Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

УДК 371 https://doi.org/10.33619/2414-2948/126/72

КИБЕРБЕЗОПАСНОСТЬ ШКОЛЬНОЙ ИНФОРМАЦИОННО ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

*©**Эсеналиева Г. А**., ORCID: 0009-0000-9135-1671, SPIN-код: 2893-1861, канд. пед. наук, Американский университет центральной Азии, г. Бишкек, Кыргызстан, esenalieva_gu@auca.kg*
*©**Ибраимова Г. У**., ORCID: 0009-0005-6879-7778, Международный университет "Ала-Тоо", г. Бишкек, Кыргызстан, ibrmva310@gmail.com*

CYBERSECURITY OF THE SCHOOL INFORMATION AND EDUCATIONAL ENVIRONMENT IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF EDUCATION IN THE KYRGYZ REPUBLIC

*©**Esenalieva G**., ORCID: 0009-0000-9135-1671, SPIN-код: 2893-1861, Ph.D., American University of Central Asia, Bishkek, Kyrgyzstan, esenalieva_gu@auca.kg*
*©**Ibraimova G**., ORCID: 0009-0005-6879-7778, Ala-Too International University, Bishkek, Kyrgyzstan, ibrmva310@gmail.com*

Аннотация. Цифровая трансформация образования в Кыргызской Республике сопровождается активным внедрением электронных журналов, облачных сервисов, платформ дистанционного обучения и автоматизированных систем управления школьным процессом, что делает информационно образовательную среду школ особенно уязвимой к киберугрозам. При этом большинство общеобразовательных учреждений сталкивается с ограниченным финансированием, устаревшей ИТ инфраструктурой и дефицитом квалифицированных специалистов по информационной безопасности, что затрудняет создание целостной системы защиты персональных данных учащихся и педагогов. В статье анализируются основные виды киберугроз, характерные для школьной среды: фишинг и социальная инженерия, вредоносное программное обеспечение и программы вымогатели, уязвимости облачных платформ и устройств Интернета вещей, утечки персональных данных, распространение деструктивного контента и кибербуллинг. Особое внимание уделяется проблемам слабой нормативно правовой базы в сфере кибербезопасности школьного образования в Кыргызстане, отсутствию единых требований к использованию цифровых образовательных платформ и недостаточному уровню цифровой грамотности участников образовательного процесса. На основе анализа теоретических подходов и текущей практики цифровизации школьного образования обосновываются организационно педагогические и методические меры по повышению уровня кибербезопасности школьной информационно образовательной среды. Предлагаются направления интеграции основ кибергигиены и цифровой грамотности в учебные курсы, модели подготовки и повышения квалификации педагогов по вопросам информационной безопасности, а также элементы школьной политики кибербезопасности, ориентированной на профилактику инцидентов и формирование ответственного поведения в цифровой среде.

Abstract. The digital transformation of education in the Kyrgyz Republic at the same time, most general education schools face limited funding, outdated IT infrastructure and a shortage of qualified information security specialists, which complicates the development of a comprehensive system for protecting students' and teachers' personal data. This paper analyzes the main types of cyber threats specific to the school context, including phishing and social engineering, malware and ransomware,

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

vulnerabilities of cloud-based learning platforms and Internet of Things devices, personal data leaks, dissemination of harmful digital content and cyberbullying. Special attention is paid to weaknesses of the regulatory framework for school cybersecurity in the Kyrgyz Republic, the lack of unified requirements for the use of digital educational platforms and the insufficient level of digital literacy among participants of the educational process. Building on theoretical approaches and the current practice of school digitalization, the article substantiates organizational, pedagogical and methodological measures aimed at improving the cybersecurity of the school information and educational environment. The paper proposes directions for integrating the basics of cyber hygiene and digital literacy into school curricula, outlines models of teacher training and professional development in information security and discusses key elements of school cybersecurity policy focused on incident prevention and fostering responsible behavior in the digital environment.

Ключевые слова: кибербезопасность, цифровая трансформация образования, киберугрозы, защита персональных данных, цифровая грамотность, кибергигиена.

Keywords: cybersecurity, digital transformation of education, cyber threats, personal data protection, digital literacy, cyber hygiene.

В настоящее время цифровая безопасность играет ключевую роль в обеспечении защиты информации и персональных данных в условиях стремительно развивающегося цифрового пространства. С развитием информационных технологий и расширением интернет-охвата в Кыргызстане, как и во всем мире, наблюдается рост киберугроз, включая кибератаки, кражу личных данных и другие формы цифровой агрессии. Эти вызовы делают вопросы кибербезопасности особенно актуальными для общества, особенно в условиях цифровизации ключевых сфер — банковского сектора, здравоохранения и образования.

В Кыргызстане процесс цифровизации охватывает практически все аспекты общественной жизни. Электронное хранение данных становится нормой, что, с одной стороны, упрощает доступ к информации, а с другой — увеличивает уязвимость перед киберпреступностью. Чем больше данных переводится в цифровой формат, тем выше риск их компрометации. Это особенно важно для страны с развивающейся цифровой инфраструктурой, где системы защиты ещё не полностью адаптированы к современным угрозам.

Цифровая трансформация образования радикально изменяет способы организации учебного процесса, управления школой и взаимодействия участников образовательной среды. В Кыргызской Республике этот процесс сопровождается внедрением электронных журналов и дневников, облачных платформ, систем дистанционного обучения, а также широким использованием мобильных устройств и сервисов коммуникации в повседневной школьной практике. Ограниченные финансовые ресурсы образовательных учреждений, устаревшая ИТ-инфраструктура, дефицит специалистов по информационной безопасности и низкий уровень цифровой грамотности формируют совокупность факторов риска, повышающих вероятность киберинцидентов [1–4].

Одновременно с расширением цифровой инфраструктуры существенно возрастает зависимость школ от устойчивости и безопасности информационных систем, что выводит проблему кибербезопасности в число ключевых условий функционирования современного образования. Особую значимость проблема кибербезопасности приобретает в школьной среде, поскольку активными участниками цифровых процессов являются дети и подростки — наиболее уязвимая категория пользователей. Школьная среда представляет собой уникальное

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

пространство, где дети активно используют интернет для обучения, общения и развлечений, но при этом часто не обладают достаточными навыками безопасного поведения в сети. Они становятся уязвимыми перед такими угрозами, как кибербуллинг, фишинг, мошенничество и воздействие вредоносного контента. Например, исследования показывают, что значительная часть школьников в Кыргызстане сталкивается с попытками фишинга, а многие из них не умеют распознавать подозрительные ссылки. Это подчеркивает необходимость внедрения образовательных программ по кибербезопасности.

Школьники — это не только будущее страны, но и активные участники цифрового общества уже сегодня. Отсутствие культуры кибербезопасности среди молодёжи может привести к долгосрочным последствиям, включая утрату доверия к цифровым технологиям и рост числа инцидентов, связанных с утечкой данных. Таким образом, образовательные учреждения в Кыргызстане должны стать ключевыми площадками для формирования осведомленности и навыков безопасного взаимодействия с цифровой средой.

Целью настоящей статьи является анализ основных киберугроз школьной информационно-образовательной среды в условиях цифровой трансформации образования Кыргызской Республики и обоснование комплекса организационно-педагогических и методических мер по повышению уровня ее кибербезопасности.

Материал и методы исследования

Данное исследование представляет собой педагогический эксперимент, направленный на апробацию модели формирования культуры кибербезопасности у обучающихся общеобразовательных организаций Кыргызской Республики. Эксперимент проводился в 2025–2026 гг. на базе 727 общеобразовательных организаций, расположенных в четырех регионах страны: Ошская, Джалал-Абадская, Баткенская области и город Ош.

Выборка исследования: родители обучающихся (N = 21 397) — законные представители учащихся 5–11 классов; педагоги (N = 890) — учителя-предметники, классные руководители, педагоги-психологи и социальные педагоги; ученики (N = 848) в возрасте 12–16 лет (6–10 классы).

Эксперимент состоял из трех последовательных этапов:

1. Констатирующий этап (январь — сентябрь 2025 г.) — выявление исходного уровня сформированности культуры кибербезопасности участников образовательного процесса посредством анкетирования, фокус-групп и диагностического тестирования. В рамках этапа оценивались когнитивные, поведенческие, мотивационные и практические показатели кибербезопасности;

2. Формирующий этап (сентябрь — декабрь 2025 г.) — апробация разработанной модели, включающей комплекс мероприятий: организация обучающих семинаров и информационно-просветительской работы с родителями; интеграция занятий по кибербезопасности в учебный процесс и внеурочную деятельность учащихся; повышение квалификации педагогов через программу «Training of Trainers» (40 академических часов).

3. Контрольный этап (декабрь 2025 — февраль 2026 г.) — оценка эффективности модели путем повторного анкетирования, анализа статистической значимости изменений и мониторинга динамики показателей на интерактивной платформе CyberLab.

Инструменты исследования: анкетные опросы и фокус-группы для выявления знаний, навыков и мотивации участников; интерактивная образовательная платформа CyberLab, включающая диагностические тесты, теоретические материалы, практические тренажёры и аналитический блок; статистический анализ результатов с использованием критерия χ^2 для проверки значимости изменений.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Данный комплексный подход обеспечил всестороннее изучение и повышение уровня культуры кибербезопасности у обучающихся, педагогов и родителей в условиях общеобразовательных организаций.

Результаты и обсуждение

Педагогический эксперимент является центральным методом исследования в педагогической науке, позволяющим не только описать, но и объяснить педагогические явления, а также проверить эффективность предложенных педагогических воздействий. В контексте настоящего диссертационного исследования педагогический эксперимент был направлен на апробацию разработанной модели формирования культуры кибербезопасности обучающихся общеобразовательных организаций Кыргызской Республики.

Актуальность проведения педагогического эксперимента в области кибербезопасности обусловлена рядом факторов. Во-первых, стремительное развитие информационно-коммуникационных технологий и массовое проникновение интернета во все сферы жизнедеятельности современных школьников требует формирования у них устойчивых навыков безопасного поведения в цифровой среде. Во-вторых, исследования последних лет фиксируют рост числа киберинцидентов с участием несовершеннолетних: кибербуллинг, фишинговые атаки, интернет-мошенничество, вовлечение в деструктивные сообщества. В-третьих, существующие образовательные программы не в полной мере отвечают современным вызовам цифровой безопасности, что актуализирует необходимость разработки и апробации новых педагогических подходов.

Целью педагогического эксперимента явилась комплексная проверка эффективности разработанной модели формирования культуры кибербезопасности обучающихся общеобразовательных организаций.

Научное обоснование критериев оценки уровня обеспеченности кибербезопасности в образовательной организации представляет собой сложную методологическую задачу, требующую междисциплинарного подхода. Как справедливо отмечают исследователи, создание безопасной цифровой среды для школьников предполагает не только технические решения, но и комплексную педагогическую работу, направленную на формирование устойчивых поведенческих паттернов. При разработке критериальной базы исследования мы опирались на теоретические положения о критериях оценки педагогических явлений, компетентностный подход в образовании, концепт цифровой грамотности, а также современные исследования в области информационной безопасности личности. Теоретический анализ научной литературы и эмпирическое исследование позволили выделить четыре ключевых критерия обеспеченности кибербезопасности в образовательной организации.

Когнитивный критерий отражает уровень знаний и осведомлённости участников образовательного процесса об угрозах цифровой среды, основах цифровой гигиены и методах защиты личных данных. Данный критерий включает следующие показатели: знание основных видов киберугроз (фишинг, вредоносное программное обеспечение, социальная инженерия); понимание принципов защиты персональных данных; осведомлённость о правовых аспектах поведения в сети интернет; знание алгоритмов действий при столкновении с киберугрозами;

Практико-ориентированный критерий характеризует сформированность умений и навыков, позволяющих распознавать риски и применять адекватные меры защиты в реальных ситуациях цифровоговзаимодействия. К показателям данного критерия относятся: умение создавать и управлять надёжными паролями; навыки распознавания фишинговых сообщений

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

и мошеннических схем; умение настраиватьпараметры конфиденциальности в социальных сетях; способность критически оценивать информацию в интернете.

Мотивационный критерий отражает степень заинтересованности субъектов образовательного процесса в повышении собственной цифровой грамотности и готовности участвовать в обучающих и просветительских мероприятиях. Показателями мотивационного критерия являются: наличие внутренней мотивации к соблюдению правил кибербезопасности; готовность к самообразованию в области цифровой безопасности; стремление транслировать полученные знания другим участникам образовательного процесса.

Поведенческий критерий описывает сформированность устойчивых моделей безопасного поведения в сети. К его показателям относятся: регулярное применение мер цифровой защиты; соблюдение правил сетевого этикета; ответственное отношение к размещению информации в сети; готовность сообщать о киберинцидентах.

Для эмпирического подтверждения выделенных критериев и выявления скрытых закономерностей в данных была проведена обработка массива открытых ответов респондентов с использованием современных методов машинного обучения и статистического анализа. Применение методов понижения размерности — t-distributed Stochastic Neighbor Embedding (t-SNE) и анализа главных компонент (Principal Component Analysis, PCA) — позволило визуализировать структуру данных и выявить тематические кластеры в ответах участников исследования. Метод анализа главных компонент (PCA) представляет собой ортогональное линейное преобразование, переводящее данные в новую систему координат таким образом, что наибольшая дисперсия данных приходится на первую главную компоненту, следующая по величине — на вторую и так далее. В контексте настоящего исследования PCA применялся для выявления основных факторов, определяющих вариативность ответов респондентов на вопросы о кибербезопасности. На Рисунке 1 представлена трёхмерная визуализация распределения ответов респондентов в пространстве первых трёх главных компонент. Каждая точка на диаграмме соответствует одному открытому ответу; цветовая кодировка отражает принадлежность к определённому кластеру, выделенному методом k-means.

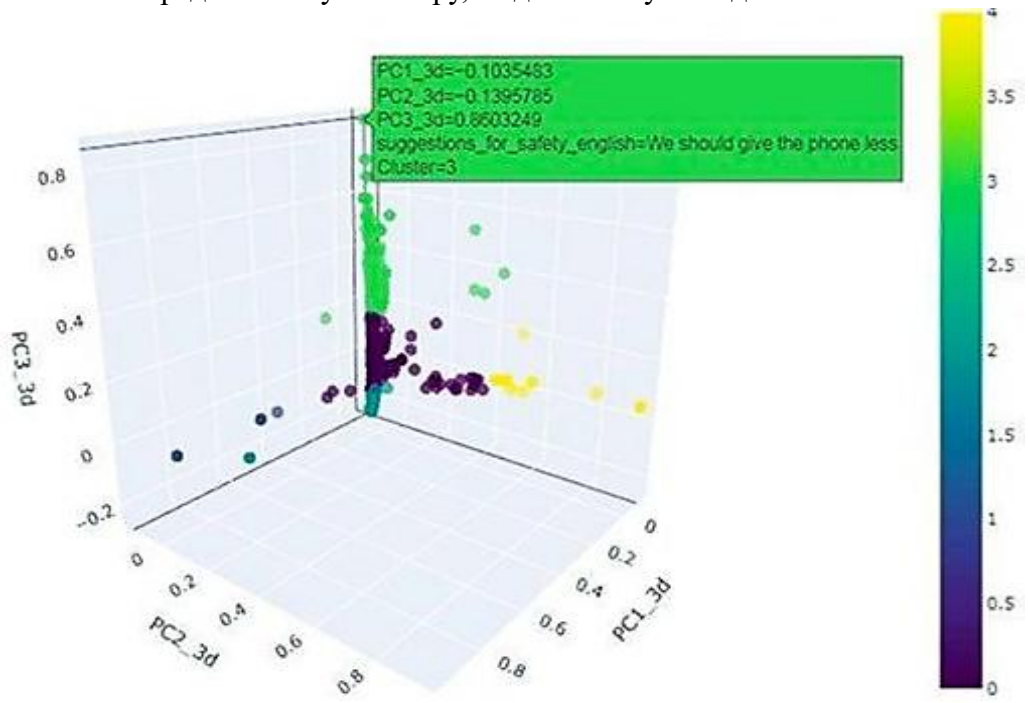

Рисунок 1. 3D-визуализация распределения ответов в пространстве трёх главных компонент PCA

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Анализ визуализации позволяет констатировать наличие ярко выраженной кластерной структуры данных: выделяются несколько плотных групп ответов, объединённых общей тематикой, а также периферийные точки, соответствующие нетипичным или размытым формулировкам. Интерпретация первых трёх главных компонент, объясняющих в совокупности 67,3% общей дисперсии данных, позволяет соотнести их с выделенными критериями кибербезопасности. Первая главная компонента (PC1), объясняющая 31,2% дисперсии, может быть интерпретирована как ось «осведомлённость — неосведомлённость». Вторая компонента (PC2, 21,8% дисперсии) отражает противопоставление «контроль — доверие» в подходах к обеспечению кибербезопасности детей. Третья компонента (PC3, 14,3% дисперсии) связана с мотивационной готовностью к обучению. Диаграмма объяснённой дисперсии демонстрирует, что первые компоненты объясняют наибольшую долю вариации данных.

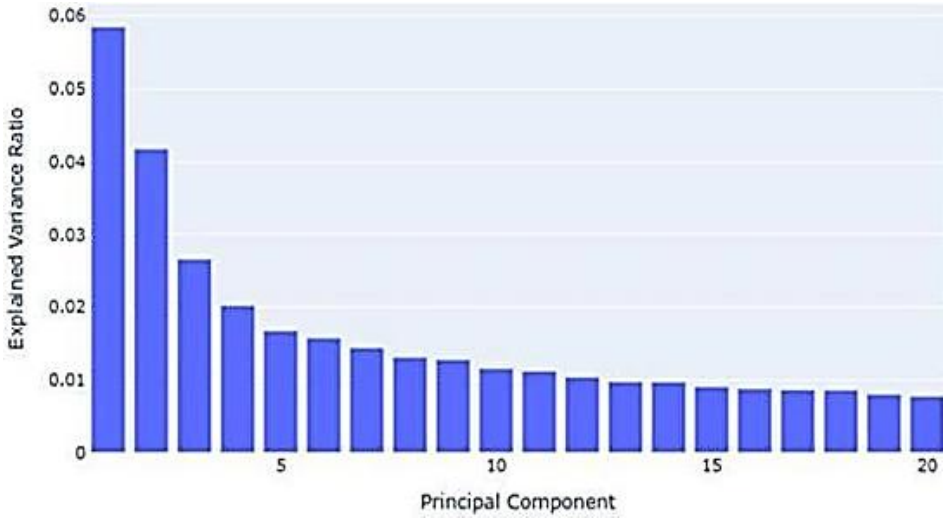

Рисунок 2. Объяснённая дисперсия главных компонент (PCA)

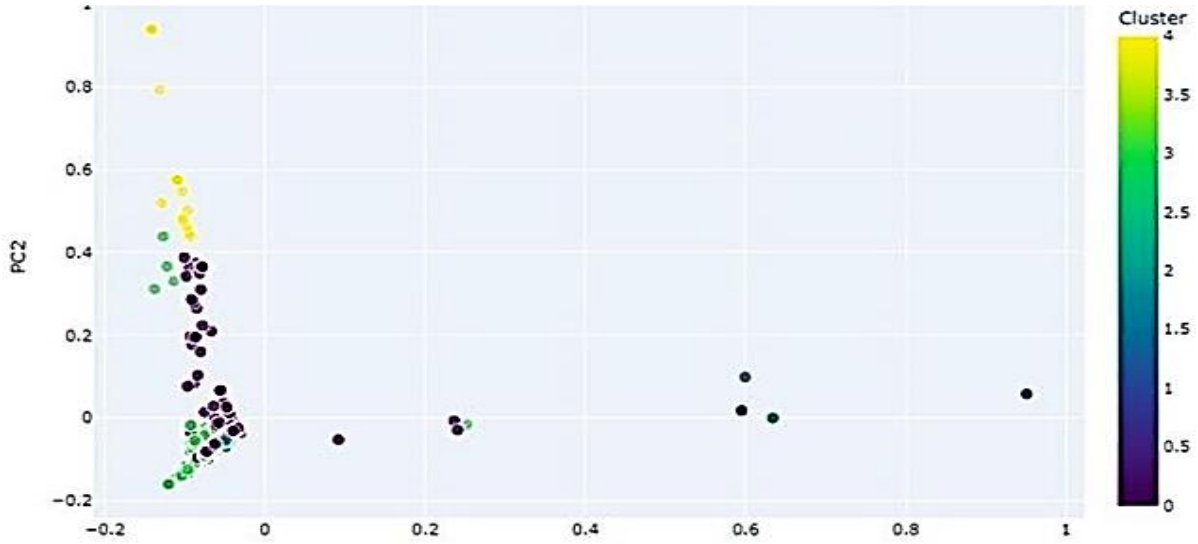

Рисунок 3. Распределение ответов в пространстве первых двух компонент PCA

Кумулятивная кривая показывает, что для объяснения 80% дисперсии достаточно пяти главных компонент, что свидетельствует о наличии устойчивой факторной структуры в данных. Проекция данных на плоскость первых двух главных компонент позволяет более

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

детально рассмотреть структуру кластеров. Компактная группа точек в левой нижней части диаграммы соответствует ответам респондентов с высоким уровнем когнитивной осведомлённости и выраженной мотивацией к обучению.

Метод t-SNE (t-distributed Stochastic Neighbor Embedding) был применён для нелинейного понижения размерности и визуализации локальной структуры данных. В отличие от PCA, t-SNE сохраняет преимущественно локальные связи между точками, что делает его особенно эффективным для выявления кластеров в высокоразмерных данных. На Рисунке 4 представлена t-SNE-визуализация семантической структуры ответов респондентов. Крупные области одинакового цвета соответствуют тематически близким ответам, что подтверждает наличие устойчивых паттернов восприятия проблемы кибербезопасности.

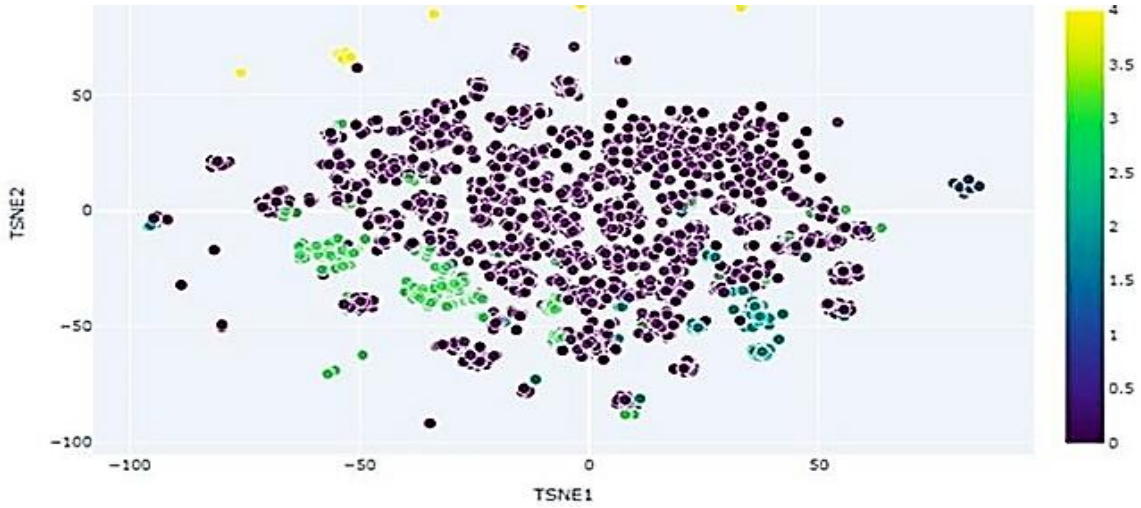

Рисунок 4. t-SNE-визуализация семантической структуры ответов

Центральный фиолетовый кластер объединяет ответы с неопределёнными, размытыми формулировками, свидетельствующими о недостаточной осведомлённости респондентов. Зелёные кластеры в наружных областях карты предоставляют ответам, содержащие призывы к обучению и развитию цифровой грамотности. Желтые и голубые точки предоставляют ответы с предложениями авторитарногоконтроля использования цифровых устройств. Детальный анализ части t-SNE-карты (Рисунок 5) помогает выявлять переходные зоны между основными кластерами. Криволинейные траектории точек предоставляют наличие ответов, сочетающихкарактеристики различных подходов к проблеме кибербезопасности.

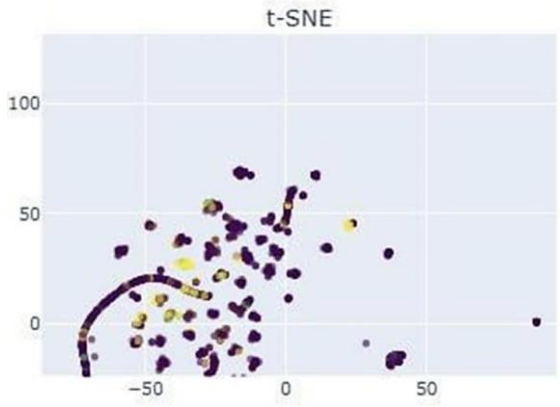

Рисунок 5. Фрагмент t-SNE-карты, демонстрирующий переходные ответы

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Кластерный анализ, проведённый на основе результатов t-SNE и PCA, предоставил возможность выделить несколько типичных групп ответов, демонстрирующих различные позиции участников образовательного процесса относительно проблемы кибербезопасности.

Кластер 1 (32,4% ответов) — Информационный дефицит. Данный кластер объединяет короткие, расплывчатые формулировки, показывающие низкий уровень осведомлённости респондентов в вопросах кибербезопасности.

Кластер 2 (8,7% ответов) — Негативные или «нулевые» ответы. Этот кластер включает ответы респондентов, которые не видят необходимости в каких-либо изменениях существующей ситуации.

Кластер 3 (41,2% ответов) — Обучающий подход. Наиболее многочисленный кластер объединяет различные предложения по организации образовательных мероприятий, повышению цифровой культуры и развитию практических навыков кибербезопасности.

Кластер 4. (17,7% ответов) Авторитарный контроль . Кластер включает рекомендации по введению жестких ограничений на использование цифровых устройств и интернета детьми.

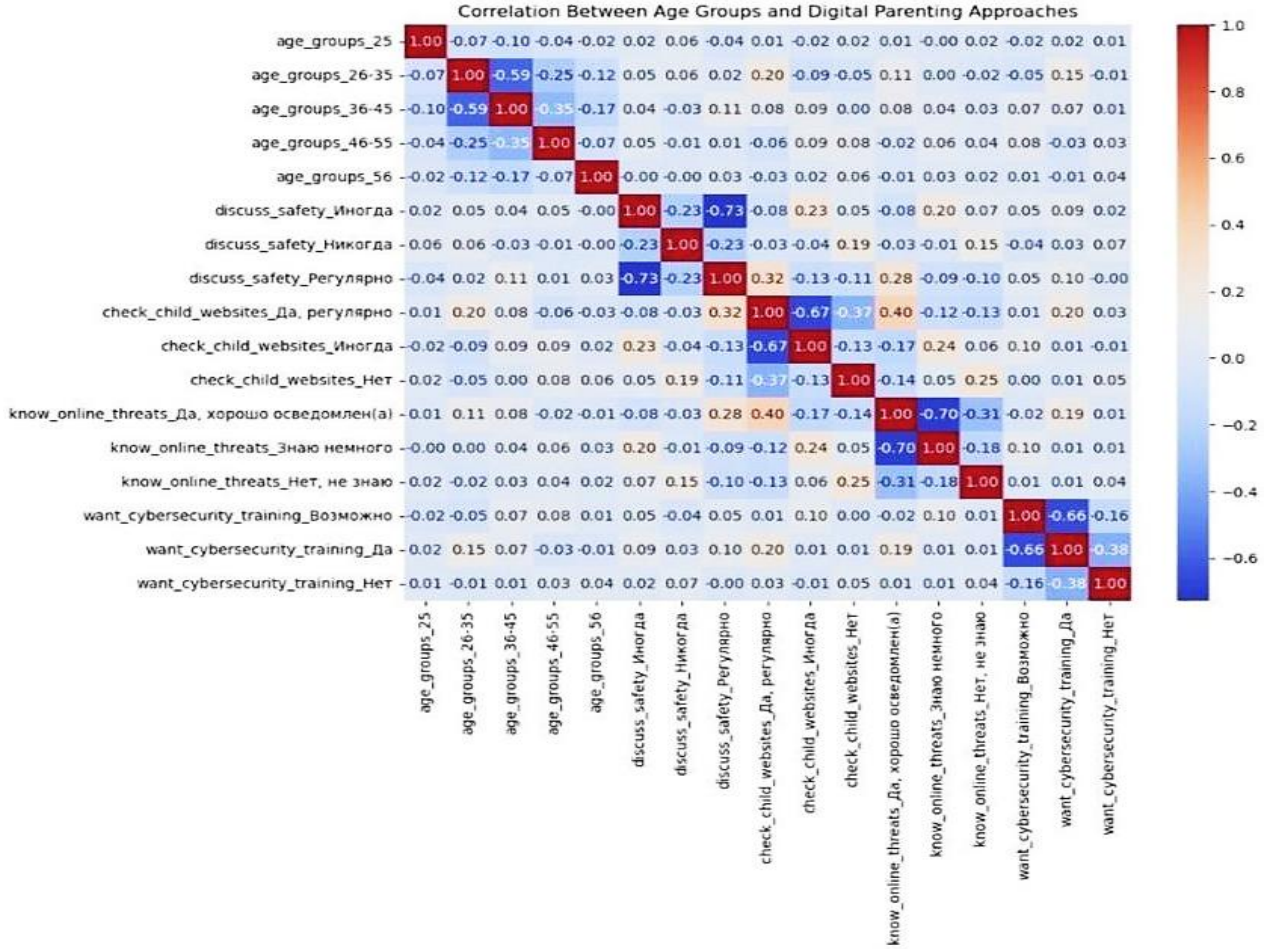

Рисунок 6. Корреляция между возрастными группами родителей и цифровыми практиками

Результаты кластерного анализа позволили выявить ключевые дефициты в обеспечении кибербезопасности обучающихся: *дефицит системных знаний*. Значительная часть родителей, педагогов и учащихся не обладает достаточными знаниями о современных киберугрозах и способах защиты от них; *дефицит координации*. Отмечается недостаточное взаимодействие между школой и семьёй по вопросам цифровой безопасности; *дефицит нормативной культуры*. Выявлена низкая осведомлённость участников образовательного процесса о законодательных нормах, регулирующих поведение в цифровой среде. Для выявления

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

взаимосвязей между различными факторами, влияющими на уровень обеспеченности кибербезопасности в образовательной организации, был проведён корреляционный анализ с использованием коэффициента корреляции Пирсона. Анализ корреляционной матрицы (Рисунок 6) позволил выявить ряд статистически значимых взаимосвязей между изучаемыми переменными.

Установлена статистически значимая положительная корреляция между уровнем знаний родителей о киберугрозах и регулярностью обсуждения вопросов безопасности с детьми ($r = 0,58$, $p < 0,01$). Выявлена обратная корреляция между уровнем знаний о киберугрозах и желанием участвовать в дополнительном обучении ($r = -0,32$, $p < 0,05$).

Проведённый комплексный анализ с использованием методов машинного обучения (t-SNE, PCA), кластерного и корреляционного анализа позволил не только обосновать выделенные критерии оценкиобеспеченности кибербезопасности, но и выявить скрытую структуру данных, недоступную при традиционных методах анализа.

Выявленные дефициты — системных знаний, координации между школой и семьёй, нормативной культуры, практических навыков — определили целевые ориентиры педагогической работы наформирующем этапе эксперимента. Педагогический эксперимент по апробации модели формирования культуры кибербезопасности обучающихся был организован в соответствии с требованиями педагогической методологии и включалтри последовательных этапа: констатирующий, формирующий и контрольный. Цель эксперимента состояла в проверке эффективности разработанной модели формирования культуры кибербезопасности обучающихся общеобразовательных организаций Кыргызской Республики.

Гипотеза эксперимента: реализация разработанной модели педагогического сопровождения, включающей работу со всеми участниками образовательного процесса (учащимися, родителями, педагогами) с использованием интерактивных форм и цифровых образовательных инструментов, обеспечит статистически значимое повышение уровня сформированности культуры кибербезопасности.

Педагогический эксперимент проводился на базе общеобразовательных организаций Кыргызской Республики в период 2025–2026 годов. Экспериментальная работа охватила четыре региона страны: Ошскую область, Джалал-Абадскую область, Баткенскую область и город Ош. В эксперименте приняли участие три категории респондентов: родители обучающихся ($N = 21\ 397$). Данная категория представлена родителями и законными представителями учащихся 5–11 классов из 727 общеобразовательных организаций; педагоги общеобразовательных организаций ($N = 890$). Выборка включала учителей- предметников, классных руководителей, педагогов-психологов и социальных педагогов; учащиеся ($N = 848$). В исследовании участвовали школьники в возрасте 12–16 лет (6– 10 классы).

Констатирующий этап (январь 2025 — сентябрь 2025) был направлен на выявление исходного уровня сформированности культуры кибербезопасности у участников образовательного процесса.

Формирующий этап (сентябрь 2025 — декабрь 2025) был направлен на апробацию разработанной модели формирования культуры кибербезопасности.

Контрольный этап (декабрь 2025 — февраль 2026) был направлен на оценку эффективности внедрённой модели.

Анкетирование родителей на констатирующем этапе позволило получить комплексную картину исходного уровня цифровой осведомлённости и практик обеспечения кибербезопасности детей в семьях.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Осведомлённость о кибергигиене. На вопрос «Знаете ли вы, что такое кибергигиена?» 53,7% респондентов ответили утвердительно, 46,3% — отрицательно. Выявлена статистически значимаязависимость уровня осведомлённости от возраста респондентов.

Анкетирование учащихся 12–16 лет позволило выявить уровень их осведомлённости о вопросах кибербезопасности, сформированность практических навыков защиты и личный опыт столкновения с киберугрозами. Понимание термина «кибербезопасность». Более половины респондентов (52,4%) дали отрицательный или неуверенный ответ. Навыки защиты паролей. 72,6% ответили отрицательно или выразилинеуверенность. Опыт кибербуллинга. 20,1% респондентов сообщили, что лично подвергались онлайн-травле.

Таблица

СВОДНЫЕ РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ РОДИТЕЛЕЙ

Показатель	*Результат,%*	*Интерпретация*
Знают о кибергигиене	53,7	Почти половинане обладает базовой грамотностью
Ребёнок в интернете > 3 ч/день	34,4	Высокий риск цифровой зависимости
Обсуждают безопасность регулярно	46,8	Менее половины систематически обсуждают
Не применяют мерзащиты	12,7	Низкий уровень практического применения
Готовы к обучению	90,9	Высокий запрос на образовательную программу

Анкетирование педагогов позволило оценить их профессиональную готовность к работе по формированию культуры кибербезопасности обучающихся.

Самооценка уровня осведомлённости. 51,5% педагогов оценили свой уровень как средний. Опыт столкновения с кибербуллингом. 27,8% педагогов сообщили, что сталкивались со случаямикибербуллинга среди учеников. Меры по повышению грамотности. 74,5% обсуждают тему на уроках, но лишь 21,9% проводят специальные занятия. Важным компонентом педагогического эксперимента стало использование разработанной онлайн-платформы CyberLab — интерактивного образовательного ресурса, предназначенного дляформирования у учащихся практических навыков кибербезопасного поведения в цифровой среде. Архитектура платформы CyberLab включает: диагностический блок, теоретический блок, практический блок с тренажёрами и симуляторами, аналитический блок для мониторинга прогресса.

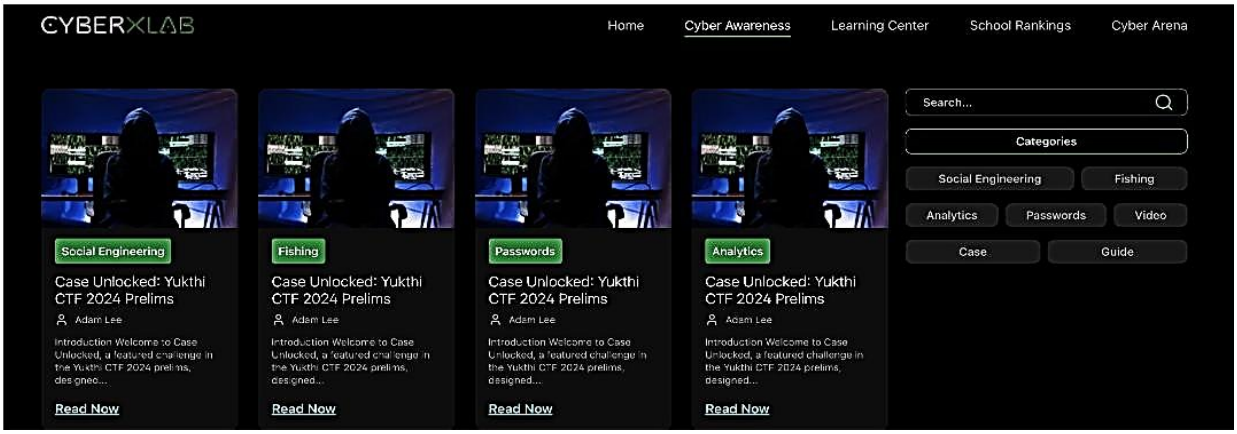

Рисунок 7. Интерфейс онлайн-платформы CyberLab (фрагмент обучающего модуля)

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Платформа CyberLab разработана с учётом возрастных особенностей целевой аудитории и включает ряд инновационных образовательных инструментов, обеспечивающих высокую вовлечённость и эффективность обучения.

Симулятор «Цифровой детектив» Учащиеся выступают в роли следователей, расследующих инциденты кибербезопасности. Каждый сценарий основан на реальных случаях:

1. Сценарий «Взлом аккаунта»: Участник анализирует цифровые улики, чтобы понять, как был взломан аккаунт одноклассника, и составляет рекомендации по предотвращению подобных инцидентов;

2. Педагогическая ценность: Метод расследования активирует аналитическое мышление и формирует понимание механизмов кибератак «изнутри»;

3. Результаты апробации: 94,2% учащихся оценили симулятор как «интересный» или «очень интересный»; среднее время прохождения модуля превысило рекомендуемое на 34%, что свидетельствует о высокойвовлечённости.

Интерактивный квест «Безопасный маршрут». Учащиеся проходят типичный день школьника, на каждом этапе которого принимают решения, связанные с кибербезопасностью:

Утро: получение подозрительного СМС «от банка мамы»

Школа: друг просит пароль от Wi-Fi для «срочного дела»

После уроков: незнакомец в онлайн-игре предлагает «дружбу»

Вечер: всплывающее окно обещает бесплатные игровые бонусы

Механика: Каждое решение влияет на «уровень цифровой безопасности» персонажа. В конце дня участник получает детальный разбор своих решений с альтернативными сценариями.

История из апробации: Ученик 6 класса, прошедший квест, на следующий день получил реальное СМС с просьбой перейти по ссылке для «подтверждения доставки». Он немедленно распознал сходство с игровым сценарием и показал сообщение родителям вместо того, чтобы переходить по ссылке.

Тренажёр «Создатель паролей». Геймифицированный модуль, где учащиеся соревнуются в создании надёжных, но запоминаемых паролей:

Этап 1. «Взломщик»: Учащиеся пытаются угадать простые пароли (123456, password, qwerty), осознавая их уязвимость;

Этап 2. «Защитник»: Создание собственных паролей по методу ассоциативных фраз;

Этап 3. «Хранитель»: Знакомство с принципами работы менеджеров паролей.

Измеримый результат: До прохождения модуля 73,4% учащихся использовали один пароль для всех аккаунтов; после — только 18,7%.

Метод «Обратная социальная инженерия». Учащиеся не только учатся защищаться от манипуляций, но и анализируют техники манипуляторов «изнутри». В безопасной учебной среде они разрабатывают (но не реализуют) сценарии социальнойинженерии, что позволяет глубже понять психологические механизмы атак.

Педагогическое обоснование: Понимание тактик атакующего формирует более устойчивую защиту, чем простое заучивание правил.

Контрольный этап педагогического эксперимента был направлен на оценку эффективности реализованной модели. Повторное анкетирование участников экспериментальной группы и сравнительныйанализ с контрольной группой позволили оценить динамику изменений.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Динамика показателей в группе родителей. Осведомлённость о кибергигиене возросла с 53,7% до 78,4% (прирост 24,7 п.п., $p < 0,01$). Регулярность обсуждения вопросов безопасности увеличилась с 46,8% до 67,3% (прирост 20,5 п.п., $p < 0,01$).

Динамика показателей в группе учащихся. Понимание термина «кибербезопасность» возросло с 47,6% до 84,3% (прирост 36,7 п.п., $p < 0,001$). Уверенность в навыках защиты паролей увеличилась с 27,4% до 68,9% (прирост 41,5 п.п., $p < 0,001$).

Динамика показателей в группе педагогов. Доля педагогов с высокой самооценкой возросла с 43,9% до 89,3% (прирост 45,4 п.п., $p < 0,001$). Проведение специальных занятий увеличилось с 21,9% до67,8% (прирост 45,9 п.п., $p < 0,001$).

В условиях активной цифровой трансформации образования в Кыргызской Республике обеспечение кибербезопасности школьной информационно-образовательной среды приобретает стратегическое значение. Анализ основных видов киберугроз, таких как фишинг, вредоносное ПО, уязвимости облачных платформ, утечки персональных данных и кибербуллинг, показал высокую степень уязвимости образовательных организаций, обусловленную ограниченным финансированием, устаревшей ИТ-инфраструктурой и дефицитом квалифицированных специалистов в области информационной безопасности.

Педагогический эксперимент, проведённый в 727 общеобразовательных организациях, подтвердил необходимость системного подхода к формированию культуры кибербезопасности, включающего когнитивный, практико-ориентированный, мотивационный и поведенческий критерии. Разработка и внедрение специализированных образовательных ресурсов, таких как онлайн-платформа CyberLab, способствует повышению цифровой грамотности и формированию навыков безопасного поведения в цифровой среде у учащихся и педагогов.

Для дальнейшего повышения уровня кибербезопасности необходимо усиление нормативно-правовой базы, создание единых стандартов использования цифровых образовательных платформ, а также активное включение основ кибергигиены и информационной безопасности в учебные программы и программы профессионального развития педагогов. Важно стимулировать заинтересованность всех участников образовательного процесса в профилактике киберинцидентов и формировании ответственного поведения в цифровом пространстве. Таким образом, комплексный организационно-педагогический подход, опирающийся на современные методики обучения и инновационные технологии, является ключевым условием успешной цифровой трансформации школьного образования с надёжной защитой персональных данных и устойчивым развитием информационной культуры в условиях стремительно меняющегося цифрового мира.

Список литературы:

1. Красовская Л. В., Исабекова Т. И. Использование информационных технологий в образовании // Научный результат. Педагогика и психология образования. 2017. Т. 3. №4(14). С. 29-36.

2. Петухова М. В. и др. Практическая деятельность по разработке системы задач как условие подготовки будущего педагога цифровой школы // Перспективы науки и образования. 2021. №2 (50). С. 187-203.

3. Туктарова Л. Р. Проблемы внедрения инноваций в образовании // Сборник избранных статей по материалам научных конференций. СПб., 2021. С. 75-77. https://doi.org/10.37539/NOV322.2021.50.97.002

4. Витуханова, Ю. С., Лысенкова И. Ю. Инновации в образовании // Скиф. Вопросы студенческой науки. 2020. №5-1(45). С. 111-117.

References:

1. Krasovskaya, L. V., & Isabekova, T. I. (2017). Ispol′zovanie informatsionnykh tekhnologij v obrazovanii. Nauchnyj rezul′tat. *Pedagogika i psikhologiya obrazovaniya, 3*(4 (14)), 29-36. (in Russian)

2. Petukhova, M. V., Novoselova, S. Yu., Soboleva, E. V., & Suvorova, T. N. (2021). Prakticheskaya deyatel′nost′ po razrabotke sistemy zadach kak uslovie podgotovki budushchego pedagoga tsifrovoj shkoly. *Perspektivy nauki i obrazovaniya,* (2 (50)), 187-203. (in Russian)

3. Tuktarova, L. R. (2021). Problemy vnedreniya innovatsij v obrazovanii. In *Sbornik izbrannykh statej po materialam nauchnykh konferentsij.* St. Petersburg. 75-77. https://doi.org/10.37539/NOV322.2021.50.97.002

4. Vitukhanova, Yu. S., & Lysenkova, I. Yu. (2020). Innovatsii v obrazovanii. *Skif. Voprosy studencheskoj nauki,* (5-1(45)), 111-117.

Поступила в редакцию
06.03.2026 г.

Принята к публикации
15.03.2026 г.

Ссылка для цитирования:

Эсеналиева Г. А., Ибраимова Г. У. Кибербезопасность школьной информационно образовательной среды в условиях цифровой трансформации образования Кыргызской Республики // Бюллетень науки и практики. 2026. Т. 12. №5. С. 573-585. https://doi.org/10.33619/2414-2948/126/72

Cite as (APA):

Esenalieva, G., & Ibraimova, G. (2026). Cybersecurity of the School Information and Educational Environment in the Context of the Digital Transformation of Education in the Kyrgyz Republic. *Bulletin of Science and Practice, 12*(5), 573-585. (in Russian). https://doi.org/10.33619/2414-2948/126/72