

Влияние цифровых угроз на психическое состояние обучающихся

Д.Ю. Немцова

ФГБОУ ВО «Тверской государственный университет», г. Тверь, Россия

В данной статье анализируется влияние цифровых угроз на психическое состояние детей и подростков в условиях цифровой трансформации образования. Рассматриваются такие основные виды онлайн-рисков, как кибербуллинг, фишинг и социальная инженерия. Автор обосновывает необходимость комплексного подхода к решению проблемы: внедрение программ формирования цифровой грамотности и кибергигиены, повышение квалификации педагогов по цифровой безопасности, проведение просветительской работы с родителями обучающихся, сотрудничество образовательных учреждений с правоохранительными органами, а также регулярный мониторинг психического состояния школьников.

Ключевые слова: цифровые угрозы, обучающиеся, кибербуллинг, фишинг, социальная инженерия, психическое состояние.

В настоящее время информационно-коммуникационные технологии постепенно проникают во все сферы деятельности человека. Их освоение происходит в любом возрасте, начиная с раннего детства и продолжается на протяжении всей жизни. Сегодня юное поколение является активными пользователями сети Интернет. Исследование Kids&Teens, проведенное компанией Mediascope, показало, что более 90% детей в возрасте от 4 до 11 лет используют сеть Интернет, в возрастной группе пользователей 6–8 лет показатель составляет 97%, а среди подростков 9–11 лет – 99% [9]. Активное взаимодействие с цифровым пространством сопровождается ростом различных угроз, с которыми может столкнуться ребёнок. К ним относятся фишинг, кибербуллинг, социальная инженерия и т.д. Наиболее частым последствием данных атак для обучающихся является ухудшение их психического состояния («целостной характеристики психической деятельности за определенный период времени, показывающую своеобразие протекания психических процессов в зависимости от отражаемых предметов и явлений деятельности, предшествующего состояния и психических свойств личности» [6, с. 20]).

Целью статьи является анализ влияния цифровых угроз на психическое состояние обучающихся, выявление основных механизмов их негативного воздействия на когнитивную, эмоциональную и поведенческую сферы, а также на основе анализа – разработка рекомендаций по минимизации этих рисков в условиях цифровизации образования.

Под цифровой угрозой (атакой, кибератакой) Е.Ю. Хрусталева и Г.А. Костюрин понимают «покушение на информационную безопасность компьютерной системы» [15]. В более широком психологическом контексте цифровая угроза представляет собой «любое целенаправленное или случайное воздействие цифровой среды, которое способно нарушить

психическое равновесие ребёнка или подростка, нанести ущерб его эмоциональной сфере, когнитивным процессам или социальному функционированию» [11]. Цифровые угрозы отличаются высокой латентностью и трудностью своевременного обнаружения.

Особую опасность для детей и подростков в цифровом пространстве представляет кибербуллинг. По мнению Е.А. Макаровой, Е.Л. Макаровой и Е.А. Махриной он выражается в «моральном и психологическом насилии, доминировании и принуждении, социальной изоляции, запугивании и вымогательстве, осуществляемыми с помощью электронных средств коммуникации» [7]. В отличие от буллинга, с которыми могут столкнуться обучающиеся учебного заведения, цифровая модель не ограничивается временным и физическим пространствами. Жертва может получать негативные сообщения постоянно, независимо от времени суток и местонахождения. Компания «Где мои дети» провела в 2024 году исследование среди подростков в возрасте 16–18 лет. Оно показало, что около 69% опрошенных хотя бы раз сталкивались с кибербуллингом [12]. Последствия такого воздействия на психику личности особенно тяжелы в подростковом возрасте, когда происходит формирование идентичности и возрастает потребность в социальном одобрении [5]. Постоянный поток отрицательных воздействий приводит к снижению мотивации к учебной деятельности и появлению прогрессирующих соматических симптомов (головных болей, нарушений сна, расстройств пищевого поведения и т.д.). В тяжелых случаях кибербуллинг провоцирует появление суицидальных мыслей и попытки их осуществления [3].

Фишинговые атаки («рассылка поддельных электронных писем, сообщений или создание фальшивых веб-сайтов с целью заставить пользователя раскрыть свои личные данные» [1]) и социальная инженерия («психологическая манипуляция человеческим поведением, направленная на получение несанкционированного доступа к техническим устройствам или информации» [13]) несут не менее опасные последствия для личности. Обучающиеся, не обладающие достаточным опытом в распознавании манипуляций, легко поддаются на сторонние провокации. Данные атаки часто маскируются под выгодные предложения в интернет-магазинах или онлайн-играх. Злоумышленники могут предложить обучающимся получить редкие внутриигровые предметы, бонусы или доступ к ограниченным предложениям. В результате ребёнок или подросток может не только потерять доступ к личному аккаунту, но и столкнуться с шантажом. Наиболее распространённой угрозой со стороны мошенников является распространение переписок или личных фотографий. Психологическое давление в таких ситуациях вызывает у обучающегося испуг, стыд и страх перед сверстниками, родителями и учителями. Это приводит к его замкнутости и отказу от общения с окружающими. Длительное пребывание в состоянии тревоги активирует хронический стресс, который в первую

очередь проявляется в когнитивных нарушениях: снижении концентрации внимания, ухудшении памяти и ослаблении интеллектуальных способностей [4].

В результате в образовательном процессе у обучающегося возникают отставание и неуспеваемость. Ему становится сложнее осваивать новый теоретический материал и выполнять практические задания.

В поведенческой сфере последствия фишинговых атак и социальной инженерии выражаются в деструктивных изменениях привычек и реакций индивида. Обучающийся может перейти к компульсивной модели поведения: чрезмерной проверке аккаунтов или полному избеганию цифровой активности. Также возможны и вспышки агрессии по отношению к окружающим и близким людям.

Хронический стресс провоцирует развитие невротических расстройств и соматических заболеваний. На физиологическом уровне он проявляется быстрой утомляемостью, нарушением сна, отсутствием аппетита, наличием кожных высыпаний и т.д. Данные симптомы могут как усиливаться во время эмоционального напряжения, так и ослабевать в спокойные периоды. В долгосрочной перспективе хронический стресс приводит к стойкому снижению когнитивных функций, истощению нервной системы и формированию устойчивых психосоматических заболеваний [14].

Стоит отметить, что отрицательный опыт столкновения обучающихся с цифровыми угрозами способствует развитию у них способности анализировать собственные эмоциональные, поведенческие реакции и умения управлять ими, а также осмысливать последствия совершенных действий в онлайн-среде. Это сказывается на формировании эмоциональной устойчивости [10].

Влияние цифровых угроз усугубляется в условиях массовой цифровизации образования. Переход на дистанционные и смешанные форматы обучения увеличил время пребывания обучающихся за экранами технических устройств. Образовательные платформы и тренажеры, электронные дневники, онлайн-сервисы – все это требует постоянного взаимодействия пользователя с виртуальным пространством. Это расширяет возможности атаки со стороны злоумышленников. При этом многие образовательные учреждения уделяют недостаточно внимания цифровой гигиене (набору мер по защите устройств, информации и данных от различных угроз [16]) [2]. Учителя, сосредоточенные на передаче предметных знаний, редко обсуждают на уроках и во внеучебной деятельности правила безопасного использования сетью Интернет, а родители часто не обладают достаточными знаниями в этой области. В результате обучающиеся остаются один на один с цифровыми рисками, не имея подходящих инструментов для их распознавания и нейтрализации.

Психическое состояние школьников в данном случае характеризуется повышенной эмоциональной лабильностью: вспышками раздражения, которые сменяются апатией; угасанием интереса к реальной жизни и появлением первых признаков зависимости от технических устройств и виртуальной реальности [8].

Остро данная проблема проявляется у обучающихся с уже имеющимися психическими особенностями (например, имеющих социальную тревожность, низкую самооценку или сталкивающихся в реальной жизни с буллингом). Для таких личностей использование сети Интернет может нести как положительные, так и отрицательные последствия. С одной стороны, возможность анонимного общения дает облегчение, вызванное снижением страха личного осуждения, с другой - отрицательная реакция в виртуальном пространстве воспринимается как подтверждение незначимости и ненужности.

Для минимизации негативного влияния цифровых угроз на психическое состояние школьника необходимо комплексное и системное решение проблемы. Целесообразным является:

- внедрение в образовательный процесс программ по формированию у обучающихся цифровой грамотности и кибергигиены (начиная с начальных классов общеобразовательной школы). Такие занятия должны включать не только изучение технических и цифровых аспектов защиты, но и специальную психологическую подготовку: обучение школьников основам эмоциональной саморегуляции и противостоянию мошенническим манипуляциям;

- повышение квалификации педагогов в области цифровой безопасности и психологии виртуального общения. Учителя должны уметь своевременно выявлять признаки кибербуллинга и оказывать первичную помощь и психологическую поддержку;

- вовлечение родителей через регулярные просветительские мероприятия, вебинары и совместные онлайн-курсы по безопасному использованию сети Интернет;

- сотрудничество образовательного учреждения с правоохранительными органами для оперативного реагирования на случаи кибербуллинга и цифрового мошенничества в отношении обучающихся;

- проведение мониторинга психического состояния обучающихся (с акцентом на симптомы, связанные с цифровыми угрозами).

Таким образом, в цифровом пространстве обучающийся может столкнуться с различными угрозами, негативно влияющими на его психическое благополучие. Освоение и использование виртуального пространства не должно происходить стихийно, а осуществляться под сторонним контролем и с опорой на развитые навыки цифровой безопасности и психологическую подготовку. В этом случае технологии

будут служить инструментом развития, а не источником угроз для психического здоровья обучающихся.

СПИСОК ЛИТЕРАТУРЫ

1. Ан Д.С., Зуфарова А.С. Классификация фишинга: различные типы и способы реализации атак // Информатика. Экономика. Управление / Informatics. Economics. Management. 2025. №1. URL: <https://cyberleninka.ru/article/n/klassifikatsiya-fishinga-razlichnye-tipy-i-sposoby-realizatsii-atak> (дата обращения: 19.02.2026).
2. Кальней В.А., Тверской А.С. Концепция, структура и содержание учебного курса «цифровая гигиена личности» в старших классах // Гуманизация образования. 2023. №2. URL: <https://cyberleninka.ru/article/n/kontseptsiya-struktura-i-soderzhanie-uchebnogo-kursa-tsifrovaya-gigiena-lichnosti-v-starshih-klassah> (дата обращения: 19.02.2026).
3. Карауш И.С., Куприянова И.Е., Кузнецова А.А. Кибербуллинг и суицидальное поведение подростков // Суицидология. 2020. №1 (38). URL: <https://cyberleninka.ru/article/n/kiberbulling-i-suitsidalnoe-povedenie-podrostkov> (дата обращения: 19.02.2026).
4. Когнитивные нарушения [электронный ресурс]. URL: <https://www.krasotaimedicina.ru/diseases/psychiatric/cognitive-disorder> (дата обращения: 19.02.2026).
5. Корчагина Ю.В. Подростки: поиск идентичности // Справочник педагога-психолога: школа. 2015. №8. С. 33–38.
6. Левитов Н.Д. О психических состояниях. М., 1964. 344 с.
7. Макарова Е.А., Макарова Е.Л., Махрина Е.А. Психологические особенности кибербуллинга как формы интернет-преступления // Российский психологический журнал. 2016. №3. URL: <https://cyberleninka.ru/article/n/psihologicheskie-osobennosti-kiberbullinga-kak-formy-internet-prestupleniya> (дата обращения: 19.02.2026).
8. Сорокоумова Е.А., Пучкова Е.Б., Темнова Л.В., Курносова М.Г., Ферапонтова М.В. Диагностика психологических рисков обучающихся в цифровой образовательной среде // Педагогика и психология образования. 2022. №2. URL: <https://cyberleninka.ru/article/n/diagnostika-psihologicheskikh-riskov-obuchayushchihya-v-tsifrovooy-obrazovatelnoy-srede> (дата обращения: 19.02.2026).
9. С четырех лет – в интернет: Mediascope исследовала активность детей в Сети. [электронный ресурс]. URL: <https://www.rbc.ru/newspaper/2025/03/03/67c1b67a9a7947a146b068c3> (дата обращения: 19.02.2026).
10. Филиппова С.А., Пазухина С.В., Куликова Т.И., Степанова Н.А. Сформированность эмоциональной устойчивости студентов к негативному влиянию информационной среды // Вестник Государственного университета просвещения. Серия: Психологические науки. 2019. №2. URL: <https://cyberleninka.ru/article/n/sformirovannost-emotsionalnoy-ustoychivosti-studentov-k-negativnomu-vliyanuyu-informatsionnoy-sredy> (дата обращения: 19.02.2026).
11. Фоминых Е.С. Нарушения информационной безопасности в контексте цифровой виктимизации детей и подростков // Виктимология. 2024. №1. URL: <https://cyberleninka.ru/article/n/narusheniya-informatsionnoy-bezopasnosti-v-kontekste-tsifrovoy-viktimizatsii-detey-i-podrostkov> (дата обращения: 19.02.2026).
12. Хоть раз сталкивались с травлей в интернете 69% российских школьников [электронный ресурс]. URL: <https://russian.rt.com/russia/news/1384085-travlya-internet-shkolniki> (дата обращения: 19.02.2026).
13. Хамраев А.М. Социальная инженерия и человеческий фактор // При прочих равных условиях. 2025. №4. URL: <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-i-chelovechesky-faktor> (дата обращения: 19.02.2026).

14. Хронический стресс – причины, симптомы, диагностика и лечение. [электронный ресурс]. URL: <https://yagla.tv/czgzSWg faktor> (дата обращения: 19.02.2026).
15. Хрусталёв Е.Ю., Костюрин Г.А. Киберугрозы: причины возникновения и рекомендации по предупреждению // Национальные интересы: приоритеты и безопасность. 2019. Т. 15, № 6. С. 1185–1194. <https://www.fin-izdat.com/journal/national/detail.php?ID=74552>
16. Шадманов З.З. Цифровая гигиена: важность и лучшие практики // Raqamli iqtisodiyot (Цифровая экономика). 2025. №10. URL: <https://cyberleninka.ru/article/n/tsifrovaya-gigiena-vazhnost-i-luchshie-praktiki> (дата обращения: 19.02.2026).

Об авторе:

Немцова Дарья Юрьевна – аспирант ФГБОУ ВО «Тверской государственный университет» (Россия, 170100, г. Тверь, ул. Желябова, 33), e-mail: Nemtsova.DY@tversu.ru

The impact of digital threats on the psychological state of students

D.Yu. Nemtsova

Tver State University, Tver, Russia

This article analyzes the impact of digital threats on the psychological state of children and adolescents in the context of digital transformation of education. It examines the main types of online risks, such as cyberbullying, phishing, and social engineering. The author substantiates the need for a comprehensive approach to solving the problem: implementation of digital literacy and cyberhygiene programs, professional development of teachers in digital security, educational work with students' parents, cooperation between educational institutions and law enforcement agencies, as well as regular monitoring of students' psychological state.

Keywords: *digital threats, students, cyberbullying, phishing, social engineering, psychological state.*

About the author:

Nemtsova Daria Yuryevna – postgraduate student, Tver State University (Russia, 170100, Tver, Zhelyabova St., 33), e-mail: Nemtsova.DY@tversu.ru

Дата поступления рукописи в редакцию: 03.04.2026.

Дата принятия рукописи в печать: 27.04.2026.