Мир науки. Педагогика и психология / World of Science. Pedagogy and psychology https://mir-nauki.com
2025, Том 13, № 1 / 2025, Vol. 13, Iss. 1 https://mir-nauki.com/issue-1-2025.html
URL статьи: https://mir-nauki.com/PDF/22PDMN125.pdf
5.8.7. Методология и технология профессионального образования (педагогические науки)

Ссылка для цитирования этой статьи:
Тарасова, А. А. Модель формирования кибербезопасного поведения будущих программистов в образовательном процессе колледжа / А. А. Тарасова // Мир науки. Педагогика и психология. — 2025. — Т. 13. — № 1. — URL: https://mir-nauki.com/PDF/22PDMN125.pdf

For citation:
Tarasova A.A. Model of formation of cybersecurity behavior of future programmers in the educational process of the college. *World of Science. Pedagogy and psychology*. 2025;13(1): 22PDMN125. Available at: https://mir-nauki.com/PDF/22PDMN125.pdf. (In Russ., abstract in Eng.)

УДК 377

Тарасова Анна Александровна
ФГБОУ ВО «Пензенский государственный университет», Пенза, Россия
Педагогический институт им. В.Г. Белинского, кафедра «Педагогика и психология», Аспирант
E-mail: tarasova.aa@pnzgu.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=1024078
ORCID: https://orcid.org/0000-0003-4002-7921

Модель формирования кибербезопасного поведения будущих программистов в образовательном процессе колледжа

Аннотация. В статье актуализируется важность проблемы формирования культуры кибербезопасного поведения обучающихся в системе среднего специального образования. В современных условиях цифровизации социальной среды важную роль играет уровень культуры кибербезопасности личности. Ее формирование начинается с интеграции цифровых устройств в жизнь ребенка. Современный образовательный процесс колледжа предполагает коммуникацию «педагог-обучающийся» посредством информационных технологий и электронной информационно-образовательной среды, что увеличивает эффективность образовательного процесса. Однако, у этого фактора есть такие негативные стороны, как влияние киберугроз на несформированное психологическое здоровье личности. Крайне важно становится сформировать навыки и опыт кибербезопасного поведения у обучающегося для самостоятельной защиты от информационных угроз. Особое внимание следует обратить на такую категорию специалистов, как будущие программисты, для которых кибербезопасное поведение является не только полезным личным качеством, но и обязательным направлением для профессиональной деятельности. Сложность формирования культуры кибербезопасного поведения заключается в отсутствии нормативной регламентации взаимодействия обучающихся в информационно-коммуникационной среде, частотой возникновения новых киберугроз и отсутствием практической подготовки по данному направлению деятельности.

В статье предложена педагогическая модель процесса формирования культуры кибербезопасного поведения будущих программистов в образовательном процессе колледжа. Изложено краткое структурное описание модели и ее компонентов, а также критерии и показатели оценки уровней сформированности культуры кибербезопасного поведения будущих программистов.

Ключевые слова: будущие программисты; образовательный процесс; кибербезопасность; модель формирования культуры кибербезопасного поведения

Введение

Развитие информационных технологий и киберпространства оказывают значительное влияние на становление личности человека, его социальную и культурную жизнь, а также на его восприятие окружающего мира. Знакомство с элементами цифрового мира происходит еще на начальной ступени образования. В современном мире процесс обучения неразрывно связан с использованием информационно-коммуникационных технологий, ведь благодаря им доступен широкий набор инструментов, помогающий легче и качественней усваивать необходимую информацию, получать обратную связь, осваивать знания людям с ограниченными возможностями.

Подчеркивают актуальность формирования культуры кибербезопасного поведения возрастные особенности обучающихся колледжа, их повышенная активность в интернет-пространстве и недостаточно сформированное психологическо-социальное сознание.

В настоящее время проблемам культуры кибербезопасного поведения уделяется особое внимание в научных трудах и литературе. О.А. Веденеева, М.А. Гарипов, Н.Я. Сайгушев рассматривают проблему формирования культуры кибербезопасности обучающихся в профессиональной подготовке и вопрос актуализации информационной грамотности студентов [1, 2]. Н.И. Саттарова определяет понятие «информационная безопасность личности» и рассматривает вопрос формирование культуры безопасности обучающихся в информационном пространстве [3]. А.А. Воскрекасенко, А.А. Киреева, Т.Т. Щелина рассматривают процесс формирования культуры кибербезопасного поведения обучающихся как педагогическую проблему [4].

Анализ научной литературы показывает, что в настоящий момент точного общепринятого определения понятия культуры кибербезопасного поведения обучающихся не выявлено, однако позиции многих авторов сходятся на том, что навыки и опыт, получаемые в процессе формирования культуры кибербезопасного поведения играют важнейшую роль в становлении личности и ее психологически-социальной модели поведения [5, 6].

В.П. Поляков считает, что информационное взаимодействие обучающегося, обучающего с интерактивным информационным ресурсом сопряжено с рядом возможных негативных последствий для личности, в том числе связанных с воздействием агрессивной или неэтичной информации, оскорбляющей моральные ценности и чувства пользователя [7].

Целью исследования является разработка модели формирования культуры кибербезопасного поведения будущих программистов в образовательном процессе колледжа. Личность будущего программиста должна быть сформирована с готовностью противостоять киберугрозам, уметь предвидеть негативные последствия деструктивного поведения в цифровой среде, а также применять навыки и опыт кибербезпасного поведения в своей профессиональной деятельности, которая касательно связана с защитой данных. Для этого необходимо выявить подходы, методы и принципы, при помощи которых в образовательном процессе колледжа является возможным сформировать культуру кибербезопасного поведения будущих программистов.

Методы и материалы

Областью настоящего исследования выступают воспитательные и образовательные направления деятельности колледжа, в реализации которых будет формироваться культура кибербезопасного поведения будущих программистов. К ним можно отнести взаимодействие педагогов и обучающихся посредством проведения кураторских часов, постановки различных

симуляций жизненных ситуаций, в которых требуется применения навыков киберзащиты, а также взаимодействие с родителями студентов и сторонними организациями.

Методологической основой данного исследования послужили научные статьи и монографии, посвященные исследованию проблеме формирования культуры кибербезопасного поведения. Также источником анализируемого материала послужил федеральный государственный образовательный стандарт специальности 09.02.07 «Информационные системы и программирование», в котором показано, что профессиональная область деятельности будущих программистов напрямую связана с защитой данных с использованием различных технологий.

Существует значительное количество киберугроз, которым могут быть подвергнут обучающийся. Киберпреступления, кибербуллинг, агрессивное информационное пространство, интернет-зависимости – этим и другим факторам обучающиеся колледжа подвергаются ежедневно. Сформированные умения и навыки кибербезопасного поведения у будущих программистов могут помочь не только обезопасить себя лично, но и осуществлять защиту при реализации своей профессиональной деятельности.

Проведенный в ходе исследования вышеперечисленных аспектов показал значимую роль культуры кибербезопасного поведения обучающихся, которая формируется с целью приобретения будущими программистами интегральных качеств личности, которым присущи навыки защиты информации с целью их применения в профессиональной сфере. Возможности человека в информационной среде достаточно расширены, но в то же время цифровые технологии несут риски в ситуациях киберпреступлений. Общественность уделяет особое внимание обеспечению кибербезопасности личности, особенно в период формирования ее психологического развития, прививая ей такое свойство, как «цифровая грамотность», которое также является составляющей культуры кибербезопасного поведения.

Также были выявлены такие негативные стороны влияния киберпространства, как проблемы со здоровьем (заболевания органов зрения, болезни сердечно-сосудистой системы, обусловленные гиподинамией, психологические истощения и расстройства различной этиологии, нарушение опорно-двигательного аппарата и т. д.), этические проблемы (переоценка нравственных норм, перенос образцов поведения из виртуальной действительности в реальную), сложности в межличностном взаимодействии и такие интеллектуальные проблемы, как изменение процессов мышления за счет формирования привычки «поверхностного чтения» [8].

Культура информационной безопасности человека должна быть заключена в невозможности нанесения ему вреда как индивидууму или личности, социальная деятельность которой (личности) в большинстве своем основывается на «переваривании» полученной информации, на взаимодействиях с другими индивидуумами [9]. Это достигается за счет сформированных профессиональных навыков и личного устойчивого поведения, а также приобретенных умений, знаний и опыта работы с киберпространством, что и будет формировать культуру кибербезопасного поведения будущих программистов.

Результаты и обсуждение

В целях повышения эффективности образовательной деятельности, ориентированной на создание условия для формирования культуры кибербезопасности обучающихся, нами была разработана модель формирования культуры кибербезопасного поведения будущих программистов в образовательном процессе колледжа.

Модель включает в себя следующие блоки: целевой, методологический функциональный, содержательный и оценочный.

Целевой блок включает в себя цели, задачи и подходы, которые направлены на формирование культуры кибербезопасного поведения, навыков и знаний будущих программистов в образовательном процессе колледжа.

Методологический блок представляет собой подходы и принципы, с помощью которых у будущих программистов будут формироваться опыт и навыки кибербезопасного поведения. Он включает в себя:

- системный подход, в основе которого лежит применения целостного комплекса взаимосвязанных элементов культуры кибербезопасного поведения, а именно вовлечение всех участников образовательной и воспитательной деятельности, применение единой системы образовательных элементов, целостное рассмотрение процесса формирования культуры кибербезопасного поведения;
- компетентностный подход, заключающийся в развитии у обучающихся;
- способности самостоятельно решать проблемы в сфере информационного пространства и профессиональных видах деятельности на основе использования социального опыта, элементом которого будет являться собственный опыт студентов;
- личностно-ориентированный подход по концепции В.В. Серикова, в основе которого заложен ситуационный принцип и такие понятия, как личностный опыт, личностно-ориентированная или личностно-утверждающая педагогическая ситуация [10].

Данные подходы предполагают следующие принципы: целостность (единство взаимодействия внешнего взаимодействия педагогов и внутренней активности обучающегося в воспитательном и образовательном процессе), комплексность (учет индивидуальных и возрастных особенностей обучающихся при выборе способов формирования кибербезопасного поведения), коммуникативность (проведение тренингов и мастер-классов по получению навыков работы в команде и формированию поведения при общении в информационно-коммуникационной среде), профессиональная мобильность (формирование готовности обучающегося к получению новых знаний и их применения на практике), самореализация (побуждение умственных и творческих способностей для использования полученных знаний по кибербезопасности на практическом опыте), субъективность (реализация образовательной и воспитательной системы, в которой каждый ее участник становится полноправным субъектом жизнедеятельном).

Функциональный блок определяется этапами и направлениями организации образовательного и воспитательного процесса колледжа по формированию культуры кибербезопасного поведения будущих программистов, а также созданием определенных условий, благодаря которым опыт и навыки кибербезопасного поведения обучающихся будут получены наиболее эффективным образом.

Содержательный блок включает следующие формы, методы и средства:

- аудиторные (лекции, практические занятия, зачеты, экзамены) и внеаудиторные (тренинги, кураторские часы, стажировки, мастер-классы, беседы, круглые столы) формы;
- традиционные (беседы, рассказы, демонстрации и др.) и интерактивные (решение ситуационных задач, ролевые игры, кейс-методы и др.) методы;
- наглядные (графики, видеоматериалы, презентации, графические изображения и др.), дидактические (учебно-методические комплексы, рабочие программы дисциплин и др.) и информационно-коммуникационные (приложение

образовательного учреждения, электронная информационно-образовательная среда, мессенджеры и др.).

Оценочный блок определяется критериями сформированности культуры кибербезопасного поведения (ценностно-мотивационный, когнитивный, информационно-коммуникационный и регулятивно-рефлексивный) и показателями (положительное отношение к профессиональному развитию как будущего программиста, сформированность личного понимания значения кибербезопасности личности, безопасная передача информации при различных форм коммуникации в информационном пространстве, активная жизненная позиция по отношению к защите общества от киберугроз).

Ценностно-мотивационный критерий определяется уровнем сформированного отношения к профессиональному и личностному развитию в информационной сфере, установке на профессиональное саморазвитие как программиста, отношения к будущей профессиональной деятельности, желание работать по специальности.

Показателями когнитивного критерия являются уровень сформированности знаний правовых норм, регламентирующих информационную безопасность в личной профессиональной сфере деятельности, способов решения задач, позволяющих обеспечить защиту от киберугроз, и представлений о новых киберугрозах с внешней стороны, представляющих опасность как для профессиональной деятельности, так и для личности

Информационно-коммуникационный критерий отражает уровень сформированности профессиональных умений и навыков кибербезопасного общения при помощи различных форм коммуникаций (электронная почта, блог, социальные сети и другие). Также показателем данного критерия является умение проявить мобильную реакцию на информационные угрозы и кибербезопасные ситуации.

Регулятивно-рефлексивный критерий определяется уровнем сформированности умения контролировать свое поведение в информационно - коммуникационной среде, осознавая ответственность за его отклонение от норм, а также навыками саморегуляции и рефлексии своей профессиональной деятельности.

Культура кибербезопасного поведения будущих программистов колледжа может оцениваться по следующим уровням:

- базовый, равнодушная оценка происходящих событий в социуме, отсутствие заинтересованности в приобретении знаний по информационной защите личности, незаинтересованность в профессиональном развитии как программиста, отсутствие желания саморазвития.
- оптимальный, получение знаний, опыта и навыков кибербезопасного поведения, позитивное отношение к профессиональному развитию, желание работать по будущей профессии, осуществление кибербезопасного общения с различными формами коммуникации.
- профессиональный, применение на практике способов решения задач, обеспечивающих личную кибербезопасность и защиту информации, используемых при проектировании баз данных и другой профессиональной деятельности, саморегуляция поведения в информационно-коммуникационной среде, высокий интерес к актуальным киберугрозам и способам защиты от них.

Результатом реализации данной модели будет сформированная культура кибербезопасного поведения программиста в образовательном процессе колледжа на достаточном уровне.

Заключение

При учете всех вышеописанных компонентов разработанной модели формирования культуры кибербезопасного поведения будущих программистов можно прогнозировать повышения уровня навыков и опыта кибербезопасности у обучающихся, формируемых в образовательной деятельности, а также повышение эффективности усвоения знаний, приобретаемых будущими программистами в образовательном и воспитательном процессе колледжа.

ЛИТЕРАТУРА

1. Сайгушев, Н.Я., Веденеева, О.А., Гарипов, М.А. К постановке проблемы формирования культуры кибербезопасности обучающихся в процессе профессиональной подготовки / Н.Я. Сайгушев, О.А. Веденеева, М.А. Гарипов // Проблемы современного педагогического образования. – 2021. – № 73-1. – С. 322-324.
2. Сайгушев, Н.Я., Веденеева, О.А., Гарипов, М.А. Актуализация информационной грамотности студентов в процессе профессиональной подготовки / Н.Я. Сайгушев, О.А. Веденеева, М.А. Гарипов // Мир науки, культуры, образования. – 2021. – № 4 (89). – С. 77-80
3. Саттарова, Н.И. О формировании культуры безопасности обучающихся в информационном пространстве / Н.И. Саттарова // Проблемы современного педагогического образования. – 2018. – № 58-4 – С. 242-244
4. Воскрекасенко, О.А., Киреева, А.А., Щелина, Т.Т. Формирование культуры кибербезопасности в системе профессиональной подготовки обучающихся колледжа как педагогическая проблема / О.А. Воскрекасенко, А.А. Киреева, Т.Т. Щелина // Современные наукоемкие технологии. – 2022. – № 10-1. – С. 125-129
5. Сосян, К.Г. Безопасность сознания школьников в киберпространстве / К.Г. Сосян // Вестник Московского информационно-технологического университета – Московского архитектурно-строительного института. – 2024. – № 1. – С. 107-110
6. Сосян, К.Г., Земш, М.Б. Риски и преимущества цифровой социализации / К.Г. Сосян, М.Б. Земш // Вестник Московского информационно-технологического университета – Московского архитектурно-строительного института. – 2023. – № 1. – С. 123-127
7. Поляков, В.П., Романенко, Ю.А. Педагогическое обеспечение информационной безопасности личности в цифровой информационно-образовательной среде. / В.П. Поляков, Ю.А. Романенко // Наука о человеке: гуманитарные исследования. — 2020. — №1. — с. 43-47.
8. Абаева, С.М., Беляева В.Г., Копылов, С.А., Тенитилова, К.С. Проблема формирования культуры информационной безопасности при изучении предмета «Основы безопасности жизнедеятельности» / С.М. Абаева, В.Г. Беляева, С.А. Копылов, К.С. Тенитилова // Международный научно-исследовательский журнал. – 2023. – № 4 (130). – С. 1-4
9. Ерина, Ю.С., Кокаева, И.Ю. Формирование культуры информационной безопасности у студентов - будущих учителей - в процессе профессиональной подготовки / Ю.С. Ерина, И.Ю. Кокаева // Вестник Кемеровского государственного университета культуры и искусств. – 2017. – № 41. – С. 186-194
10. Мусина, Л.М. Личностно-ориентированные подходы в обучении / Л.М. Мусина // Педагогическая наука и практика. – 2021. – № 2 (32). – С. 37-42

Tarasova Anna Alexandrovna
Penza state University, Penza, Russia
E-mail: tarasova.aa@pnzgu.ru
RSCI: https://elibrary.ru/author_profile.asp?id=1024078
ORCID: https://orcid.org/0000-0003-4002-7921

Model of formation of cybersecurity behavior of future programmers in the educational process of the college

Abstract. The article actualizes the importance of the problem of forming the culture of cybersecurity behavior of students in the system of secondary specialized education. In modern conditions of digitalization of the social environment, the level of personal cybersecurity culture plays an important role. Its formation begins with the integration of digital devices in the life of a child. The modern educational process of the college involves communication "teacher-student" through information technologies and electronic information and educational environment, which increases the effectiveness of the educational process. However, this factor has such negative sides as the impact of cyber threats on the unformed psychological health of the individual. It is extremely important to develop skills and experience of cybersecurity behavior in the student for self-protection from information threats. Special attention should be paid to such a category of specialists as future programmers, for whom cybersecurity behavior is not only a useful personal quality, but also a mandatory direction for professional activity. The complexity of forming the culture of cybersecurity behavior lies in the lack of normative regulation of students' interaction in the information and communication environment, the frequency of new cyber threats and the lack of practical training in this area of activity.

The article proposes a pedagogical model of the process of forming the culture of cybersecurity behavior of future programmers in the educational process of the college. A brief structural description of the model and its components, as well as criteria and indicators for assessing the levels of formation of the culture of cybersecurity behavior of future programmers.

Keywords: future programmers; educational process; cybersecurity; model of formation of cybersecurity behavior culture