Научная статья
УДК 004.056
DOI: 10.46724/NOOS.2025.4.88-93

А. Р. Романова

ФОРМИРОВАНИЕ КИБЕРБЕЗОПАСНОГО ПОВЕДЕНИЯ У МЛАДШИХ ПОДРОСТКОВ: ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ И ВЛИЯНИЕ ЛИЧНОСТНЫХ ФАКТОРОВ

Аннотация. В статье рассматриваются особенности кибербезопасного поведения подростков в условиях интенсивного использования цифровых технологий. Целью исследования являлось определение уровня осведомленности подростков о безопасном поведении в Интернете и выявление влияния специального обучения на формирование соответствующих навыков. В ходе эмпирического исследования применялись методы анкетирования и тестирования. Выборка составила 34 подростка 11—12 лет, разделенных на две группы: прошедших курс «Кибергигиена» и не прошедших его. Результаты показали, что подростки, обучавшиеся на курсе, демонстрируют более высокий уровень осведомленности, чаще применяют меры безопасности и реже испытывают неуверенность при столкновении с киберугрозами. При этом не выявлено значимой связи между уровнем внушаемости и подверженностью киберугрозам. Делается вывод о необходимости системного образовательного подхода к формированию кибербезопасного поведения у подростков.

Ключевые слова: кибергигиена, киберугрозы, кибербезопасное поведение, младшие подростки, конформность-внушаемость.

Ссылка для цитирования: Романова А. Р. Формирование кибербезопасного поведения у младших подростков: оценка уровня осведомленности и влияние личностных факторов // Ноосферные исследования. 2025. Вып. 4. С. 88—93.

Original article

A. R. Romanova

DEVELOPING CYBERSAFE BEHAVIOR IN YOUNGER ADOLESCENTS: ASSESSING THE LEVEL OF AWARENESS AND THE INFLUENCE OF PERSONALITY FACTORS

Abstract. This paper considers the cyber-secure behavior of teenagers in an environment where digital technology is used intensively. The aim of the study was to determine the level of teenagers' awareness of safe online behavior and to identify the impact of specialized training on the development of these skills. The empirical study employed survey and testing methods. The study involved 34 teenagers aged 11 and 12. They were divided into two groups: those who completed the Cyber Hygiene course and those who did not. The results showed that the

teenagers who had completed the course demonstrated a higher level of awareness, used safety measures more often and felt uncertain less often when they encountered cyber threats. However, no significant link between suggestibility and susceptibility to cyber threats was found. This study concludes that a systemic educational approach to the development of cyber-secure behavior in teenagers is necessary.

Keywords: cyber hygiene, cyber threats, cyber-safe behavior, younger adolescents, conformity-suggestibility.

Citation Link: Romanova A. R. (2025) Developing cybersafe behavior in younger adolescents: assessing the level of awareness and the influence of personality factors, *Noospheric Studies*, no. 4, pp. 88—93.

В современных социокультурных условиях проблема безопасности[1] пользователей в цифровом пространстве приобретает все большую значимость[2]. Особенно актуальным является вопрос кибербезопасности подростков [Ушкин, Коваль, Мартынова, 2025], поскольку именно эта возрастная группа является наиболее активными пользователями Интернета и компьютерных технологий. Подростки проводят в сети значительное количество времени, что делает их уязвимыми перед разнообразными угрозами: кибербуллингом, фишингом, мошенничеством, кражей личных данных и другими формами киберпреступлений. Статистические данные указывают, что около 89 % подростков ежедневно используют социальные сети, проводя в онлайн-среде в среднем 4—5 часов [Смирнова, Захарова, Синогина, 2017]. В связи с этим возникает необходимость изучения специфики кибербезопасного поведения подростков и разработки эффективных мер по формированию у них соответствующих навыков и осознанного отношения к рискам цифрового пространства[3].

Исследование было направлено на оценку уровня информированности подростков относительно безопасного поведения в сети Интернет и выявление эффективности специализированного курса обучения в формировании такого поведения.

Для достижения целей были использованы следующие исследовательские методики:

- анкетирование с применением оригинальной анкеты «Кибербезопасность подростков», включающей десять вопросов, касающихся частоты и целей использования Интернета, понимания понятия кибербезопасности, самооценки уровня знаний, опыта столкновений с онлайн-угрозами, используемых мер защиты и способов реагирования на потенциальные риски;
- тестирование для оценки уровня внушаемости участников посредством теста «Конформность-внушаемость» авторов С. В. Клаучека и В. В. Деларю.

[1] Обратим внимание, что проблемное пространство кибербезопасности вписывается в более масштабный дискурс ноосферной безопасности [Смирнов, 2021].

[2] Концепция информационной безопасности детей: утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р. URL https://www.garant.ru/products/ipo/prime/doc/71167034/ (дата обращения: 20.01.2025).

[3] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации». URL https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.01.2025).

Исследовательская выборка состояла из 34 подростков в возрасте 11—12 лет, распределенных на две группы: экспериментальная группа (11 человек), прошедшая образовательный курс «Кибергигиена»; контрольная группа (23 человека), не участвовавшая в данном обучении.

Проведение исследования осуществлялось на базе центра технического творчества «Новация».

В рамках настоящего исследования была разработана концептуальная основа, определяющая ключевые категории в области кибербезопасности и соответствующего поведения несовершеннолетних пользователей.

Кибербезопасность трактуется нами как система организационных и технических мер, направленная на обеспечение защищенности личности и ее цифровых ресурсов от угроз, исходящих из киберпространства. Данная концепция подразумевает комплексный подход, сочетающий технические средства защиты с формированием у пользователей навыков правильного и безопасного поведения в условиях современного цифрового мира. Важнейшими аспектами являются защита информации, минимизация возможных рисков и формирование безопасной цифровой среды.

Киберугрозы определяются как любые целенаправленные действия, осуществляемые с использованием компьютеров и сетей, способные нанести вред физическим лицам либо их активам. Наиболее распространенными видами угроз выступают: кибербуллинг, фишинг, распространение вредоностного ПО, кибераддикация и др.

Киберпреступления представляют собой незаконные действия, происходящие в виртуальной среде и подлежащие уголовной ответственности. Они включают широкий спектр правонарушений, таких как хищение личных данных, финансовое мошенничество, пиратство и терроризм в цифровом пространстве [Кочкина, 2017].

Особенностью подросткового периода является сочетание стремления к самостоятельности и интенсивного поиска собственной идентичности. Эта фаза развития сопровождается повышенной чувствительностью к мнению окружающих и усиленной восприимчивостью к внешним стимулам, включая социальные нормы и ожидания сверстников. Данные характеристики определяют специфический стиль поведения подростков в сети и увеличивают вероятность их попадания в опасные ситуации.

Эмпирическое исследование позволило подтвердить положительную динамику изменений в поведении подростков, завершивших программу «Кибергигиена». Полученные данные свидетельствуют о значительном повышении уровня осведомленности и готовности действовать ответственно в условиях киберрисков.

Анализ показал, что участники эксперимента демонстрируют гораздо более разнообразные способы использования Интернета. Так, практически все представители экспериментальной группы (100 %) регулярно посещают интернет-ресурсы преимущественно для развлекательных целей, однако значительная часть (81 %) также активно использует сеть для коммуникации, 73 % — для образовательных нужд и около 64 % — для участия в социальных медиа. Это свидетельствует о зрелом подходе к интернет-деятельности, отличающемся многообразием функций и мотиваций, в отличие от контрольной группы, члены которой использовали Интернет менее структурированно и ограниченно.

При анализе восприятия терминологии выявлено, что абсолютно все подростки, изучившие основы кибербезопасности, понимают значение термина «кибербезопасность» и связывают его непосредственно с мерами защиты в цифровом пространстве. Напротив, в контрольной группе 17 % респондентов не смогли точно определить смысл этого понятия, что подчеркивает важность специальных курсов в формировании базовой цифровой грамотности.

Несмотря на то что субъективная оценка собственных знаний оказалась несколько заниженной у обучающихся курсу (только 36 % заявили о полной уверенности в своей компетенции, тогда как в контрольной группе показатель составил 43 %), их фактическое поведение демонстрирует существенно более высокую степень подготовленности. Участники экспериментальной группы значительно чаще используют двухфакторную аутентификацию (73 % против 26 %), создают надежные пароли (73 % против 52 %) и устанавливают защитные программы (73 % против 43 %).

Кроме того, обнаружилось, что учащиеся экспериментальной группы чаще сталкивались с проявлениями различных видов киберугроз, такими как фишинг (63 % против 57 %), мошеннические схемы (55 % против 35 %), заражение вирусами (55 % против 26 %) и даже случаи буллинга в сети (45 % против 17 %). Этот феномен можно интерпретировать не как признак слабости, а скорее, как свидетельство повышенного уровня осознания рисков и способности адекватно реагировать на возникающие проблемы [Фортова, 2022: 11].

Что касается реакций на гипотетические инциденты, экспериментальная группа показала значительную готовность предпринимать активные действия. Например, подавляющее большинство опрошенных (91 %) сообщили, что немедленно сменили бы пароль или учетную запись в случае возникновения подозрительной активности, а каждый второй участник указал на намерение обратиться за поддержкой к родителям или специалистам. Подобные позитивные реакции подчеркивают эффективность предложенных методов подготовки.

Однако корреляционный анализ (коэффициент Пирсона) не выявил значимой связи между уровнем внушаемости и частотой столкновения с киберугрозами (уровень значимости $p = 0{,}947$). Это указывает на то, что уязвимость подростков в цифровом пространстве определяется более сложным комплексом факторов, включающим не только психологические особенности, но и уровень цифровой грамотности, опыт взаимодействия с Интернетом, социальное окружение и качество полученного образования в области безопасности.

Таким образом, результаты исследования подтверждают значимость специальной образовательной программы «Кибергигиена» в развитии базовых компетенций кибербезопасности у подростков (ср. [Руденкин, 2022]). Такое обучение позволяет не только повысить осведомленность детей о существующих угрозах, но и выработать устойчивые модели поведения, снижающие возможные негативные последствия пребывания в сети (см. [Самохина, 2023]).

По итогам анализа полученных данных можно заключить следующее:

- обучение основам кибербезопасности заметно повышает уровень цифровой грамотности подростков, расширяя кругозор и формируя рациональное восприятие рисков;
- прохождение специализированного курса способствует улучшению навыков практической защиты, выражающихся в соблюдении принципов

надежной аутентификации, создании сложных паролей и установке необходимых защитных инструментов;

- высокий процент зафиксированных случаев встречи с киберугрозами среди учащихся курса отражает улучшение навыков идентификации опасных ситуаций, а не рост уязвимости;
- несмотря на ожидаемую связь психологической восприимчивости с уязвимостью перед угрозами, эмпирические данные не выявили статистически значимых зависимостей между этими показателями;
- полученные результаты говорят о необходимости включения тематики кибербезопасности в школьную программу (ср. [Селюнина, Горбачева, 2017]), разработки учебных материалов и вовлечения родителей и педагогов в совместную работу над повышением уровня цифровой грамотности подрастающего поколения.

Библиографический список / References

Кочкина Э. Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162—169.

(Kochkina E. L. Definition of the concept “Cybercrime”. Separate types of cybercrimes, *Siberian Criminal Procedure and Forensic Readings*, 2017, no. 3 (17), pp. 162—169. — In Russ.)

Самохина Н. Н. Безопасность личности в интернет-пространстве: установление и защита новых границ конфиденциальности // Экономические и социально-гуманитарные исследования. 2023. № 1. С. 148—154.

Samokhina N. N. Personal security in the internet space: establishing and protecting new boundaries of privacy, *Economic and Social Research*, 2023, no. 1, pp. 148—154. — In Russ.)

Селюнина С. В., Горбачева Н. А. Теоретические и практические аспекты обеспечения информационной безопасности детей и подростков в глобальной сети // Здоровье населения и среда обитания. 2017. № 8. С. 11—17.

Selyunina S. V., Gorbacheva N. A. Theoretical and practical aspects of ensuring information security of children and teenagers in global network, *Public Health and Life Environment*, 2017, no. 8, pp. 11—17. — In Russ.)

Смирнов Д. Г. Этика ноосферной безопасности: к постановке проблемы // Вестник Ивановского государственного университета. Серия: Гуманитарные науки. 2021. № 4. С. 135—142. DOI 10.46726/H.2021.4.15.

(Smirnov D. G. Ethics of noospheric security: towards the formulation of the problem, *Ivanovo State University Bulletin*. *Series*: *Humanities*, 2021, no. 4, pp. 135—142. — In Russ.)

Смирнова А. А., Захарова Т. Ю., Синогина Е. С. Киберугрозы безопасности подростков // Научно-педагогическое обозрение. Pedagogical Review. 2017. № 3 (17). С. 99—107.

(Smirnova A. A., Zakharova T. Yu., Sinogina E. S. Cyber threats to the security of adolescents, *Scientific and Pedagogical Review. Pedagogical Review*, 2017, no. 3 (17), pp. 99—107. — In Russ.)

Руденкин Д. В. Уровень развития навыков цифровой гигиены современной российской молодежи: итоги социологического исследования // Социодинамика. 2022. № 1. С. 36—55. DOI: 10.25136/2409-7144.2022.1.37487

Rudenkin D. The level of development of digital hygiene skills of modern russian youth: The results sociological research, *Sociodynamics*, 2022, no. 1, pp, 36—55. — In Russ.)

Ушкин С. Г., Коваль Е. А., Мартынова М. Д. Цифровая безопасность подростков: социологический анализ // Интеграция образования. 2025. Т. 29, № 1. С. 114—131. doi:10.15507/1991-9468.029.202501.114-131
(Ushkin S. G., Koval E. A., Martynova M. D. Digital security of teenagers: sociological analysis, *Integration of Education*, 2025, vol. 29, no. 1, pp. 114—131. — In Russ.)

Фортова Л. К., Юдина А. М., Не Ч. К вопросу о формировании компетенций у подростков, обеспечивающих их кибербезопасность, в формате дистанционного обучения // Современное педагогическое образование. 2022. № 8. С. 10—12.
(Fortova L. K., Yudina A. M., Nie Zh. To the question of the formation of competencies in adolescents, ensuring their cybersecurity, in the format of distance learning, *Modern Pedagogical Education*, 2022, no. 8, pp. 10—12. — In Russ.)

Статья поступила в редакцию 25.01.2025; одобрена после рецензирования 22.11.2024; принята к публикации 02.12.2025.

The article was submitted 25.01.2025; approved after reviewing 22.11.2024; accepted for publication 02.12.2025.

Информация об авторе / Information about the author

Романова Александра Романовна — студентка института гуманитарных наук, Ивановский государственный университет, г. Иваново, Россия, aromanova1012@gmail.com

Romanova Alexandra Romanovna — student at the Institute of Humanities, Ivanovo State University, Ivanovo, Russian Federation, aromanova1012@gmail.com