УДК 004.056; УДК 005.935.33

ЦИФРОВАЯ ГРАМОТНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ. МЕТОДЫ ЭФФЕКТИВНОЙ БОРЬБЫ С КИБЕРБУЛЛИНГОМ

Д. П. КАРАБЕЦ
(Представлено: канд. тех. наук, доц. И. Б. БУРАЧЁНОК)

В статье рассмотрено понятие цифровой грамотности. Рассмотрены методы эффективного и безопасного использования цифровых технологий. Приведено понятие кибербуллинга и изучены его основные формы. Разработан и предложен вариант теста для оценки уровня цифровой грамотности, включая вопросы осведомленности граждан в вопросах кибербуллинга, для разных возрастных групп. Приведены результаты исследования.

Ключевые слова: *цифровая грамотность, кибербуллинг, кибербезопасность, повышение цифровой грамотности, метод опроса.*

Введение. Оскорбления, травля, запугивания и публичное унижение в интернете в современном мире наносят реальный вред психике человека, разрушая его самооценку и чувство безопасности. Проблема усугубляется тем, что многие не знают, как распознать признаки кибербуллинга, не умеют правильно реагировать на его отдельные формы и часто оказываются в изоляции. Поэтому решение этой проблемы возможно лишь с применением системного подхода к формированию цифровой грамотности каждого, отдельно взятого человека. Причем под этой грамотностью понимается не только умение пользоваться компьютером или смартфоном. Это прежде всего комплексное развитие у человека навыков его безопасного поведения в сети, умение различать достоверную информацию, мошеннических схем и фишинга, понимание основ работы цифровых технологий и сервисов, защищать свои личные данные, противостоять манипуляциям и, что особенно важно, не оставаться безучастным к насилию в онлайн-пространстве. Поэтому разработка новых методов оценки цифровой грамотности населения и выявление наиболее слабых (уязвимых) мест в отдельно взятых возрастных группах является актуальной задачей.

Целью представленной работы является оценка уровня цифровой грамотности населения методом опроса разных возрастных групп и выработка рекомендаций и предложений для предотвращения кибербуллинга.

Основные понятия. Для достижения поставленной цели первоначально рассмотрим основные понятия «грамотность», «цифровая грамотность» и «кибербуллинг».

Понятие грамотности в нашей стране и за рубежом развивалось в соответствии с потребностями общества, производства – от простейших умений до владения минимумом общественно необходимых знаний и навыков. За основу понятия цифровая грамотность возьмем определение ООН, согласно которому «*цифровая грамотность – это способность безопасно и надлежащим образом управлять, понимать, интегрировать, обмениваться, оценивать, создавать информацию и получать доступ к ней с помощью цифровых устройств и сетевых технологий для участия в экономической и социальной жизни*» [1].

В понятии «цифровая грамотность» выделяются шесть главных умений:

– находить нужную информацию в интернете и уметь оценивать её достоверность и качество;

– анализировать проблему и подбирать цифровые инструменты, с помощью которых можно найти её решение;

– непрерывно обучаться на протяжении всей жизни, используя доступ к информации;

– оценивать постоянно изменяющиеся технологические инструменты и выбирать из них наиболее подходящие для решения конкретных задач;

– адаптироваться и перестраиваться для успешной работы с постоянно обновляющимися цифровыми технологиями;

– комбинировать различные цифровые инструменты и настраивать их под собственные потребности для достижения поставленной цели [2].

Исследования и оценка цифровой грамотности человека сводится к единой цели – систематизации теоретических знаний и применением их на практике в цифровой среде. Г.У. Солдатовой предложена четырёхкомпонентная структура цифровой компетентности, включающая в себя: знания, умения и навыки, мотивацию, ответственность, в том числе в вопросах безопасности [2].

Каждый из указанных компонентов может быть реализован в различных сферах деятельности с информационными и интернет-источниками (при работе с контентом, в коммуникации, в сфере технологий, при потреблении) в разной степени. Выделение ключевых элементов цифровой грамотности позволяет точнее определить, какие знания и навыки необходимо развивать у различных групп населения для

повышения их устойчивости к цифровым угрозам и успешной адаптации к требованиям современного информационного общества. Далее в таблице 1 представлены основные элементы цифровой грамотности, формирующие её содержательную основу.

Таблица 1. – Основные элементы цифровой грамотности

Название	Определение	Пример
Работа с информацией	Навыки поиска, обработки, оценки и применения цифровой информации. Это включает умение находить достоверные источники, анализировать данные и использовать их для принятия решений	Способность эффективно искать информацию в интернете, проверять её достоверности анализировать данные для подготовки отчётов или презентаций
Цифровая коммуникация	Навыки общения и взаимодействия через цифровые каналы. Это включает электронную почту, мессенджеры, видеоконференции, социальные сети и другие онлайн-платформы	Использование корпоративных мессенджеров и инструментов для удалённой работы, таких как Zoom или Microsoft Teams, для координации работы с коллегами
Безопасность и конфиденциальность	Знание основных принципов кибербезопасности и способность защищать свою цифровую информацию. Это включает использование паролей, двухфакторной аутентификации и антивирусного ПО, а также понимание рисков, связанных с киберугрозами	Умение создавать безопасные пароли, использовать VPN для защиты данных и избегать фишинговых атак
Функциональное Использование цифровых технологий	Способность использовать цифровые инструменты для решения задач, связанных с работой, обучением или повседневной жизнью. Это включает использование программного обеспечения для управления проектами, анализа данных и автоматизации процессов	Использование инструментов для управления проектами, таких как Trello или Asana, для координации задач и отслеживания прогресса
Творческое Использовани цифровых технологий	Навыки создания контента и применения цифровых технологий для разработки новых продуктов, услуг или идей. Это может включать использование различных графических редакторов, видеомонтажных и аудио программ для креативных решений	Создание презентаций с использованием Canva или редактирование видеоконтента для корпоративных целей с помощью Adobe Premiere
Этика и цифровое гражданство	Осознанное и ответственное использование цифровых технологий, уважение авторских прав, признание других пользователей и участие в цифровом обществе	Соблюдение норм поведения в интернете, уважение авторских прав и ответственное участие в онлайн-дискуссиях и сообществе

Таким образом, цифровая грамотность представляет собой комплексное и многокомпонентное явление, включающее не только технические навыки работы с цифровыми устройствами, но и когнитивные, коммуникативные, этические и социальные компетенции. Современное понимание цифровой грамотности выходит за рамки простого владения технологиями и подразумевает осознанное, безопасное и продуктивное использование цифровой среды для обучения, профессиональной деятельности и повседневного взаимодействия. Развитие цифровых компетенций способствует формированию ответственного поведения пользователей в сети, укреплению личной информационной безопасности и повышению уровня участия граждан в социально-экономической и культурной жизни общества.

Что же такое кибербуллинг? Исследователь Дэвид Фейган определяет кибербуллинг как применение силы и личной значимости, прямо или косвенно (устно, письменно или физически), либо путем обнародования снимков, символики и/или чего-либо прочего с целью травли, запугивания, угроз при помощи интернета и других современных технологий. Среди российских исследователей стоит выделить Е.С. Ефимову: «*кибербуллинг – преследование электронными сообщениями, которые оскорбляют, унижают, запугивают получателя при помощи интернет – сервисов*» [3].

Как и традиционный буллинг (травля), кибербуллинг может быть прямым и косвенным. Прямой кибербуллинг – это непосредственные атаки на человека через письма или сообщения. При косвенном в процесс травли жертвы вовлекаются другие люди (как дети, так и взрослые), не всегда с их согласия; преследователь может взломать аккаунт жертвы и, мимикрируя под хозяина, рассылать с этого аккаунта сообщения знакомым жертвы, разрушая коммуникативное поле жертвы и порождая сомнение в его моральных качествах. Одна из наиболее угрожающих ситуаций – когда преследователь публикует в сети информацию, которая в действительности подвергает жертву опасности, например, от ее имени размещает объявление о поиске сексуальных партнеров. Как и традиционная травля, кибербуллинг включает

в себя континуум поступков, на одном полюсе которого действия, с трудом распознающиеся окружающими как преследование, а на другом – жестокое поведение агрессора, которое может приводить даже к смерти жертвы.

Выделяют несколько форм кибербуллинга [4-6]:

– бойкот. Это ситуация, когда жертва игнорируется в социальных сетях и общих чатах, вплоть до удаления из переписки;

– доксинг. Процесс раскрытия личной информации о жертве в интернете, включая данные о месте жительства, номер телефона, реквизиты банковских карт и прочую чувствительную информацию;

– сталкеринг. Агрессивное поведение, при котором человек внимательно наблюдает за страницами жертвы, собирая персональную информацию и фотографии без ее согласия;

– домогательства. Ситуация, в которой агрессор (чаще всего мужского пола) навязывается жертве с вопросами, шантажом или принуждением к общению;

– троллинг. Форма агрессии, нацеленная на высмеивание внешности или личных качеств жертвы в уничтожительном тоне;

– диссинг. Размещение личной информации, которая может негативно сказаться на репутации жертвы, например, публикация компрометирующих фотографий без ее согласия;

– фрейпинг. Когда агрессор получает доступ к аккаунту жертвы и публикует материалы от ее имени, не получив на это согласие;

– кетфишинг. Схож с фрейпингом, но в этом случае агрессор создает аккаунт, который точно копирует аккаунт жертвы, и затем устраивает провокации от ее имени;

– секстинг. Отправка сообщений сексуального характера. Такая переписка может содержать текст, эмодзи, фото и видео, содержащие наготу или демонстрирующие имитацию половых органов. Возможна также отправка тематических голосовых сообщений;

– флейминг. Это бесцельная дискуссия в чате, личной переписке или комментариях, сопровождающаяся негативными эмоциями;

– хейтинг. Немотивированно злобные, оскорбительные и агрессивные комментарии, посты и сообщения в социальных сетях;

– груминг. Общение взрослого человека с несовершеннолетним в сети с целью совращения.

Таким образом, кибербуллинг представляет собой одну из наиболее опасных форм насилия в цифровой среде, затрагивающую как психологическое, так и социальное благополучие личности. Он отличается от традиционного буллинга своей анонимностью, постоянной доступностью и масштабом распространения информации, что значительно усложняет процесс защиты жертвы и делает последствия травли более длительными и разрушительными.

Разнообразие форм кибербуллинга – от бойкота и троллинга до доксинга и груминга – свидетельствует о том, что цифровое пространство становится не только инструментом коммуникации и самовыражения, но и потенциальной зоной риска. В связи с этим особую актуальность приобретает развитие цифровой грамотности и формирование культуры ответственного поведения в сети. Осознание пользователями механизмов кибербуллинга, а также знание способов защиты и реагирования на подобные угрозы, являются ключевыми условиями обеспечения личной безопасности в современном информационном обществе.

Методы исследования. Для получения объективных данных о текущем уровне знаний участников и выявления пробелов в понимании ключевых аспектов цифровой безопасности использовался метод опроса разных возрастных групп. На основании опроса осуществлена оценка цифровой грамотности и владения вопросами кибербуллинга респондентами. Метод опроса позволил также определить направления для последующей просветительской и профилактической работы. Кроме того, результаты тестир вания послужили доказательной базой для подтверждения гипотезы о важности системного подхода к формированию цифровой культуры среди населения.

Опрос проведен с использованием сервиса «Google Формы». Это позволило эффективно собрать и обработать данные в онлайн-формате. Выбор данной платформы обусловлен её доступностью, удобным интерфейсом для респондентов, а также широкими возможностями для автоматического подсчёта результатов и анализа ответов. Формат Google Форм обеспечил анонимность участия, что способствовало большей откровенности и достоверности полученных данных.

В рамках исследования цифрового грамотности разработан тест «Повышение цифровой грамотности в киберпространстве», содержащий 25 вопросов охватывающие различные компоненты цифровой грамотности. По каждому вопросу предлагалось респондентам ответы с вариантами для одиночного выбора.

Тест основан на ключевых аспектах, необходимых для безопасного и осознанного поведения в цифровой среде. Его структура охватывает такие темы, как защита персональных данных, оценка

надежности интернет-ресурсов, создание и использование надежных паролей, правила поведения при взаимодействии с незнакомыми пользователями, а также реагирование на киберугрозы. Отдельное внимание уделено теме кибербуллинга – его формам, последствиям, способам противодействия и профилактики.

Вопросы теста позволяют оценить уровень осведомлённости респондентов о цифровой безопасности, их способность распознавать потенциальные угрозы и принимать верные решения в различных ситуациях, связанных с общением в интернете и защитой личной информации.

Примеры некоторых вопросов и вариантов ответов из предлагаемого теста:

Как вы определяете, безопасен ли сайт?

- Проверяю наличие "https" в адресной строке и значка замка.
- Смотрю на дизайн сайта – если красивый, то безопасный.
- Доверяю, если сайт рекомендуют знакомые.
- Никогда не задумывался о безопасности сайта.

Если в соцсетях вам пишут незнакомые люди с просьбой помочь в финансовом вопросе, вы не будете?

- Переводить деньги, если история кажется правдоподобной.
- Игнорировать такие сообщения.
- Проверять информацию и источники, прежде чем реагировать.
- Сообщать о таких сообщениях в службу поддержки.

Как вы реагируете на оскорбления или кибербуллинг в соцсетях?

- Оскорбляю в ответ.
- Зову друзей, чтобы они помогли забуллить обидчика.
- Игнорирую.
- Участвую в конфликте.

Полученные результаты. В опросе приняли участие 88 человек, возрастом от 12 до 23 лет включительно. Респонденты были поделены на две возрастные группы: первая группа от 12 до 17, и вторая группа от 18 до 23. Важно отметить преобладание респондентов определенного возраста, в частности от 17 до 19. Уже на данном этапе это показывает заинтересованность и демонстрирует осведомленность участников опроса в представленной тематике.

В таблице 2 заметна значительная разница между набранными баллами двух возрастных групп.

Таблица 2. – Данные опроса

Возрастная группа респондентов	12-17 лет		18-23 лет	
Количество респондентов	33 человека		55 человек	
Минимальная и максимальная оценка результата (баллов)	13	22	8	25
Усредненный результат всех респондентов (баллов)	18,67		20,98	

Выводы. В результате проведенного исследования удалось выявить существенные различия в уровне цифровой грамотности между двумя возрастными группами: подростками от 12 до 17 лет и молодыми взрослыми от 18 до 23 лет. Участники старшей группы в целом демонстрируют более высокий уровень знаний и осведомлённости в вопросах безопасного поведения в интернете, лучше понимают риски, связанные с киберугрозами, и чаще выбирают правильные стратегии защиты.

Полученные данные подтверждают, что цифровая грамотность напрямую связана с возрастом и жизненным опытом. Старшие респонденты чаще осознают важность защиты личных данных, умеют распознавать потенциально опасные ситуации в сети и знают, как реагировать на угрозы вроде кибербуллинга и интернет-мошенничества. Проведенное исследование также показало, что среди младшей группы больше распространены ошибки и недостаток базовых знаний в сфере цифровой безопасности. Это говорит о необходимости формирования цифровой грамотности, особенно среди подростков, которые наиболее уязвимы к онлайн-угрозам.

ЛИТЕРАТУРА

1. Оценка уровня цифровой грамотности населения методом опроса. [Электронный ресурс]. – Режим доступа: https://elib.psu.by/handle/123456789/46111. – Дата доступа: 06.04.2025.
2. К вопросу о понятии цифровой грамотности. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-tsifrovoy-gramotnosti/viewer. – Дата доступа: 06.04.2025.

3. Кибербуллинг: виды и особенности проявления. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kiberbulling-vidy-i-osobennosti-proyavleniya/viewer. – Дата доступа: 06.04.2025.
4. Кибербуллинг – травля в интернете. [Электронный ресурс]. – Режим доступа: https://reputation.moscow/2018/06/25/kiberbulling_travlya_v_internete/ – Дата доступа: 06.04.2025.
5. Виды кибербуллинга и их связь с типом межличностного поведения. [Электронный ресурс]. – Режим доступа: https://scipress.ru/pedagogy/articles/vidy-kiberbullinga-i-ikh-svyaz-s-tipom-mezhlichnostnogo-povedeniya.html – Дата доступа: 06.04.2025.
6. Кибербуллинг: виды и особенности проявления. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kiberbulling-vidy-i-osobennosti-proyavleniya/viewer – Дата доступа: 06.04.2025.