
ПУБЛИЧНАЯ СФЕРА В АСПЕКТЕ МАССОВЫХ КОММУНИКАЦИЙ THE PUBLIC SPHERE IN THE ASPECT OF MASS COMMUNICATIONS

Знак: проблемное поле медиаобразования. 2023. № 2 (48). С. 108–117.

eISSN 2949-3641; ISSN 2070-0695 (print).

Знак: проблемное поле медиаобразования. 2023;2(48): 108–117.

eISSN 2949-3641; ISSN 2070-0695 (print).



Научная статья

УДК 070

DOI 10.47475/2070-0695-2023-48-2-108-117

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ: РЕЗУЛЬТАТЫ СОЦИОЛОГИЧЕСКОГО ОПРОСА СТУДЕНТОВ ПРОФЕССИОНАЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Сергей Сергеевич Бредихин¹, Анна Анатольевна Морозова², Елизавета Витальевна Щетинина³

¹ Челябинский институт развития профессионального образования;

Южно-Уральский государственный университет, Челябинск, Россия, Sergei189@mail.ru,

<https://orcid.org/0000-0001-9050-5034>

^{2,3} Челябинский институт развития профессионального образования;

Челябинский государственный университет, Челябинск, Россия

² roxfan@rambler.ru, <https://orcid.org/0000-0003-4510-421X>

³ schetininaev@ya.ru, <https://orcid.org/0000-0001-9056-9126>

Аннотация. В статье исследуются вопросы цифровой безопасности в социальных сетях среди обучающихся в профессиональной образовательной организации (ПОО): медиаугрозы, с которыми они сталкиваются, проблемы и способы защиты личных страниц. Цель исследования – изучить субъективное представление о цифровой безопасности в социальных сетях студентов профессиональной образовательной организации. В качестве метода исследования выступил социологический онлайн-опрос обучающихся ПОО Челябинской области (хронологические рамки опроса – с 16 по 31 января 2023 года). Таким образом, материалом исследования стали результаты социологического опроса (N=16169). Результаты проведенного опроса относительно популярности социальных сетей полностью коррелируют с результатами крупных отечественных социологических исследований: наиболее часто за прошедший год студенты ПОО использовали сеть «ВКонтакте» и мессенджер Telegram; в целом, страница студента в социальной сети позволяет составить достаточно полное представление о человеке и его деятельности; обучающиеся на данных ресурсах наиболее часто сталкиваются с обманом и мошенничеством, взломом личной страницы, оскорблениями и угрозами в личных сообщениях, а также созданием страницы-клона; к эффективным способам защиты своего аккаунта и своей личности респонденты относят отсутствие контактов на личной странице, своевременный выход из аккаунтов на чужих устройствах, закрытие страницы для тех, кто не в друзьях, а также ограничение в размещении личной информации на странице и отсутствие геолокации. Авторы статьи приходят к выводам о недостаточной компетентности студентов в вопросах цифровой безопасности и необходимости проведения регулярных профилактических мероприятий для повышения общего уровня медиаграмотности и медиабезопасности обучающихся.

Ключевые слова: цифровая безопасность, социальные сети, студенты, профессиональная образовательная организация, социологический опрос.

Благодарности: Исследование частично выполнено при финансовой поддержке Российского научного фонда Конкурса «Проведение фундаментальных научных исследований и поисковых научных исследований отдельными научными группами» (региональный конкурс) 22–18–20011 «Цифровая грамотность: междисциплинарное исследование (региональный аспект)».

Для цитирования: Бредихин С. С., Морозова А. А., Щетинина Е. В. Цифровая безопасность в социальных сетях: результаты социологического опроса студентов профессиональных образовательных организаций // Знак: проблемное поле медиаобразования. 2023. № 2 (48). С. 108–117. doi: 10.47475/2070-0695-2023-48-2-108-117

Original article

DIGITAL SAFETY IN SOCIAL NETWORKS: SOCIOLOGICAL SURVEY RESULTS AMONG STUDENTS OF VOCATIONAL EDUCATIONAL ORGANIZATIONS

Sergei S. Bredikhin¹, Anna A. Morozova², Elizaveta V. Shchetinina³

¹ Chelyabinsk Institute for the Development of Vocational Education; South Ural State University, Chelyabinsk, Russia, Sergei189@mail.ru, <https://orcid.org/0000-0001-9050-5034>

^{2,3} Chelyabinsk Institute for the Development of Vocational Education; Chelyabinsk State University, Chelyabinsk, Russia

² roxfan@rambler.ru, <https://orcid.org/0000-0003-4510-421X>

³ schetininaev@ya.ru, <https://orcid.org/0000-0001-9056-9126>

Abstract. The article examines the issues of digital safety in social networks among students in a vocational educational organization: media threats they face, problems and ways to protect personal pages. The purpose of the study is to study the subjective idea of digital safety in social networks of students of a vocational educational organization. The sociological online survey of vocational educational organization students in the Chelyabinsk region was used as a research method (the chronological scope of the survey is from January 16 to January 31, 2023). Thus, the material of the study was the results of a sociological survey (N=16169). The results of the survey regarding the popularity of social networks are fully correlated with the results of large domestic sociological surveys – most often over the past year, vocational educational organization students used VKontakte and Telegram; in general, a student's page on a social network allows you to get a fairly complete picture of a person and his activities; students on these resources most often encounter deception and fraud; hacking a personal page, insults and threats in private messages, as well as creating a clone page; respondents refer to effective ways to protect their account and their identity: the absence of contacts on the personal page, the timely exit from accounts on other people's devices, closing the page for those who are not friends, as well as limiting the placement of personal information on the page and the lack of geolocation. The authors of the article draw the conclusion about the insufficient competence of students in matters of digital security and the need for regular preventive measures to improve the overall level of media literacy and media security of students.

Key words: digital safety, social networks, students, vocational educational organization, sociological survey.

Acknowledgments: The study was partially supported by the Russian Science Foundation Competition “Conducting fundamental scientific research and exploratory scientific research by individual scientific groups” (regional competition) 22-18-20011 “Digital Literacy: Interdisciplinary Research (Regional Aspect)”.

For citation: Bredikhin S. S., Morozova A. A., Shchetinina E. V. Digital safety in social networks: sociological survey results among students of vocational educational organizations. *Znak: problemnoe pole mediaobrazovaniya*. 2023; 2(48): 108–117. (In Russ.). doi: 10.47475/2070-0695-2023-48-2-108-117

Проблемы медиапотребления, медиаграмотности и медиабезопасности являются важным предметом для обсуждения и их перманентного изучения (Жилавская 2017; Медиапотребление «цифровой молодежи» в России 2021; Мурзина 2020; Оборский, Игнатов 2015; Пищова 2018; Фатеева 2018). Это связано с постоянно изменяющейся медиасредой, что обусловлено различными факторами: развитием цифровой среды и увеличением доли цифровизации, преобладанием в зоне внимания аудитории одних медиаресурсов над другими в определенный период времени, текущей геополитической обстановкой, потребностями и запросами пользователей Интернета и т.д.

Так, например, 2022 год внес существенные коррективы в работу социальных медиа. Были запрещены на территории Российской Федерации некоторые популярные социальные сети, следовательно, изменились информационные и рекламные потоки, вместе с этим произошло перемещение функций и контента из одних соцсетей в другие, в частности, очередной скачок в развитии получили отечественные ресурсы «ВКонтакте» и Telegram: наиболее популярной социальной сетью в апреле стала «ВКонтакте», среднесуточный охват составил 40 % населения старше 12 лет против 38 % в январе – феврале. Охват Telegram за этот период вырос с 22 % до 34 % населения, а в тройку лидеров интернет-потребления вошли соцсети (21 %), видео (18 %), мессенджеры (15 %) (<https://ict.moscow/research/mediapotrebienie-2022/?ysclid=ldshmqw14f742633755>).

Особое место Интернет и социальные медиа занимают у молодежной аудитории и являются ресурсами, удовлетворяющими ее медиапотребности (<https://wciom.ru/analytical-reviews/analiticheskii-obzor/trendy-mediapotrebieniia-2022?ysclid=ldshmsvipg578364332>), что обуславливает необходимость постоянного мониторинга и анализа результатов использования цифровой среды данной категорией населения.

Постоянное пребывание молодежи в среде социальных медиа коррелирует с проблемами их медиабезопасности, поскольку медиасреда не свободна от различного рода угроз (Гончарова, Земцова 2021;

Друкер 2019а; Друкер 2019б; Коханая, Головин 2021; Медиабезопасность и профилактика правонарушений в социальных сетях 2019).

Особое внимание стоит уделить цифровой безопасности студентов, обучающихся в профессиональной образовательной организации (Иванова 2019; Ковалева 2019; Коновалова, Мусифуллин 2022; Степанян 2019). Во-первых, возрастная аудитория 15–19 лет, в частности студенты системы среднего профессионального образования, является наиболее уязвимой категорией среди подростков и молодежи, поскольку поступление в образовательную организацию происходит за несколько лет до совершеннолетия. Не обладая определенной долей компетентности, студенты младших курсов быстро погружаются во взрослую жизнь, увеличивающую количество рисков, с которыми они могут столкнуться в цифровой среде. Во-вторых, рассмотрению уровня медиаграмотности и медиабезопасности обучающихся именно профессиональной образовательной организации посвящено крайне недостаточное количество научных трудов и различного рода исследований, поскольку основное внимание традиционно сосредоточено на подростковой аудитории или студентах вузов. В-третьих, среди обучающихся ПОО достаточно редко проводятся медиаобразовательные занятия либо не проводятся вообще, и практически исключено повышение медиаграмотности в виде последовательного и системного подхода. Следовательно, медиаграмотность и цифровая безопасность таких студентов является актуальной темой для изучения.

Цель исследования – изучить субъективное представление студентов профессиональных образовательных организаций о цифровой безопасности в социальных сетях.

Материал и методология исследования. В качестве метода исследования был выбран социологический онлайн-опрос обучающихся профессиональных образовательных организаций Челябинской области. Анкета была размещена на платформе «Яндекс Формы» и посредством централизованной рассылки отправлена в подведомственные и неподведомственные организации системы профессионального образования. Контроль качества первичных данных осуществлялся посредством оценки полноты заполнения анкет и отбраковки анкет, содержащих неполные или явно некорректные данные, касающиеся возраста, места учёбы и т. д. Анкета состояла в основном из закрытых (с вариантами ответов) и нескольких открытых вопросов (варианты ответов не были предложены). Период проведения исследования – с 16 по 31 января 2023 года. Всего было опрошено 16169 обучающихся ПОО Челябинской области.

Первично результаты опроса были обработаны автоматически средствами самой платформы опроса, затем для получения более детальных аналитических данных использовалась ручная обработка статистических данных.

Проблемы исследования:

- 1) выявить предпочтения студентов ПОО в отношении используемых социальных сетей;
- 2) определить уровень защищенности обучающимися своих страниц в социальной сети, которой они пользуются наиболее часто;
- 3) обозначить наиболее распространенные медиаугрозы, с которыми сталкивались респонденты;
- 4) сформулировать способы защиты личного аккаунта в социальных сетях, которые обучающиеся считают наиболее эффективными.

Результаты социологического опроса студентов профессиональной образовательной организации. С точки зрения социально-демографических характеристик обучающихся опрошено 58,3 % девушек и 41,7 % юношей; возраст респондентов: 15 лет – 1,3 %, 16 лет – 23,3 %, 17 лет – 26,5 %, 18 лет – 25,4 %, 19 лет – 15,2 %, 20 лет – 6,2 %, 21 год – 1,6 %, 22 года – 0,5 %. Представительность выборки позволяет рассматривать мнение опрошенных как мнение всех обучающихся ПОО в возрасте 15 лет и старше по Челябинской области со статистической погрешностью до 0,87 % при доверительном интервале 95 %.

Исследование включило в себя два смысловых блока, первый из которых был посвящен вопросам медиабезопасности, а второй – проблемам распространения экстремизма и фейковой информации в сети Интернет. В данной статье будут проанализированы вопросы первого блока.

Смысловой блок, посвященный проблемам медиабезопасности обучающихся, включил 11 вопросов.

Первый вопрос фиксировал, какой социальной сетью за последний год обучающиеся пользовались чаще всего. Вопрос имеет особую актуальность в условиях новой политики в отношении ряда социальных сетей, действующей с начала 2022 года. Ответы респондентов показывают существенное изменение в использовании социальных сетей в сравнении с данными исследования 2021 года (опрос проводился Центром мониторинга социальных сетей, в настоящее время – Научно-исследовательский центр мониторинга и профилактики деструктивных проявлений в образовательной среде). Наиболее популярной социальной сетью среди обучающихся ПОО Челябинской области является социальная сеть «ВКонтакте» – 58,5 %, на втором месте Telegram – 26,4 %, также в тройку лидеров входит «ТикТок» – 10,2 %.

Со значительным отставанием, согласно ответам респондентов, располагается «Инстаграм»¹ – 3,2 %, далее следуют «Одноклассники» – 1,3 % и «Фейсбук»² – 0,4 %.

Сравнивая данные с результатами аналогичного опроса обучающихся ПОО в ходе исследования 2021 года³, обнаруживаем значительные изменения. Так, в 2021 году пятерка лидеров по популярности среди обучающихся ПОО социальных сетей выглядела так (в порядке убывания популярности): «ВКонтакте», «Инстаграм», «ТикТок», Telegram, «Твиттер».

Второй вопрос был посвящен субъективной оценке обучающимися своей защищенности в социальных сетях. Согласно полученным ответам, большинство опрошенных считают себя скорее защищенными, чем нет (45,9 %), чуть меньшее количество опрошенных уверены, что они защищены полностью (44,5 %), в той или иной мере незащищенными себя ощущают 9,6 % опрошенных.

Указанные данные могут быть интерпретированы следующим образом. С одной стороны, малый процент тех, кто чувствует себя в той или иной мере незащищенным в социальных сетях, может свидетельствовать о том, что в целом опрошенные имеют высокий уровень доверия к системам безопасности и настройкам конфиденциальности в социальных сетях, которые они используют, и принимают меры для защиты своей личной информации и контроля над доступом к ней. Каждый десятый, указавший на свою незащищенность, возможно, лично сталкивался с проблемами безопасности в прошлом или не уверен в надежности мер защиты, которые использует. Основываясь на этом, можно говорить о достаточно высоком уровне защищенности обучающихся. С другой стороны, вопрос фиксировал именно субъективную оценку, в которой респонденты могут быть излишне оптимистичны и недооценивают реальный уровень своей незащищенности. Это подчеркивает важность повышения осведомленности о безопасности в онлайн-среде и предоставления пользователям средств и инструментов для эффективной защиты их личной информации.

Следующий вопрос был направлен на определение того, насколько открыты страницы респондентов в социальных сетях. 28,4 % опрошенных ответили, что их страница и личные сообщения полностью открыты. Это может указывать на то, что эти люди предпочитают публичность и открытость в социальных сетях. Они, скорее всего, готовы делиться своей личной информацией и контентом с широкой аудиторией и не видят необходимости в ограничении доступа к ним.

Почти такое же число опрошенных – 28 % – указали обратную ситуацию: закрыта и страница, и личные сообщения. Это может свидетельствовать о том, что эти люди предпочитают сохранять свою личную информацию и контент в приватности. Они, скорее всего, ограничивают доступ к своим профилям для дифференцированного уровня трансляции информации различным пользователям.

Другие варианты набрали меньшее число ответов: «Страница закрыта, но открыты личные сообщения» – 22,5 %; «Страница открыта, но закрыты личные сообщения» – 21,1 %. Это может означать, что эти люди применяют разные настройки приватности для различных аспектов своих профилей, чтобы найти баланс между доступностью для публики и защитой своей приватности.

Исходя из этих данных, можно сделать вывод, что предпочтения в настройках приватности в социальных сетях различны у опрошенных. Некоторые люди выбирают полную открытость, позволяя широкой аудитории получить доступ к своей личной информации и контенту. Другие предпочитают полную приватность, ограничивая доступ к своим профилям. Есть также те, кто применяет комбинированные настройки, чтобы достичь баланса между доступностью и защитой приватности. Следовательно, важно учитывать индивидуальные предпочтения и потребности пользователей при разработке политики и инструментов для защиты личной информации в социальных сетях.

Четвертый вопрос был сформулирован следующим образом: «Какая информация размещена на вашей личной странице?» Ответы представлены в таблице № 1.

Таблица 1

Виды информации, размещенной на странице в социальной сети у респондентов

Вид информации	Доля от числа опрошенных
Личное фото	71,5 %
Возраст	51,4 %
Сообщества и подписки	44,9 %
Фотографии из жизни (своей, друзей, близких)	35,6 %

¹ Запрещенная соцсеть в РФ; принадлежит корпорации Meta, деятельность которой по реализации продуктов-социальных сетей запрещена в РФ по основаниям осуществления экстремистской деятельности

² Запрещенная соцсеть в РФ; принадлежит корпорации Meta, деятельность которой по реализации продуктов-социальных сетей запрещена в РФ по основаниям осуществления экстремистской деятельности

³ Опрос проводился среди обучающихся ПОО Челябинской области, всего опрошено 11 565 человек.

Место работы / учебы	32,2 %
Место рождения / проживания	22,9 %
Личные интересы	15,0 %
Информация о семье	5,7 %
Геолокация	3,4 %

Информация всех указанных видов представлена на странице всего у 0,7 % опрошенных.

Можно сделать вывод о том, что, несмотря на незначительную долю тех, кто предоставляет полные данные о себе в открытый доступ, личные сведения различного характера в своих аккаунтах демонстрирует подавляющее большинство опрошенных. Вероятно, это указывает на имеющиеся различия взглядов у обучающихся относительно видов личной информации. Так, собственным фото готовы поделиться более 2/3 опрошенных, что может быть связано с желанием показать свою внешность, установить личные связи или просто поделиться своей жизнью с другими людьми в онлайн-среде. Однако данные о геолокации предоставляет только небольшая доля опрошенных. Вероятно, это связано с более высоким уровнем осведомленности о рисках раскрытия местоположения и желанием сохранить свою физическую безопасность и приватность.

Далее респондентов просили ответить на вопрос «Что лучше описывает ваш обычный подход к добавлению друзей в социальных сетях?». Согласно полученным ответам, абсолютное большинство опрошенных (80,3 %) добавляют в друзья только тех, кого знают лично или кому доверяют, 12,7 % не добавляют никого, кроме самых близких, меньшинство опрошенных (7,1 %) добавляют всех, кто присылает приглашения, включая незнакомых людей.

Как видно из результатов, абсолютное большинство опрошенных предпочитают добавлять в друзья только тех людей, которых они знают лично или кому доверяют. Это указывает на то, что для большинства опрошенных важна реальная связь и установленные отношения, чтобы принять решение о добавлении в друзья в социальных сетях. Они, скорее всего, стремятся поддерживать связь с реальными друзьями, знакомыми или коллегами, а также сохранять более ограниченный круг общения.

12,7% опрошенных заявили, что они не добавляют в друзья никого, кроме самых близких. Следовательно, для этих людей социальные сети в большей степени служат инструментом поддержания связи с очень ограниченным кругом людей, таким как семья и самые близкие друзья. Они, вероятно, предпочитают сохранять свою онлайн-сеть контактов очень узкой.

Меньшинство опрошенных – 7,1 % – заявили, что они добавляют в друзья всех, кто присылает приглашения, включая незнакомых людей. Это может указывать на более открытый и широкий подход к социальным сетям, где эти люди стремятся расширить свою сеть контактов и возможности для социального взаимодействия. Они могут быть более открытыми для знакомства с новыми людьми и налаживания новых связей.

Анализ результатов по данному вопросу показывает, что подход к добавлению друзей в социальных сетях является индивидуальным и зависит от предпочтений и ценностей каждого опрошенного. Важно отметить, что выбор подхода к добавлению друзей в социальных сетях может быть связан с обеспечением приватности и безопасности. Так, ограничение доступа только для знакомых людей может помочь избежать нежелательной коммуникации и контента в ленте.

Следующие четыре вопроса были посвящены выявлению тех ситуаций по основным направлениям медиаугроз, с которыми сталкивались респонденты в социальных сетях. Ответы приведены в таблице № 2.

Таблица 2

Медиаугрозы, с которыми сталкивались респонденты в социальных сетях

Сталкивались ли вы сами или ваши близкие...	Нет, такого не происходило	Да, такое случилось один–два раза	Да, такое случается иногда	Да, такое случается постоянно
со случаями преследования и домогательств в социальной сети	63,9 %	21,1 %	12 %	3,1 %

со случаями намеренных оскорблений и угроз в течение продолжительного времени (кибербуллинг) в социальной сети	58,1 %	22,6 %	14,4 %	4,8 %
с попытками неправомерного использования персональных данных в социальной сети	67,3 %	20,3 %	9,8 %	2,6 %
с обманом и мошенничеством в социальной сети	39,3 %	36 %	19,6 %	5,1 %

Полученные данные показывают, что значительное количество респондентов сталкивались с какими-либо угрозами онлайн-среды. Наибольшее число опасностей связано с обманом и мошенничеством, хотя и более серьезные виды угроз, такие как случаи домогательств и преследований, оскорблений, затрагивают немалую часть пользователей из среды обучающихся. Это во многом подтверждает гипотезу о том, что в ответе на вопрос об оценке уровня своей защищенности пользователи давали излишне оптимистичные ответы, в то время как реальная ситуация выглядит более угрожающей.

Десятый вопрос продолжил блок вопросов, направленных на фиксацию различных ситуаций медиаугроз, и был сформулирован так: «С чем из перечисленного вы или ваши близкие сталкивались хотя бы раз?» Результаты ответов представлены на диаграмме 1.

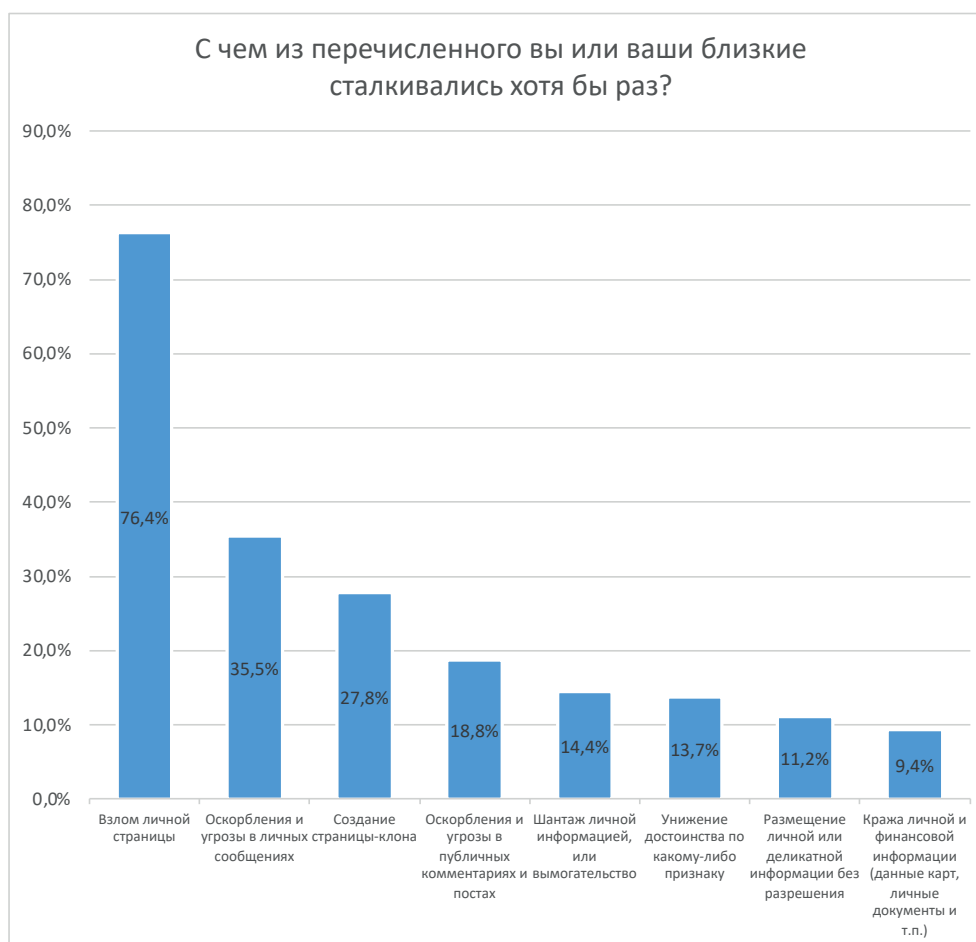


Диаграмма 1. Угрозы в социальной сети, с которыми респонденты или их близкие сталкивались хотя бы раз

И вновь результаты показывают, что в реальной практике пользователи из числа обучающихся сталкиваются с большим количеством угроз, среди которых лидирует неправомерный доступ к личной странице. Кроме того, каждый третий сталкивался с оскорблениями и угрозами в личных сообщениях, что свидетельствует о высоком уровне агрессивности онлайн-среды.

Завершающий вопрос анализируемого смыслового блока был посвящен определению того, какой из вариантов защиты личного аккаунта в социальных сетях обучающиеся считают наиболее эффективным. Согласно полученным ответам, к наиболее результативным способам респонденты относят: «Не указывать контакты (телефон, электронный адрес и т. д.)» – 57,7 %, «Не оставлять данные для входа в аккаунт на чужих устройствах» – 54,8 %, «Закрывать страницу» – 54,3 %, «Не указывать геолокацию» – 45,2 %, «Не размещать личную информацию на странице» – 44,9 %.

Менее популярны иные варианты: «Двухфакторная аутентификация» (40,6 %), «Не добавлять в друзья незнакомых людей» (35 %), «Не размещать фотографии и видеозаписи личного характера» (22,8 %), «Не указывать место работы или учебы» (22,5 %), «Не указывать город проживания» (17,7 %), «Закрывать сообщения на личной странице» (16,2 %), «Закрывать комментарии на личной странице» (12,1 %), «Не указывать личные интересы» (10,5 %), «Не пользоваться социальными сетями» (8 %).

Как видим, большинство опрошенных считают, что наиболее эффективные способы защиты их личного аккаунта в социальных сетях связаны с ограничениями раскрытия персональных данных и контролем за доступом к личному профилю.

Респонденты также предоставили ответы, которые указывают ряд мер по защите данных в качестве неэффективных. Это может говорить о разнообразии подходов и предпочтений в отношении безопасности аккаунта в социальных сетях у обучающихся. Различные факторы, такие как уровень осведомленности о настройках приватности, личный комфорт и привычки, могут влиять на выбор конкретных мер защиты.

Некоторые варианты защиты, такие как двухфакторная аутентификация, недобавление в друзья незнакомых людей или ограничение размещения фотографий и видеозаписей личного характера, имеют относительно низкую популярность среди опрошенных. Возможно, это связано с недостаточной осведомленностью о возможностях и преимуществах этих мер или недостаточной значимостью данных аспектов для опрошенных.

В целом, данные указывают на осознанность и интерес опрошенных к безопасности своих аккаунтов в социальных сетях. Большинство придерживаются основных мер защиты, таких как ограничение раскрытия контактов и личной информации. Однако существуют различия в предпочтениях и восприятии эффективности возможных мер безопасности.

Выводы. На основании полученных результатов сформулируем выводы о вопросах цифровой защищенности в социальных сетях студентов профессиональных образовательных организаций.

1. Результаты проведенного опроса относительно популярности социальных сетей полностью коррелируют с результатами крупных отечественных социологических исследований (ВЦИОМ, Mediascope): наиболее часто за прошедший год студенты ПОО использовали «ВКонтакте» и Telegram.

2. Если представить обобщенно страницу в социальной сети обучающегося ПОО, то она будет выглядеть следующим образом: чаще всего аккаунт и сообщения открыты для всех; заполнены такие данные, как личная фотография в профиле или в целом на странице, указан возраст, отображаются сообщества и подписки, нередко размещены не только свои фотографии, но и фотографии близких и друзей, обозначено место работы или учебы, что может позволить составить достаточно полное представление о человеке и его деятельности; в друзьях – те, кому респонденты доверяют, либо те, кого знают лично.

3. Студенты сталкиваются в социальных сетях с рядом угроз, а наиболее часто – с обманом и мошенничеством; также сами студенты и их близкие были подвержены взлому личной страницы (более 2/3 респондентов), оскорблениям и угрозам в личных сообщениях, а также созданию страницы-клона.

4. К наиболее эффективным способам защиты своего аккаунта и своей личности респонденты относят: отсутствие контактов (телефона, электронный адрес и т. д.) на личной странице, своевременный выход из аккаунтов на чужих устройствах и несохранение паролей на них, закрытие страницы для тех, кто не в друзьях, а также ограничение в размещении личной информации на странице и отсутствие геолокации.

5. Несмотря на то, что большинство респондентов считают себя в целом в безопасности в социальных сетях (90 %), обучающиеся сталкиваются с угрозами, а их аккаунты недостаточно защищены, что может свидетельствовать об излишне оптимистичной оценке уровня своей защищенности, являющейся следствием недооценки угроз либо недостаточного уровня медийно-информационной грамотности. Кроме того, возможно, что у обучающихся выработалась своего рода «толерантность» к различного рода угрозам и рискам в социальных сетях, благодаря которой они не воспринимают их в качестве серьезных, а представляют неискоренимым атрибутом информационного пространства.

По мнению авторов статьи, данные исследования демонстрируют достаточно субъективное представление о цифровой безопасности в социальных сетях студентов профессиональной образовательной

организации, но, тем не менее, такая информация поможет определить проблемные моменты и сформировать основные направления по профилактике цифровой безопасности данной категории обучающихся.

Несмотря на то, что студенты ПОО в целом имеют базовый уровень знаний об основных угрозах медиасреды, обладают представлением о необходимых способах защиты своего аккаунта, потреблении информации, основных аспектах безопасной коммуникации, группы обучающихся в то же время нуждаются в проведении для них профилактических мероприятий по цифровой безопасности, поскольку:

- студенты периодически сталкиваются с существующими угрозами;
- постоянно развивается цифровая среда и изменяются основные риски;
- разные студенты имеют различный уровень медийной грамотности.

На основе полученных данных авторы считают возможным в качестве рекомендаций указать следующие основные направления по достижению цифровой безопасности данной категории обучающихся.

1. Необходимость усиления работы по формированию медийно-информационной грамотности в аспекте защиты личного аккаунта и персональных данных обучающихся в социальных сетях как с технической стороны (защита паролей, двухфакторная аутентификация и т. д.), так и с точки зрения размещаемой информации, с акцентом на следующих темах:

- осознанное использование настроек приватности: пользователи должны быть ознакомлены с настройками приватности в социальных сетях и использовать их наиболее эффективно; рекомендуется активно настраивать приватность своих профилей, чтобы ограничить доступ к личной информации и контролировать, кто может видеть определенные данные и активности;
- ограничение раскрытия личных данных: важно подчеркнуть необходимость осторожности при раскрытии личных данных в социальных сетях; рекомендуется ограничивать раскрытие контактной информации, геолокации, личных интересов и других конфиденциальных сведений;
- бережное добавление новых контактов: необходимо быть внимательными при добавлении новых контактов в социальных сетях; следует придерживаться политики добавления только тех, кого пользователь знает лично или кому доверяет.

2. Необходимость разработки и внедрения алгоритмов действий для профилактики в случае столкновения с кибербуллингом (оскорбления, угрозы), киберсталкингом (домогательства, преследования), шантажом, мошенничеством и обманом.

3. Разработка и повсеместное внедрение этических норм использования социальных сетей как в процессе коммуникации, так и создания и потребления медиаконтента.

4. Постоянное обновление знаний о безопасности в социальных сетях. Технологии и методы взлома и кибератак постоянно развиваются, поэтому важно следить за обновлениями и обучаться новым методам безопасности в социальных сетях.

Итак, цифровая безопасность в социальных сетях является важной, не теряющей актуальности темой для исследования, поскольку объем личной и конфиденциальной информации на данных площадках постоянно увеличивается. По мере развития технологий меняются и методы, применяемые киберпреступниками для доступа к этой информации и способы ее использования, поэтому важно быть в курсе существующих угроз и применять надежные меры безопасности для защиты своих данных как с технической точки зрения (надежные пароли, включение двухфакторной аутентификации и т. д.), так и с содержательной – осуществлять регулярный мониторинг информации на своих аккаунтах.

Список источников

Гончарова Ю. И., Земцова Ю. В. Защита персональных данных в социальных сетях в условиях современной цифровой грамотности // Инновационные научные исследования. 2021. № 5–2 (7). С. 310–315.

Друкер М. М. Деструктивные компоненты социальных медиа // Челябинский гуманитарий. 2019а. № 4 (49). С. 27–32.

Друкер М. М. Технологии профилактики рисков и угроз психологическому здоровью школьников в социальных медиа // Поколение Z: социальный характер, идентичность и ориентации современных подростков : сборник статей Всероссийской научной конференции с международным участием, Уфа, 14–15 ноября 2019 года. Уфа : Башкирский государственный университет, 2019 б. С. 80–84.

Жилавская И. А. Медиаобразование как профилактика информационных рисков // Журналист. Социальные коммуникации. 2017. № 2 (26). С. 147–151.

Иванова Л. А. Инкорпорирование медиаобразования в программу подготовки специалистов среднего звена по специальности 44.02.06 Профессиональное обучение (по отраслям) // Современное состояние медиаобразования в России в контексте мировых тенденций (к 65-летию почетного президента Ассоциации кинообразования и медиапедагогике России, профессора А. В. Федорова) : Материалы международной научной конференции, Таганрог, 06 ноября 2019 года. Таганрог: Ростовский государственный экономический университет «РИНХ», 2019. С. 139–146.

Ковалева Л. А. Медиаобразовательная деятельность в среднем профессиональном образовании // MEDIAОбразование: векторы интеграции в цифровое пространство : Материалы IV международной научной конференции, Челябинск, 26–27 ноября 2019 года / Составитель А. А. Морозова. Челябинск : Челябинский государственный университет, 2019. С. 197–201.

- Коновалова Д. Т., Мусифуллин С. Р. Формирование медиаграмотности у студентов среднего профессионального образования // XVII акмоллинские чтения : Материалы Международной научно-практической конференции, Уфа, 02–03 декабря 2022 года. Том II. Уфа : Башкирский государственный педагогический университет им. М. Акмуллы, 2022. С. 286–288.
- Коханая О. Е., Головин Ю. А. Цифровые медиа как мощный фактор воздействия на поведение детей и подростков // Челябинский гуманитарий. 2021. № 4 (57). С. 28–37.
- Медиабезопасность и профилактика правонарушений молодежи в социальных сетях : Материалы Межрегиональной научно-практической конференции (г. Уфа, 5 декабря 2019 г.). Уфа : Изд-во БГПУ, 2019. 188 с.
- Медиапотребление «цифровой молодежи» в России : монография / под ред. Д. В. Дунаса. Москва : Факультет журналистики МГУ : Издательство Московского университета, 2021. 406 с.
- Мурзина Е. В. Медиапотребление в условиях трансформации современного общества // Вестник Сургутского государственного педагогического университета. 2020. № 5 (68). С. 228–235.
- Оборский А. Ю., Игнатов П. Н. Осознанное медиапотребление как значимый фактор успешного обучения в вузе // Современные тенденции развития науки и технологий. 2015. № 9–2. С. 138–141.
- Пишова А. В. Медиабезопасность субъектов образовательного процесса: проблемы и риски // Философско-педагогические проблемы непрерывного образования : Сборник научных статей, Могилев, 26–27 апреля 2018 года. Могилев: Могилевский государственный университет имени А. А. Кулешова, 2018. С. 271–274.
- Степанян Г. Г. Информационно-образовательная и медийная среда образовательного пространства в СПО // Проблемы современного педагогического образования. 2019. № 62-1. С. 293–297.
- Фатеева И. А. Что такое медиабезопасность, и как она соотносится с информационной безопасностью? // Экология медиасреды : Материалы III Открытой межвузовской научно-практической конференции, Москва, 27 апреля 2018 года. М. : Московский педагогический государственный университет, 2018. С. 98–107.

References

- Goncharova, Yu. I. & Zemcova, Yu. V. (2021). Zashchita personal'nykh dannykh v social'nykh setyakh v usloviyakh sovremennoy cifrovoy gramotnosti [Protection of personal data in social networks in the context of modern digital literacy]. *Innovacionnye nauchnye issledovaniya*, 5–2 (7), 310–315. (In Russ.).
- Druker, M. M. (2019a). Destruktyvnye komponenty social'nykh media [Destructive components of social media]. *Chelyabinskij gumanitarij*, 4 (49), 27–32. (In Russ.).
- Druker, M. M. (2019b). Tekhnologii profilaktiki riskov i ugroz psihologicheskomu zdorov'yu shkol'nikov v social'nykh media [Technologies for the prevention of risks and threats to the psychological health of schoolchildren in social media]. *Pokolenie Z: social'nyj karakter, identichnost' i orientacii sovremennykh podrostkov : sbornik statej Vserossijskoj nauchnoj konferencii s mezhdunarodnym uchastiem*. Ufa, 14–15 November 2019. Ufa: Bashkir State University, 80–84. (In Russ.).
- Zhilavskaya, I. A. (2017). Mediaobrazovanie kak profilaktika informacionnykh riskov [Media Education as Prevention of Information Risks]. *Zhurnal. Social'nye kommunikacii*, 2 (26), 147–151. (In Russ.).
- Ivanova, L. A. (2019). Inkorporirovanie mediaobrazovaniya v programmu podgotovki specialistov srednego zvena po special'nosti 44.02.06 Professional'noe obuchenie (po otraslyam) [Incorporation of media education into the training program for mid-level specialists in the specialty 44.02.06 Vocational training (by industry)]. *Sovremennoe sostoyanie mediaobrazovaniya v Rossii v kontekste mirovykh tendencij (k 65-letiyu pochetnogo prezidenta Associacii kinoobrazovaniya i mediapedagogiki Rossii, professora A. V. Fedorova)*. Taganrog: Rostov State Economic University «RINH», 139–146. (In Russ.).
- Kovaleva, L. A. (2019). Mediaobrazovatel'naya deyatel'nost' v srednem professional'nom obrazovanii [Media educational activities in secondary vocational education]. *MEDIAObrazovanie: vektory integracii v cifrovoe prostranstvo : Materialy IV mezhdunarodnoj nauchnoj konferencii*. Chelyabinsk, 26–27 November 2019. Compiled by A. A. Morozova. Chelyabinsk: Chelyabinsk State University, 197–201. (In Russ.).
- Konovalova, D. T. & Musifullin, S. R. (2022). Formirovanie mediagramotnosti u studentov srednego professional'nogo obrazovaniya [Formation of media literacy among students of secondary vocational education]. *XVII akmolinskije chteniya : Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii*. Ufa, 02–03 December 2022. Volume II. Ufa: Bashkir State Pedagogical University. M. Akmuully, 286–288. (In Russ.).
- Kohanaya, O. E. & Golovin, Yu. A. (2021) Cifrovye media kak moshchnyj faktor vozdejstviya na povedenie detej i podrostkov [Digital media as a powerful factor influencing the behavior of children and adolescents]. *Chelyabinskij gumanitarij*, 4 (57), 28–37. (In Russ.).
- Медиабезопасность и профилактика правонарушений молодежи в социальных сетях (2019). [Media security and prevention of youth delinquency in social networks]. *Materialy Mezhregional'noj nauchno-prakticheskoj konferencii*. Ufa: Publishing house of BSPU. 188 p. (In Russ.).
- Медиапотребление «цифровой молодежи» в России (2021). : монография [Media consumption of «digital youth» in Russia: monograph]. ed. D. V. Dunas. Moscow: Faculty of Journalism of Moscow State University: Moscow University Press. 406 p. (In Russ.).
- Мурзина, Е. В. (2020). Медиапотребление в условиях трансформации современного общества [Media consumption in the context of the transformation of modern society]. *Vestnik Surgut'skogo gosudarstvennogo pedagogicheskogo universiteta*, 5 (68), 228–235. (In Russ.).
- Оборский, А. Ю. & Игнатов, П. Н. (2015). Осознанное медиапотребление как значимый фактор успешного обучения в вузе [Conscious media consumption as a significant factor in successful education at the university]. *Sovremennye tendencii razvitiya nauki i tekhnologii*, 9–2, 138–141. (In Russ.).
- Пишова, А. В. (2018). Медиабезопасность субъектов образовательного процесса: проблемы и риски [Media security of the subjects of the educational process: problems and risks]. *Filosofsko-pedagogicheskie problemy nepreryvnogo obrazovaniya*, Mogilev, April 26–27, 2018. Mogilev: A. A. Kuleshov Mogilev State University, 271–274. (In Russ.).
- Степанян, Г. Г. (2019). Информационно-образовательная и медийная среда образовательного пространства в СПО [Information-educational and media environment of educational space in secondary vocational education]. *Problemy sovremennogo pedagogicheskogo obrazovaniya*, 6–21, 293–297. (In Russ.).
- Фатеева, И. А. (2018). Что такое медиабезопасность, и как она соотносится с информационной безопасностью? [What is media security and how does it relate to information security?]. *Ekologiya mediasredy : Materialy III Otkrytoj mezhvuzovskoj nauchno-prakticheskoj konferencii*. Moscow, April 27, 2018. Moscow: Moscow State Pedagogical University, 98–107. (In Russ.).

Информация об авторах

С. С. Бредихин – кандидат философских наук, заведующий сектором мониторинга и анализа Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде, Челябинский институт развития профессионального образования; доцент кафедры социологии, Южно-Уральский государственный университет

А. А. Морозова – кандидат филологических наук, заведующий сектором исследований педагогических инструментов профилактики деструктивных проявлений в образовательной среде Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде, Челябинский институт развития профессионального образования; доцент кафедры медиапроизводства, Челябинский государственный университет

Е. В. Щетинина – кандидат философских наук, руководитель Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде, Челябинский институт развития профессионального образования; доцент кафедры политических наук и международных отношений, Челябинский государственный университет

Information about the authors

Sergey S. Bredikhin – Candidate of Philosophy, Head of the Sector for Monitoring and Analysis of the Research Center for Monitoring and Preventing Destructive Manifestations in the Educational Environment, Chelyabinsk Institute for the Development of Vocational Education; Associate Professor, Department of Sociology, South Ural State University.

Anna A. Morozova – Candidate of Philology, Head of the Sector for Research of Pedagogical Instruments for the Prevention of Destructive Manifestations in the Educational Environment of the Research Center for Monitoring and Prevention of Destructive Manifestations in the Educational Environment, Chelyabinsk Institute for the Development of Vocational Education; Associate Professor, Department of Media Production, Chelyabinsk State University.

Elizaveta V. Shchetinina – Candidate of Philosophy, Head of the Research Center for Monitoring and Prevention of Destructive Manifestations in the Educational Environment, Chelyabinsk Institute for the Development of Vocational Education; Associate Professor, Department of Political Science and International Relations, Chelyabinsk State University.

Все авторы сделали эквивалентный вклад в подготовку публикации.

Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 14.04.2023; одобрена после рецензирования 23.08.2023; принята к публикации 28.08.2023.

The article was submitted 14.04.2023; approved after reviewing 23.08.2023; accepted for publication 28.08.2023.