Эсеналиева Гульзада Ашимовна,
доцент,
Американский университет в Центральной Азии,
Кыргызская Республика, город Бишкек

Ибраимова Гулайым Урановна,
бакалавр,
Международный университет «Ала-Тоо»,
Кыргызская Республика, город Бишкек

КИБЕРБЕЗОПАСНОСТЬ ШКОЛЬНИКОВ В КЫРГЫЗСТАНЕ КАК СОЦИАЛЬНО-ПЕДАГОГИЧЕСКАЯ ПРОБЛЕМА

Эсеналиева Гульзада Ашимовна,
доцент,
Борбордук Азиядагы Америка университети,
Кыргыз Республикасы, Бишкек шаары

Ибраимова Гүлайым Урановна,
бакалавр,
Эл аралык университет «Ала-Тоо»,
Кыргыз Республикасы, Бишкек шаары

КЫРГЫЗСТАНДАГЫ ОКУУЧУЛАРДЫН КИБЕРКООПСУЗДУГУ СОЦИАЛДЫК-ПЕДАГОГИКАЛЫК МАСЕЛЕ КАТАРЫ

Esenalieva Gulzada Ashimovna,
Associate Professor,
American University of Central Asia,
Kyrgyz Republic, Bishkek city,

Ibraimova Gulaiym Uranovna,
Bachelor,
International University «Ala-Too»,
Kyrgyz Republic, Bishkek city

CYBERSECURITY OF SCHOOLCHILDREN IN KYRGYZSTAN AS A SOCIO-PEDAGOGICAL PROBLEM

Аннотация: *В работе анализируются современные риски цифровой среды, влияющие на безопасность учащихся, и особенности их проявления в условиях активной цифровизации Кыргызстана. Рассматриваются основные направления педагогической работы, направленные на развитие ответственного и защищенного поведения детей в интернете. Показано, что недостаточная цифровая грамотность делает школьников уязвимыми перед различными онлайн-угрозами, требующими системной профилактики. Акцентируется внимание на необходимости комплексного взаимодействия педагогов, родителей и образовательных учреждений для формирования безопасной информационной среды.*

Аннотация: *Бул иште мектеп окуучуларынын киберкоопсуздугу маанилүү социалдык-педагогикалык көйгөй катары каралат, ал коомдун активдүү санариптешүүсүнүн шартында күчөп бара жатканын көрсөтөт. Теманын изилденүү деңгээли жана окуучулардын санариптик коопсуздугун камсыз кылуунун учурдагы абалы талданат. Кыргызстанда технологиянын тез өнүгүшү киберкоркунучтардын көбөйүшүнө алып келгендиктен, мектеп окуучулары онлайнда коопсуз жүрүүнүн билим жана көндүмдөрүнүн жетишсиздигинен улам алсыз топтордун бири болуп саналат. Кибербуллинг, фишинг жана алдамчылык сыяктуу тобокелдиктерге жана системалуу педагогикалык колдоонун зарылдыгына өзгөчө көңүл бурулган. Коопсуз билим берүү чөйрөсүн түзүүдө мугалимдердин, ата-энелердин жана билим берүү уюмдарынын биргелешкен ишинин маанилүүлүгү баса белгиленет.*

Annotation: *This study examines schoolchildren's cybersecurity as an important socio-pedagogical issue, which is becoming increasingly significant amid the rapid digitalization of society. The extent of research on the topic and the current state of ensuring students' digital safety are analyzed. Due to the rapid development of technology in Kyrgyzstan, schoolchildren remain among the most vulnerable groups because of insufficient knowledge and skills for safe online behavior. Special attention is given to risks such as cyberbullying, phishing, and fraud, as well as the need for systematic educational support. The importance of coordinated efforts among teachers, parents, and educational institutions in creating a safe learning environment is emphasized.*

Ключевые слова: *цифровая безопасность, учащиеся, интернет-угрозы, цифровая грамотность, педагогическая поддержка, профилактика рисков, образовательная среда.*

Түйүндүү сөздөр: *киберкоопсуздук, мектеп окуучулары, социалдык-педагогикалык көйгөй, санариптешүү, санариптик сабаттуулук, киберкоркунучтар, педагогикалык колдоо.*

Key words: *cybersecurity, schoolchildren, socio-pedagogical issue, digitalization, digital literacy, cyber threats, cyberbullying, phishing, fraud, safe educational environment, educational support.*

Введение. Современное образование в Кыргызской Республике активно интегрируется в глобальное цифровое пространство, что закреплено в стратегических документах страны, подчеркивающих необходимость надежного и устойчивого функционирования информационных систем [3; 4]. Однако стремительная цифровизация, особенно в школьной среде, порождает ряд новых и существенных угроз. Школьники, будучи активными пользователями интернета для обучения, общения и развлечений, часто не обладают достаточными навыками безопасного поведения в сети, что делает их уязвимыми к кибербуллингу, фишингу и мошенничеству [7; 8].

Проблема кибербезопасности в школьной системе Кыргызстана остаётся многоаспектно уязвимой – с нормативной, технической, организационной, кадровой и образовательной сторон. Усиление цифровизации без адекватных мер защиты создаёт риски, затрагивающие не только инфраструктуру школ, но и права обучающихся [5]. Глобальные инциденты утечки данных на крупнейших цифровых платформах свидетельствуют о том, что даже высокотехнологичные структуры не всегда обеспечивают

должный уровень защиты информации, в то время как образовательные учреждения, обладая ограниченными ресурсами и кадровым потенциалом, оказываются особенно уязвимыми [1; 2].

Таким образом, обеспечение кибербезопасности школьников является важнейшей социально-педагогической проблемой, требующей научного анализа и практического осмысления. Настоящее исследование направлено на формирование рекомендаций по улучшению уровня цифровой безопасности посредством анализа современных угроз, оценки рисков и разработки практических мер защиты информации в школьной среде Кыргызстана [6; 7].

Целью исследования является формирование рекомендаций по улучшению уровня цифровой безопасности на основе анализа современных угроз и методов их предотвращения, а также оценка рисков и уязвимостей для разработки практических мер защиты информации.

Методы исследования. В ходе исследования использовались методы теоретического анализа и обобщения научных источников, анализ нормативно-правовых документов Кыргызской Республики, классификация современных киберугроз, а также сравнительный анализ международного и отечественного опыта обеспечения информационной безопасности в образовательной сфере.

Основное содержание. Стремительная цифровизация школьного образования в Кыргызской Республике, закрепленная в Концепции цифровой трансформации на 2024–2028 годы и Стратегии защиты киберпространства, открывает новые образовательные возможности, но одновременно формирует многоуровневые риски для учащихся [3; 4]. Активное использование цифровых платформ и онлайн-сервисов делает школьников потенциальными объектами кибербуллинга, фишинговых атак и утечек персональных данных [8; 9].

Исследования показывают, что кибербуллинг является одной из наиболее распространенных угроз для подростков, отрицательно влияя на психоэмоциональное состояние и мотивацию к учёбе [11; 14]. Кроме того, недостаточная цифровая грамотность учащихся повышает уязвимость перед социальными и техническими угрозами в сети, включая фишинг, мошенничество и распространение вредоносного контента [9; 10].

Комплексный анализ выявил ключевые категории уязвимостей школьной цифровой среды: нормативные, технические, организационные, кадровые и образовательные. Нормативная уязвимость выражается в отсутствии унифицированных стандартов информационной безопасности для школ и региональных образовательных программ [3; 4]. Техническая уязвимость связана с использованием устаревшего оборудования, отсутствием систем шифрования и резервного копирования, что усиливает риск несанкционированного доступа и кибератак [6; 7]. Организационные пробелы проявляются в слабом контроле за использованием цифровых устройств и отсутствии планов реагирования на инциденты. Кадровая уязвимость выражается в недостаточной подготовке педагогов и низком уровне сертификации по кибербезопасности, особенно в удалённых районах [7].

Образовательная уязвимость проявляется в недостаточном внедрении программ цифровой грамотности. Образовательная уязвимость школьников во многом обусловлена недостаточным уровнем сформированности цифровых компетенций, что затрудняет их способность безопасно и осознанно использовать информационные технологии в учебной деятельности. Международный опыт показывает, что включение обязательных модулей по безопасному поведению в сети, регулярные семинары для педагогов и родительские обучающие курсы способствуют снижению риска киберугроз [9]. Например, модели цифровой грамотности включают практические занятия по распознаванию фишинга, защите личных данных и противодействию кибербуллингу.

Для повышения безопасности школьников рекомендуется комплексное взаимодействие всех заинтересованных сторон: образовательных учреждений, педагогов, родителей и государственных органов. Важным инструментом является внедрение стандартизированных чек-листов и аудит цифровой инфраструктуры школ на основе международных руководств, таких как *International CIIP Handbook*. Пилотные реализации в школах Бишкека и областных центрах позволяют апробировать эти меры перед масштабированием.

Кроме того, внедрение образовательных программ должно сочетаться с техническими мерами: прокси-серверами, двухфакторной аутентификацией, регулярными обновлениями программного обеспечения, резервным копированием данных, а также с использованием защищённых платформ для дистанционного обучения [9; 10].

Развитию практических навыков учащихся и формированию культуры безопасного поведения в цифровой среде. Программы должны быть адаптированы к возрасту и особенностям учеников, включая обучение распознаванию опасного контента, соблюдению конфиденциальности и этическому поведению в сети. «Особое внимание уделяется развитию навыков и компетенций, востребованных в XXI веке, таких как критическое мышление, умение анализировать информацию и применять знания в реальных жизненных ситуациях» [15, с. 13].

Практическое решение обозначенной проблемы кибербезопасности школьников предполагает поэтапное внедрение системной модели обеспечения цифровой безопасности в образовательной среде. В основе данной модели лежит сочетание педагогических, организационных и технических механизмов, направленных на формирование устойчивых навыков безопасного поведения в цифровом пространстве.

На педагогическом уровне ключевым элементом решения является интеграция модулей цифровой безопасности в содержание общеобразовательных дисциплин и классных часов. Эти модули должны носить прикладной характер и включать обучение распознаванию фишинговых сообщений, защите персональных данных, критическому восприятию информации и противодействию кибербуллингу. Эффективность данного подхода подтверждается исследованиями, демонстрирующими снижение числа инцидентов при регулярном обучении цифровой гигиене [9; 10].

Организационный компонент решения проблемы предполагает разработку и внедрение в школах регламентов реагирования на киберинциденты, а также распределение ответственности между администрацией, педагогами и школьными психологами. В этой связи целесообразно введение «паспорта цифровой безопасности школы», включающего аудит технической инфраструктуры, оценку рисков и план профилактических мероприятий. Такой инструмент позволяет перейти от фрагментарных мер к управляемой системе обеспечения безопасности.

Кадровое обеспечение рассматривается как одно из ключевых условий реализации предложенной модели. Повышение квалификации педагогов в области цифровой грамотности и основ кибербезопасности должно осуществляться на регулярной основе через курсы повышения квалификации, онлайн-тренинги и профессиональные сообщества. Формирование цифровых компетенций педагогов позволяет не только снизить уязвимость образовательной среды, но и повысить качество профилактической работы с учащимися [6; 7].

Технические меры включают использование защищённых образовательных платформ, настройку фильтрации контента, двухфакторную аутентификацию, резервное копирование данных и обновление программного обеспечения. Однако данные меры рассматриваются не как самостоятельное решение, а как поддерживающий элемент педагогической стратегии, ориентированной на осознанное и ответственное поведение школьников в сети [9].

Особое значение в решении проблемы имеет взаимодействие школы с родителями. Консультативные встречи, информационные

рассылки и обучающие материалы способствуют формированию единого подхода к цифровой безопасности ребёнка как в школе, так и в домашней среде. Согласованность действий всех участников образовательного процесса существенно повышает устойчивость учащихся к цифровым угрозам.

Таким образом, обеспечение кибербезопасности школьников требует системного подхода, включающего нормативные, технические, организационные, кадровые и образовательные меры, а также активное участие родителей и педагогов. Эффективная интеграция этих элементов позволит снизить риски цифровых угроз, повысить цифровую грамотность и создать безопасную образовательную среду, способствующую гармоничному развитию школьников [6; 7; 9].

Выводы. В ходе исследования установлено, что в условиях ускоренной цифровизации школьная система Кыргызской Республики характеризуется повышенной уязвимостью к современным киберугрозам. Анализ показал, что ключевыми факторами риска являются недостаточная цифровая грамотность участников образовательного процесса, ограниченность нормативного регулирования и слабая интеграция профилактических мер в школьную практику.

Полученные результаты подтверждают необходимость перехода от изолированных решений к целостной модели обеспечения кибербезопасности школьников, ориентированной на профилактику рисков и развитие цифровой культуры. Практическая значимость исследования заключается в возможности использования сформулированных рекомендаций при разработке образовательных программ и локальных стратегий цифровой безопасности. Перспективы дальнейших исследований связаны с эмпирической апробацией предложенных мер и оценкой их эффективности в различных типах образовательных организаций.

Литература:

1. Андерсон Р. Инженерия безопасности: создание надёжных распределённых систем / Р. Андерсон. – Хобокен: Wiley, 2020. – 1182 с.
2. Шнайер Б. Секреты и ложь: цифровая безопасность в сетевом мире / Б. Шнайер. – Нью-Йорк: Wiley, 2015. – 367 с.
3. Концепция цифровой трансформации Кыргызской Республики на 2024–2028 годы / Утв. Постановлением Правительства Кыргызской Республики. – Бишкек, 2023. – [Электронный ресурс]: https://cbd.minjust.gov.kg/30-164/edition/6414/ru
4. Стратегия кибербезопасности Кыргызской Республики. – Бишкек, 2022. – [Электронный ресурс]: https://cbd.minjust.gov.kg/15479/edition/962966/ru
5. Кузнецов А.В. Информационная безопасность: анализ и оценка угроз, кибер / криптозащита организаций, разработка безопасного ПО / А.В. Кузнецов. – СПб: Наука и техника, 2025. – 425 с.
6. Иванов А.В. Обзор информационных технологий и их значение в образовательной среде / А.В. Иванов // Вестник РУДН. Серия: Информатизация образования. – 2018. – Т. 15, № 1. – С. 1-7.
7. Ливингстон С., Смит П. Кибербуллинг: определение, масштабы и меры вмешательства / С. Ливингстон, П. Смит. – 2019. – 320 с.
8. Ковальски Р.М., Лимбер С.П., Агатстон П.У. Кибербуллинг: травля в цифровую эпоху / Р.М. Ковальски, С.П. Лимбер, П.У. Агатстон. – 2-е изд. – Оксфорд: Wiley-Blackwell, 2018. – 296 с.
9. Организация экономического сотрудничества и развития (ОЭСР). Образование детей XXI века: эмоциональное благополучие в цифровой эпохе. – Париж: OECD Publishing, 2021. – 251 с.
10. ЮНИСЕФ. Состояние детей в мире 2017: Дети в цифровом мире. – Нью-Йорк: Детский фонд ООН (UNICEF), 2017. – 35 с.
11. Эсеналиева Г.А. Кибербезопасность в системе образования / Г.А. Эсеналиева. – Бишкек, 2022. – 5 с.
12. Эсеналиева Г.А., Исаев Р.Р., Эрдолатов С.С., Абдиллаева Э., Дозжанов Н.

Формирование цифровой грамотности педагогов / Г.А. Эсеналиева, Р.Р. Исаев, С.С. Эрдолатов, Э. Абдиллаева, Н. Дозжанов. – 2023. – 12 с.
13. Эсеналиева Г.А. Кибербезопасность в системе образования // Alatoo Academic Studies. – Бишкек, 2022. – № 1. – С. 171-180.
14. Эсеналиева Г.А., Исаев Р.Р., Эрдолатов С.С., Абдиллаева Э., Дозжанов Н. Формирование цифровой грамотности педагогов // Alatoo Academic Studies. – Бишкек, 2023. – Т. 1. – С. 180–192.
15. Камчиева А.М., Мамытов А.М. Роль НООДУ в оценке математической грамотности учеников 4, 8 классов образовательных организаций Кыргызской Республики // Известия Кыргызской академии образования. – №1 (65), 2025. – Бишкек. – С. 11-19.

Рецензент:

Мамбетакунов У.Э.,
доктор педагогических наук, профессор