профессионального мастерства, разработка этических нормативов; создание этических структур – различных должностей и комитетов, с помощью которых образовательные организации могут стимулировать соответствующее моральным принципам поведение сотрудников (комитетов по этике, уполномоченных по этике и т. п.); создание «горячих линий» относительно нарушения преподавателями этических норм.

Для эффективного формирования профессионально-педагогической культуры преподавателя военного ВУЗа важно обеспечить методическую подготовку педагогов к этому процессу, то есть усвоение ими знаний, умений и навыков, необходимых для непосредственного осуществления этого процесса.

Выводы. Педагогическая культура преподавателя – это личностное образование, интегрированная система педагогических ценностей, в основу которых положены духовные ценности, что является достаточно устойчивой основой, согласно которой преподаватель соотносит свою жизнь и профессионально-педагогическую деятельность. От уровня сформированности педагогической культуры преподавателя будет зависеть результативность его деятельности, профессиональный уровень и степень самореализации его личности. Осознание преподавателем особенностей каждого этапа профессионального становления, умелое решение задач, определение проблем и их решение является основой для достижения максимальных результатов во время профессиональной педагогической деятельности.

1. Асриев С.А., Шилова С.В., Перелогов И.О., Стрижков А.П. Педагогическая культура преподавателя как условие и показатель качества образовательного процесса // Актуальные проблемы профессионально-прикладной физической культуры и спорта. – 2020. – С. 7-10.
2. Караванов А.А., Устинов И.Ю. Исследование феномена профессионально-педагогической культуры преподавателя военного ВУЗа: история и современность // Научное обозрение. Педагогические науки. – 2017. – № 4. – С. 62-79.
3. Кизянов В.П. Формирование профессионально-педагогической культуры преподавателей военного ВУЗа по применению информационно-коммуникативных технологий // Альманах Пермского военного института войск национальной гвардии. – 2021. – № 3 (3). – С. 78-84.
4. Кириллова Т.В. К вопросу о содержании понятия профессиональной культуры преподавателей образовательных организаций // Вопросы педагогики. – 2021. – № 1-1. – С. 106-109.
5. Костенко П.И., Панасенко Ю.А. Профессионально - педагогическая культура преподавателя военного ВУЗа: сущность, структура, содержание, особенности и условия развития // Вестник Таджикского национального университета. – 2018. – № 1. – С. 208-214.
6. Толстов А.В. Педагогическая культура преподавателя военных образовательных организаций высшего образования: основные проблемы и тенденции развития // В сборнике: Актуальные вопросы гуманитарных и социально-экономических наук. – 2018. – С. 268-272.

Яновский В.В.¹, Кадеева О.Е.²

Вопросы обучения кибербезопасности в школьном курсе информатики

¹Школа педагогики Дальневосточный федеральный университет

²Департамент теории и практики преподавания математики, информатики,
естественных наук ШП ДВФУ
(Россия, Владивосток)

doi: 10.18411/trnio-01-2022-162

Аннотация

Данная работа посвящена исследованиям, лежащим в области изучения вопросов обучения кибербезопасности в школьном курсе информатики. Описаны различные вопросы о целесообразности изучения данного вопроса в школе и о том, с какого возраста это нужно делать. А также описаны программы обучения кибербезопасности, предложенные некоторыми авторами.

Ключевые слова: кибербезопасность, компьютерная грамотность, защита информации, информационное воздействие, информатика, обучение.

Abstract

This work is devoted to research underlying the study of cybersecurity education in the school computer science course. Various questions are described about the advisability of studying this issue in school and about the age at which it should be done. It also describes cybersecurity training programs offered by some authors.

Keywords: cybersecurity, computer literacy, information security, information impact, informatics, training.

В последние годы угрозы информационной безопасности детей стали особенно актуальны в связи с массовым распространением смартфонов и компьютеров, а также доступностью ресурсов сети Интернет. Компьютерная грамотность детей позволяет им уже с раннего возраста использовать компьютерные программы, позволяющие обходить родительские ограничения на просмотр запрещенных видеофайлов или фотографий. В результате детям становится доступна информация, которая может негативно влиять на их психическое развитие, подрывая отношение к семейным ценностям, отношению к собственной жизни и здоровью, а также формирующая ложные идеалы, следуя которым ребенок может стать на путь совершения преступлений.

В России принят ряд нормативных правовых актов, которые регулируют деятельность в сфере защиты детей от подобной информации, основными из которых являются Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [1], а также Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [2]. В данных документах определено, что доступ детей к информации должен осуществляться в соответствии с возрастными ограничениями, а также должны быть минимизированы риски использования информации, которая может нанести вред жизни или здоровью ребенка.

В настоящее время вопросам обучения кибербезопасности в школе уделяется недостаточно внимания. Например, в курсе информатики базовой школы только один-два часа посвящаются угрозам работы с Интернетом. При наличии в школе профильных классов акцент делается в зависимости от направления обучения. Так классы с экономическим уклоном изучают правовые нормы защиты информации, классы с гуманитарным профилем изучают этические нормы сетевого общения. В классах технического профиля акцент делается на технических и программных методах защиты информации [3].

Однако, проведенные среди старшеклассников опросы указали на то, что все дети знают, что интернет содержит много угроз, большинство знает о вреде игровой зависимости, однако только небольшое количество детей смогли правильно ответить на третий вопрос, как защитить себя при работе в Интернете.

В доступных источниках информации имеются различные предложения по совершенствованию школьных программ в направлении практических аспектов проведения занятий. Например, Н.Н. Кочемиров [4] в своей публикации «Особенности изучения вопросов информационной безопасности в школьном курсе информатики» критикует учебные программы из-за недостатка практических вопросов, посвященных правилам работы с интернетом. Он предлагает в школе ввести новую содержательную линию [4] «Защита информации и информационная безопасность». При этом изучение вопросов информационной безопасности следует начинать после изучения основ сетевых технологий и системного программного обеспечения. То есть, в более старших классах. При этом основной акцент следует сделать на постановке задачи информационной безопасности в целом, истории развития средств защиты информации, классификации и анализе угроз информационной безопасности, видах мер противодействия угрозам безопасности, а также на определении основных понятий информационной безопасности. В более старших классах предложено изучать технологии защиты данных: симметричные криптосистемы шифрования, тройной стандарт шифрования данных 3-DES, усовершенствованный стандарт

шифрования AES и ассиметричные криптосистемы шифрования – стандарт шифрования RSA, работу функции хеширования и алгоритмы цифровых подписей DSA.

По моему мнению, такой подход не решит основных проблем и является несколько устаревшим. Во-первых, планшетами и смартфонами дети начинают пользоваться уже с первого класса. Именно в этот период у них формируется мировоззрение. Поэтому изучение основ кибербезопасности должно начинаться уже с первого класса, базируясь на примерах мультипликационных героев о недопустимости просмотра информации негативного содержания. Во-вторых, обучение в старших классах технологиям защиты данных должно базироваться не на анализе содержания устаревших алгоритмов шифрования, а на практическом изучении компьютерных программ, которые используют данные алгоритмы для защиты информации. Кроме того, автор статьи несколько заблуждается, выводя защиту информации на первое место. Ведь информационная безопасность более широкое понятие и включает в себя процесс защиты информации.

Ю.И. Богатырева и Е.С. Калугина [3], авторы статьи «Угрозы информационного воздействия на учащихся и методы противодействия им в образовательной организации» предлагают достаточно обоснованно с первого класса вводить уроки медиабезопасности для привития школьникам навыков безопасного и ответственного поведения при использовании информационно-телекоммуникационной среды. Кроме того, предложено проведение внеклассных мероприятий с обучающимися и их родителями (законными представителями) по тематике информационной безопасности. Предложенная тематика достаточно интересна по своему содержанию и направлена на развитие возможностей критического мышления школьников в направлении повышения способности анализировать предоставляемую информацию, сопоставляя её с уже известными типами (недостоверной, непристойной, неэтичной, деструктивной), делать выводы о возможном ее негативном воздействии (причинение вреда жизни и здоровью, влияние на общение со сверстниками) и принимать единственные правильные решения в зависимости от складывающейся ситуации (закрывать страницу, выключить компьютер, позвонить по нужному номеру телефона, сказать взрослым и др.).

Авторы статьи «Методика обучения информационной безопасности старшеклассников: о содержании обучения в школьном курсе информатики» М.И. Бочаров, И.В. Симонова [5] предлагают в процессе обучения старшеклассников рассматривать два уровня базовый и профильный. При этом предложено выделить пять ключевых аспектов информационной безопасности (рисунок 1).

Рисунок 1. Модель обучения информационной безопасности (предложенная Бочаровым М.И.)

Достоинством предложенного подхода является введение в рамках уроков информатики элективных курсов по информационной безопасности, а также проведение

внеурочных экскурсий с посещением специализированных выставок по тематике занятий. В совокупности предложенный подход должен позволить обеспечить духовно-нравственное развитие, воспитание и социализацию школьников.

Недостатком подхода можно считать отсутствие обучения вопросам информационной безопасности в младших классах.

Таким образом, в настоящее время вопросам обучения кибербезопасности в школе уделяется недостаточно внимания, однако работы по совершенствованию образовательного процесса ведутся.

1. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". [Электронный ресурс] – Режим доступа: <http://www.consultant.ru>
2. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] – Режим доступа: www.consultant.ru
3. Богатырева Ю.И., Калугина Е.С. Угрозы информационного воздействия на учащихся и методы противодействия им в образовательной организации [Электронный ресурс] – Режим доступа: <http://rpedagogy.ru/journal/article/822/>
4. Кочемиров Н.Н. Особенности изучения вопросов информационной безопасности в школьном курсе информатики [Электронный ресурс] – Режим доступа: https://урок.рф/library/osobennosti_izucheniya_voprosov_informatcionnoj_bezop_093433.html
5. Бочаров М.И. Методика обучения информационной безопасности старшеклассников: о содержании обучения в школьном курсе информатики / М.И. Бочаров, И.В. Симонова // Пространство и время. – 20014. №3 (17) [Электронный ресурс] – Режим доступа: <https://cyberleninka.ru/article/n/metodika-obucheniya-informatsionnoy-bezopasnosti-starsheklassnikov>

Bashmakova N.I.

Professional training for the judiciary through the prism of the Federal State Educational Standard

*The North Western branch of the Federal State Budget-Funded Educational Institution of Higher Education "The Russian State University of Justice"
(Russia, Saint-Petersburg)*

doi: 10.18411/trnio-01-2022-163

Abstract

The article deals with the problem of professional training for the judiciary. The object of the study is the professional training of specialists for the judiciary in a higher education institution. The subject of the study is the requirements of the Federal State Educational Standards to the professional training of specialists for the judiciary in the context of the new technological order. The purpose of the study is to analyze professional training for the judiciary in the context of the existing federal state educational standards.

Keywords: professional training for the judiciary, higher education institution, requirements, specialists, the Federal State Educational Standard.

Аннотация

Статья посвящена проблеме профессиональной подготовки специалистов для судебной системы. Объектом исследования является профессиональная подготовка специалистов для судебной системы в высшем учебном заведении. Предметом исследования служат требования ФГОС ВПО к профессиональной подготовке специалистов для судебной системы в условиях нового технологического уклада. Цель исследования заключается в том, чтобы проанализировать профессиональную подготовку специалистов для судебной системы в контексте действующих федеральных государственных образовательных стандартов.

Ключевые слова: профессиональная подготовка кадров для судебной системы, высшее учебное заведение, требования, специалисты, Федеральный государственный образовательный стандарт.