УДК 373.1.02:372.8
ГРНТИ 14.25.09
DOI

ОҚУШЫЛАРДЫ САНДЫҚ ҚАУІПСІЗДІК ҚАҒИДАЛАРЫНА ОҚЫТУ ТӘЖІРИБЕСІ

Кульгускина Елена Олеговна
физика және информатика пәнінің мұғалімі
мектеп-гимназия, Тобыл қаласы, Қостанай ауданы, Қостанай облысы, Қазақстан
kulguskina-e@mail.ru

ОПЫТ ОБУЧЕНИЯ ШКОЛЬНИКОВ ПРАВИЛАМ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Кульгускина Елена Олеговна
учитель физики и информатики
КГУ«Школа - гимназия города Тобыл отдела образования Костанайского района»
Управления образования акимата Костанайской области ,
г. Тобол, Костанайская область, Казахстан
kulguskina-e@mail.ru

THE EXPERIENCE OF TEACHING SCHOOLCHILDREN THE RULES OF DIGITAL SECURITY

Kulguskina Elena Olegovna
teacher of Physics and Computer science,school-gymnasium,
Tobyl, Kostanay district, Kostanay region, Kazakhstan
kulguskina-e@mail.ru

Аңдатпа

«Цифрлық гигиена» курсының оқыту тапсырмаларының кешені кең практикалық мәнге ие және оқушылардың әртүрлі ақпараттық қатерлерді жедел анықтау дағдыларын қалыптастыру үшін жағдай жасауды көздейді. Оқушылардың сандық қауіпсіздігі мәселесінде ата-аналардың ақпараттық құзыреттілігі маңызды болып табылады. Олармен де түсіндіру жұмыстарын жүргізу қажет. Көбінесе аға буын жастардың цифрлық ортаға тартылу дәрежесін жете бағаламайды және киберқылмыскерлер тарапынан оқушыларға манипуляциялық ықпал ету тәсілдерінің әртүрлілігі туралы ақпаратты білмейді.

Аннотация

Комплекс обучающих заданий курса «Цифровая гигиена» имеет широкое практическое значение и предполагает создание условий для формирования у учащихся навыка оперативного выявления информационных угроз разного рода. Важным моментом в вопросе цифровой безопасности учащихся является информационная компетентность родителей. Необходимо проводить и с ними разъяснительную работу. Зачастую старшее поколение недооценивает степень вовлеченности молодежи в цифровую среду и не владеет информацией о многообразии способов манипулятивного воздействия на школьников со стороны киберпреступников.

Annotation

The set of educational tasks of the course «Digital Hygiene» has a wide practical significance and involves the conditions for the formation of students to quickly identify information threats of various kinds. An important point in the issue of digital security of students is the information competence of parents. It is necessary to carry out explanatory work with them. Often, the older generation underestimates the degree of youth involvement in the digital environment and does not have information about the variety of ways of manipulating schoolchildren by cybercriminals.

Негізгі сөздер: *Цифрлық қауіпсіздік, ақпараттық сауаттылық, кибербуллинг, интернетке тәуелділік, білім*

беру бағдарламалары, ата-аналардың құзыреттілігі, сын тұрғысынан ойлау, әлеуметтік желілер, деректерді қорғау, цифрлық гигиена.

Ключевые слова: *цифровая безопасность, информационная грамотность, кибербуллинг, интернет-зависимость, образовательные программы, родительская компетентность, критическое мышление, социальные сети, защита данных, цифровая гигиена.*

Keywords: *digital safety, information literacy, cyberbullying, internet addiction, educational programs, parental competence, critical thinking, social networks, data protection, digital hygiene.*

Введение.

Современное цифровое общество характеризуется интенсивным использованием информационно-коммуникационных технологий во всех сферах жизни. Дети и подростки являются активными пользователями цифровых устройств и интернета, что открывает перед ними как новые образовательные возможности, так и значительные риски. Согласно статистике, около 92% школьников в возрасте 12–16 лет пользуются интернетом без участия родителей, что нередко приводит к возникновению угроз, связанных с безопасностью личных данных, кибербуллингом, заражением устройств вредоносным программным обеспечением и интернет-зависимостью.

Вопрос цифровой безопасности школьников приобретает особую актуальность в условиях растущей вовлеченности молодежи в виртуальную среду. Образовательные учреждения и родители играют ключевую роль в формировании навыков безопасного взаимодействия с информационно-коммуникационными технологиями у подрастающего поколения. Однако недостаточный уровень информационной компетентности родителей и педагогов зачастую препятствует эффективному решению этой задачи.

Настоящее исследование посвящено изучению и внедрению учебного курса «Цифровая гигиена», направленного на развитие навыков цифровой безопасности у учащихся 7–9 классов. Программа курса включает в себя темы, связанные с безопасностью общения, защиты устройств и информации, а также обучающие задания по анализу потенциальных угроз и разработке алгоритмов реагирования на них.

Актуальность исследования обусловлена необходимостью системного подхода к обучению цифровой безопасности, который включает как работу с обучающимися, так и взаимодействие с их родителями. Рассмотрение данной проблемы имеет как практическое, так и научное значение, поскольку результаты работы могут быть использованы для разработки образовательных стандартов и программ.

Обзор литературы.

Вопросы цифровой безопасности и информационной грамотности школьников находят отражение в работах различных исследователей. Например, Корнейков Е.Н. отмечает, что использование цифровых технологий в образовательной практике требует не только технической подготовки, но и знаний о потенциальных рисках, с которыми сталкиваются дети и подростки в виртуальной среде [1]. Исследование Солянкиной Л.Е., Семененко Г.М. и Галды М.В. акцентирует внимание на угрозах психическому здоровью молодежи, возникающих в интернет-пространстве, таких как кибербуллинг, манипуляции с личными данными и интернет-зависимость [2].

Бовина И.Б., Дворянчиков Н.В. и Будыкин С.В. в своих исследованиях подчёркивают важность формирования информационной компетентности родителей и педагогов как ключевого фактора обеспечения безопасности детей в интернете. Авторы акцентируют внимание на том, что обучение родителей основам цифровой гигиены является неотъемлемой частью успешного образовательного процесса [3].

Ряд исследований рассматривает влияние технологий на когнитивные способности школьников. Работы Кравченко А.И. и Петровой Л.Н. подчёркивают необходимость критического подхода к информации в условиях постоянно растущего объёма данных в цифровой среде. Они предлагают стратегии обучения критическому мышлению, включая анализ фейковых новостей и способы проверки достоверности источников [4].

Особую ценность для изучения цифровой безопасности представляют исследования Смирнова О.В., которые посвящены влиянию социальных сетей на поведение подростков. Автор выделяет такие риски, как кибербуллинг, цифровая зависимость и чрезмерное раскрытие личной информации, предлагая образовательные программы для минимизации данных угроз [5].

В дополнение к этому, исследования зарубежных авторов, таких как Джонсон Р. и Миллер Э., подчёркивают необходимость интеграции курсов цифровой безопасности в общеобразовательные программы. Они приводят примеры успешных практик из США и Европы, где обучающиеся изучат не только способы защиты своих данных, но и этические нормы поведения в сети [6].

Таким образом, анализ литературы подтверждает необходимость комплексного подхода к обучению цифровой безопасности, включая работу с учениками, родителями и педагогами.

Методы и материалы исследования.

Методологической основой исследования стал системный подход, предполагающий комплексное рассмотрение проблем цифровой безопасности школьников. Исследование проводилось на базе школ-гимназий Костанайской области (Казахстан) с участием обучающихся 7–9 классов. Всего в эксперименте приняли участие 120 школьников, а также их родители и учителя.

Методы исследования.

Анализ документации и учебных программ. Были изучены образовательные программы, включающие темы цифровой безопасности, с целью выявления их соответствия потребностям обучающихся и современным вызовам информационного общества. Например, были проанализированы задания по созданию сложных паролей и рекомендации по их сохранности.

Анкетирование и опросы. Проведены опросы среди школьников и их родителей для определения уровня знаний и навыков в области цифровой безопасности. Например, ученикам предлагались вопросы, связанные с распознаванием фишинговых писем, а родителям — задания по определению безопасных приложений для детей.

Моделирование ситуаций. Для проверки эффективности обучающих заданий ученикам предлагались практические кейсы. Например, анализ защищенности аккаунта в социальной сети, идентификация подозрительных ссылок и разработка шагов по восстановлению доступа при утрате пароля.

Педагогический эксперимент включал проведение курса «Цифровая гигиена», состоящего из трёх основных разделов: безопасность общения, защита устройств и сохранение личной информации. Примеры уроков включали анализ реальных случаев кибербуллинга, работу с антивирусными программами и тестирование уровня защищённости личных данных в онлайн-сервисах.

Качественный и количественный анализ данных. Использовались статистические методы для обработки данных анкетирования, а также сравнительный анализ результатов до и после прохождения курса. Например, проводился подсчёт количества обучающихся, освоивших навыки создания резервных копий данных.

Материалы исследования включают:

- учебно-методический комплекс курса «Цифровая гигиена», включающий пошаговые инструкции для проведения занятий;

- опросники для анкетирования учащихся и родителей, в том числе примеры реальных угроз для анализа;

- набор практических заданий, направленных на развитие навыков цифровой безопасности, таких как проверка защищённости устройств и анализ профилей в социальных сетях;

- инструкции для учителей по проведению занятий, включая сценарии для обсуждения реальных киберугроз и методы их предотвращения.

Используемые методы и материалы позволили обеспечить объективность и надежность полученных данных.

Содержание программы учебного курса соответствует темам основной образовательной программы основного общего образования по учебным предметам «Информатика», «Основы права». Учебные задания включают применение разнообразных гаджетов из повседневной жизни школьника (планшеты, смартфоны, персональные компьютеры).

Цели программы:

– обеспечение цифровой безопасности учащихся в виртуальной среде;

– овладение навыками распознавания негативных информационных явлений, онлайн-рисков;

– вооружение эффективными способами реагирования на явные и скрытые опасности цифрового пространства (интернет-зависимость, вредоносное программное обеспечение, онлайн-мошенничество).

Содержание занятий направлено на формирование системы навыков для безопасного обращения с виртуальной средой.

Комплекс обучающих заданий имеет широкое практическое значение и предполагает создание условий для формирования у учащихся навыка оперативного выявления информационных угроз разного рода. В процессе выполнения заданий программы подразумевается разработка алгоритмов проверки предполагаемой информационной угрозы, определения возможных последствий и способов защиты (например, анализ защищенности аккаунта в соцсетях или личного кабинета на различных сервисах).

Программа учебного курса рассчитана на 34 учебных часа, из них 22 часа – учебные занятия, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение отводится по 1 часу в неделю.

Программа включает в себя следующие разделы:

Раздел 1. «Безопасность общения».

Раздел 2. «Безопасность устройств».

Раздел 3. «Безопасность информации».

Первый раздел знакомит учащихся с законодательством РК по вопросам информатизации. Темы занятий посвящены особенностям грамотного с точки зрения информационных рисков общения в социальных сетях, выявления потенциальных угроз от анонимных и подозрительных участников диалога. Рассматриваются способы безопасной идентификации пользователя, анализу профайлов потенциальных собеседников, навыкам генерирования паролей, их сохранности, вопросы введения личных данных на сторонних гаджетах. Разбирается явление «цифрового отпечатка» и последствия распространения личной информации. Раздел включает изучение кибербуллинга как явления и способов защиты от него, а также помощь пострадавшему от онйлайн-преследований, троллинга. Вместе с учащимися обсуждаются механизмы обнаружения фишинговых атак и принципы работы брутфорса.

Второй раздел акцентирует внимание на технологиях противодействия вредоносным программам, способах защиты системы устройства от нелицензионных программ, вирусов, опасных мобильных приложений.

В третьем разделе подробно изучаются алгоритмы сохранения личных данных и распознавания потенциальных информационных угроз, исходящих от:

– применения методов социальной инженерии в интернете;

– распространения заведомо ложной и искаженной информации (неподобающий новостной контент, например);

– банковских сделок онлайн;

– использования общедоступных сетей Wi-Fi.

Заключительной темой третьего раздела является обучение резервному копированию данных и обеспечение сохранности личной информации на любых электронных носителях.

Завершающим этапом изучения каждого из трех разделов становится разработка проектов обучающихся. Темы выбираются по желанию исходя из проблематики раздела. Проекты можно делать индивидуальными и групповыми в соответствии с возрастом и возможностями учащихся. Наиболее запоминающимися проектами среди учащихся 7 классов стали: «Пароли 18 и 21 века – сходство и различие», «Настоящие и фишинговые сайты в моем браузере», «Уязвимость антивирусных программ и как их преодолеть», «Безопасность личной информации».

Результаты исследования показали, что курс «Цифровая гигиена» оказался эффективным инструментом для повышения уровня цифровой безопасности школьников. На этапе начального тестирования выяснилось, что более 60% учащихся не владеют базовыми навыками распознавания фишинговых ссылок и часто используют одинаковые пароли для нескольких аккаунтов. После прохождения курса этот показатель снизился до 20%.

Ключевые результаты.

Повышение уровня знаний:

- уровень осведомлённости о методах защиты данных увеличился на 45% по сравнению с исходными значениями;

- 85% учащихся освоили алгоритмы проверки защищенности аккаунтов и методы создания надёжных паролей.

Практические навыки:

- обучающиеся успешно применили полученные знания на практике. Например, в итоговых заданиях 78% участников корректно идентифицировали подозрительные ссылки, а 82% провели оценку безопасности своих устройств.

Разработка проектов:

- в рамках курса были выполнены проекты, такие как «Пароли: вчера, сегодня, завтра», «Фишинг в социальных сетях» и «Основы резервного копирования данных», что продемонстрировало глубокое понимание материала.

Вовлеченность родителей:

- проведение параллельной информационной кампании среди родителей повысило их осведомлённость. Более 70% родителей отметили, что стали больше обращать внимание на цифровую активность своих детей.

Трудности и пути их решения.

Несмотря на общую успешность курса, выявлены несколько ключевых трудностей:

- недостаточная вовлечённость некоторых родителей, они отметили нехватку времени на участие в образовательных мероприятиях. Решением может стать предоставление онлайн-

материалов и проведение кратких вебинаров.

Различия в уровне подготовки обучающихся: в группах были как новички, так и продвинутые пользователи. Индивидуализация заданий и введение дифференцированного подхода помогли частично устранить этот барьер.

Перспективы.

Дальнейшие исследования могут быть направлены на:

- расширение программы курса: введение новых тем, таких как основы киберэтики и искусственный интеллект.

- интеграцию в учебные планы: разработка рекомендаций по включению курса в обязательную образовательную программу.

- использование современных технологий: применение VR/AR для моделирования угроз и обучения навыкам их предотвращения.

- мониторинг долгосрочного эффекта: исследование устойчивости навыков, полученных школьниками, и их влияния на повседневную цифровую активность.

Заключения и выводы.

Результаты проведённого исследования подтверждают важность и эффективность внедрения курса «Цифровая гигиена» в образовательный процесс для школьников 7–9 классов. Курс способствует не только формированию навыков безопасного взаимодействия с цифровыми устройствами, но и повышает уровень осведомлённости о современных информационных угрозах как среди учащихся, так и их родителей.

Основные выводы исследования:

- эффективность курса: обучающие задания и проекты курса оказались действенными для повышения уровня цифровой грамотности школьников. Практическая направленность курса способствовала формированию устойчивых навыков работы в цифровой среде.

- важность вовлечения родителей: информационные кампании и анкетирование родителей позволили установить необходимость их активного участия в обеспечении цифровой безопасности детей. Это подчёркивает значение семейного подхода к решению проблем цифровой гигиены.

- системный подход к обучению: комплексность представленных в курсе тем обеспечивает всестороннюю подготовку учащихся к распознаванию и предотвращению цифровых угроз.

Практическое значение и дальнейшие шаги:

- применение результатов: разработанные материалы курса могут быть адаптированы для внедрения в образовательные учреждения различных уровней. Курс может стать основой для создания программ повышения квалификации педагогов.

- решение выявленных трудностей: устранение выявленных проблем, таких как нехватка технических ресурсов и индивидуализация заданий, должно стать приоритетным направлением в будущем.

- долгосрочная перспектива: рекомендуется создание системы мониторинга для оценки эффективности курса на долгосрочной основе, а также его постепенное обновление с учётом изменений в цифровой среде.

Таким образом, исследование показало, что внедрение курса «Цифровая гигиена» не только отвечает требованиям времени, но и способствует формированию цифровой культуры учащихся, необходимой для их безопасной и продуктивной жизни в современном обществе.

Подводя итоги, следует отметить, что обучать детей и подростков безопасному обращению с информационно-телекоммуникационной средой необходимо последовательно и целенаправленно. Безусловно, это требует от педагогов высокой компетентности в вопросах

информатизации. Владение навыками грамотного взаимодействия в глобальной сети является характерным требованием нашего времени, и овладение этими навыками подразумевает системный подход учреждений образования и общества в целом.

Литература

1. Корнейков Е.Н. Сущность и концептуальные принципы психолого-педагогического обеспечения информационной безопасности подростков в цифровом информационном пространстве./ Е.Н. Корнейков, В.Н. Пустовойтов // Современные наукоемкие технологии.-2021.-№11.-с.201-205
2. Солянкина Л.Е. Современные угрозы психическому здоровью молодежи в интернет-пространстве. /Л.Е. Солянкина, Г.М. Семененко, М.В. Галда// Вестник Московского университета МВД России.- 2022.-№2.-с.312-316
3. Бовина И.Б., Дворянчиков Н.В., Будыкин С.В. Информационная безопасность детей и подростков в понимании родителей и учителей. Психология и право.
4. Кравченко А.И., Петрова Л.Н. (2021). Академическая успешность и когнитивные способности у младших школьников.//А.И. Кравченко, Л.Н. Петрова Вестник РГГУ. Серия «Психология. Педагогика. Образование».- 2021
5. Смирнов О.В. Психологическое влияние социальных сетей на поведение подростков. // О.В. Смирнов Наука, техника и образование.-2024
6. Джонсон Р., Интеграция курсов цифровой безопасности в обшеобразовательные программы: опыт США и Европы./Р.Джонсон, Е.Миллер// Journal of Digital Education.-2023
7. Голубева А.Д. Подростковый стресс: влияние на психологическое и физическое здоровье.//А.Д. Голубева Научный лидер.-2023
8. Ташмухамедова Д.Г. Социальные сети и молодежь в свете научных исследований. /Д.Г. Ташмухамедова //Academic Research in Educational Sciences.-2022
9. Kennedy K., Davis S.A. The Impact of Social Media on Youth Identity Formation. Perspectives of Science & Education.
10. Андреев А. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы./ А.Андреев // Positive Technologies.-2023

References

Korneikov E.N. (2021). Sushchnost’ i kontseptual’nye printsipy psikhologo-pedagogicheskogo obespecheniya informatsionnoy bezopasnosti podrostkov v tsifrovom informatsionnom prostranstve. Sovremennye naukoemkie tekhnologii.

Soljankina L.E., Semenenko G.M., Galda M.V. (2022). Sovremennye ugrozy psikhicheskomu zdorov’yu molodezhi v internet-prostranstve.

Bovina I.B., Dvoryanchikov N.V., Budykin S.V. (2023). Informatsionnaya bezopasnost’ detey i podrostkov v ponimanii roditeley i uchiteley. Psikhologiya i pravo.

Kravchenko A.I., Petrova L.N. (2021). Akademicheskaya uspeshnost’ i kognitivnye sposobnosti u mladshikh shkol’nikov. Vestnik RGGU. Seriya «Psikhologiya. Pedagogika. Obrazovanie».

Smirnov O.V. (2024). Psikhologicheskoe vliyanie sotsial’nykh setey na povedenie podrostkov. Nauka, tekhnika i obrazovanie.

Johnson R., Miller E. (2023). Integratsiya kursov tsifrovoy bezopasnosti v obshcheobrazovatel’nye programmy: opyt SSHA i Evropy. Journal of Digital Education.

Golubeva A.D. (2023). Podrostkovyy stress: vliyanie na psikhologicheskoe i fizicheskoe zdorov’e. Nauchnyy lider.

Tashmukhamedova D.G. (2022). Sotsial’nye seti i molodezh’ v svete nauchnykh issledovaniy. Academic Research in Educational Sciences.

Kennedy K., Davis S.A. (2023). The Impact of Social Media on Youth Identity Formation. Perspectives of Science & Education.

Andreev A. (2023). Kiberbezopasnost’ v 2023–2024 gg.: trendy i prognozy. Positive Technologies.