***Меркачева Е.*** Депутаты обсудили меры борьбы с абьюзерами и сталкерами [Электронный ресурс] // MK.ru: электрон. период. изд. / Редакция газеты «Московский комсомолец». 25.06.2024. URL: https://www.mk.ru/social/2024/06/25/deputaty-obsudili-mery-borby-s-abyuzerami-i-stalkerami.html (дата обращения: 16.07.2024).
9. ***Мишина В.*** Сетевые протоколы [Электронный ресурс]: в России начали учить на медиаполицейских // Известия: [портал]. 08.11.2023. URL: https://iz.ru/1601617/valeriia-mishina/setevye-protokoly-v-rossii-nachali-uchit-na-mediapolitceiskikh (дата обращения: 15.07.2024).
10. ***Мрочко Л. В., Пирогов А. И.*** Информационная безопасность молодежи как социокультурная проблема // Вестник Московской государственной академии делового администрирования. Серия: Философские, социальные и естественные науки. 2012. № 3 (15). С. 109—113. EDN: PMIWJX.
11. ***Ненашев С. М.*** Информационно-технологическая и информационно-психологическая безопасность пользователей сетей // Вопросы кибербезопасности. 2016. № 5 (18). С. 65—72. https://doi.org/10.21581/2311-3456-2016-5-65-72 EDN: XEFZHP.
12. Психологическая безопасность личности: учебник и практикум для вузов / А. И. Донцов, Ю. П. Зинченко, О. Ю. Зотова, Е. Б. Перелыгина. М.: Юрайт, 2024. 222 с.
13. Семья [Электронный ресурс]: сохранить, нельзя потерять // XII Петербургский международный юридический форум: [сайт]. 27.06.2024. URL: https://legalforum.info/programme/business-programme/5380/ (дата обращения: 17.07.2024).
14. Социальные сети и психологическая безопасность: учеб. пособ. для вузов / А. Г. Остапенко, Е. Б. Белов, А. О. Калашников и др.; под ред. Д. А. Новикова. М.: Горячая линия — Телеком, 2021. 232 с. (Теория сетевых войн; вып. 5.).
15. ***Строганов В. Б.*** Методы противодействия манипуляции в Интернете // Инновационный потенциал молодежи: информационная, социальная и экономическая безопасность: материалы Междунар. молод. науч.-исслед. конф. (Екатеринбург, 04—05 дек. 2017). Екатеринбург: Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина, 2017. С. 414—417. EDN: YPHRHX.
16. ***Черноситова В. А.*** Психологическая безопасность личности в Интернете // Парадигмы аппроксимации данных в науке и практике: современное состояние и перспективы развития: сб. науч. статей по итогам Междунар. межвуз. студенч. науч.-практ. конф. (С.-Петербург, 18—20 дек. 2020). СПб.: КультИнформПресс, 2020. С. 39—41. EDN: HMOOHS.
17. ***Яковлева Ю. В.*** Взаимосвязь информационной безопасности и информационной культуры // Вестник науки. 2022. № 1 (46). С. 77—81. EDN: PVTNKX.

References

1. Bikamova Z. I., Gimazetdinova Yu. R., Iksanov R. A. “Digital Security of Child in the Internet”. *Alleya nauki = Alley of Science* 2.4 (20) (2018): 145—149. (In Russian). EDN: XOHOXR.
2. Bukhantseva A. S., Leont’yeva V. L. “Influence of Information Field on Behavior of Internet Users”. *Nedelya nauki SPbPU: materialy nauch.-prakt. konf. s mezhdunar. uchastiyem* (S.-Peterburg, 19—24 noyab. 2018). Pt. 1. St. Petersburg: Peter the Great St. Petersburg Polytechnic Univ., 2019. 277—279. (In Russian). EDN: ZAEMGT.
3. Denisov D. V. “Security in the Internet: Protection against External Threats”. *Prikladnaya informatika = Journal of Applied Informatics* 11.2 (62) (2016): 57—64. (In Russian). EDN: VVERTR.
4. Zabolotskaya A. V., Tkacheva E. G. “Psychological Safety of a Person on the Internet”. *Avtonomiya lichnosti = Autonomy of the Personality* 1 (27) (2022): 91—97. (In Russian). EDN: PUXMVM.
5. Klyacheva A. V., Anashkina O. M. “Information and Psychological Safety of Adolescents on the Internet”. *Aktual’nyye problemy bezopasnosti zhiznedeyatel’nosti v obrazovanii: materialy Vseros. nauch.-prakt. konf.* (Saratov, 8 fevr. 2022). Saratov: Saratovskiy istochnik, 2022. 76—81. (In Russian). EDN: KWOUGT.
6. Luchinkina A. I., Yudeyeva T. V., Ushakova V. R. *Information and Psychological Safety of Personality in Internet Space:* study guide. Simferopol: DIAYPI, 2015. 151 p. (In Russian). EDN: VNTFSX.

7. Lyz' N. A., Veselov G. E., Lyz' A. E. "Information-Psychological Security in the Human Security and State Information Security Systems". *Izvestiya YuFU. Tekhnicheskiye nauki = Izvestiya SFedU. Engineering Sciences* 8 (157) (2014): 58—66. (In Russian). EDN: STQREF.
8. Merkacheva Eva. "Deputies Have Discussed Crackdown against Abusers and Stalkers". *MK.ru*. Moskovskiy komsomolets, 25 June 2024. (In Russian). Web. 16 July 2024. <https://www.mk.ru/social/2024/06/25/deputaty-obsudili-mery-borby-s-abyuzerami-i-stalkerami.html>.
9. Mishina Valeriya. "Network Protocols: In Russia They Started to Train Media Policemen". *Izvestiya*. OOO MITs "Izvestiya", 08 Nov. 2023. (In Russian). Web. <https://iz.ru/1601617/valeriia-mishina/setevye-protokoly-v-rossii-nachali-uchit-na-mediapolit·seiskikh>.
10. Mrochko L. V., Pirogov A.I. "Information Security of Youth as Socio-Cultural Problem". *Vestnik Moskovskoy gosudarstvennoy akademii delovogo administrirovaniya. Seriya: Filosofskiye, sotsial'nyye i estestvennyye nauki* 3 (15) (2012): 109—113. (In Russian). EDN: PMIWJX.
11. Nenashev S. "Information-Technical and Information-Psychological Security of Social-Network Users". *Voprosy kiberbezopasnosti* 5 (18) (2016): 65—72. (In Russian). https://doi.org/10.21581/2311-3456-2016-5-65-72 EDN: XEFZHP.
12. Dontsov A. I., Zinchenko Yu. P., Zotova O. Yu., Perelygina E. B. *Psychological Security of Personality:* study guide and practical course for universities. Moscow: Yurayt, 2024. 222 p. (In Russian).
13. "Preserving the Institution of the Family". *12th St. Petersburg International Legal Forum*. 27 June 2024. Web. 17 July 2024. <https://legalforum.info/ en/programme/business-programme/5380/>.
14. Ostapenko A. G., Belov E. B., Kalashnikov A. O., Los' V. P., Ostapenko O. A. *Social Networks and Psychological Security:* study guide for universities. Ed. by D. A. Novikov. Moscow: Goryachaya liniya — Telekom, 2021. 232 p. (In Russian). Teoriya setevykh voyn 5.
15. Stroganov V. B. "Methods of Counteracting Manipulation on the Internet". *Innovatsionnyy potentsial molodezhi: informatsionnaya, sotsial'naya i ekonomicheskaya bezopasnost': materialy Mezhdunar. molod. nauch.-issled. konf.* (Ekaterinburg, 04—05 dek. 2017). Ekaterinburg: Ural Federal Univ. n. a. the first President of Russia B. N. Yeltsin, 2017. 414—417. (In Russian). EDN: YPHRHX.
16. Chernositova V. A. "Psychological Safety the Person". *Paradigmy approksimatsii dannykh v nauke i praktike: sovremennoye sostoyaniye i perspektivy razvitiya: sb. nauch. statey po itogam Mezhdunar. mezhvuz. studench. nauch.-prakt. konf.* (S.-Peterburg, 18—20 dek. 2020). St. Petersburg: Kul'tInformPress, 2020. 39—41. (In Russian). EDN: HMOOHS.
17. Yakovleva Yu. V. "The Relationship of Information Security and Information Culture". *Vestnik nauki* 1 (46) (2022): 77—81. (In Russian). EDN: PVTNKX.

Информация об авторах

Мрочко Владимир Леонидович — кандидат исторических наук, генеральный директор ООО «Центр Специальных Проектов Консалтинг» (Россия, 109028, Москва, Покровский б-р, 16/10, стр. 1).

Рощина Татьяна Михайловна — старший преподаватель кафедры журналистики факультета рекламы, журналистики, психологии и искусства Московского гуманитарного университета (Россия, 111395, Москва, ул. Юности, 5).

Тарасов Максим Денисович — ведущий менеджер (супервайзер) компании «Свит Лайф Фудсервис» (Россия, 196240, Санкт-Петербург, ул. Кубинская, 84); магистрант Московского гуманитарного университета (Россия, 111395, Москва, ул. Юности, 5).

Information about the authors

Vladimir L. Mrochko — Cand. Sci. (Hist.), Director General, OOO "Center for Special Projects Consulting" (Russia, 109028, Moscow, Pokrovsky ave., 16/10, bld. 1).

Tatiana M. Roshchina — Senior Lecturer at the Department of Journalism of the Faculty of Advertising, Journalism, Psychology and Art, Moscow State University for the Humanities (Russia, 111395, Moscow, Yunosti st., 5).

Maxim D. Tarasov — Leading Manager (Supervisor), "Sweet Life Foodservice" company (Russia, 196240, St. Petersburg, Kubinskaya st., 84); Master's student, Moscow University for the Humanities (Russia, 111395, Moscow, Yunosti str., 5).

Статья поступила в редакцию после доработки 03.07.2024.

The article was submitted after updating 03.07.2024.