УДК 373.1+004.056.5
DOI 10.25688/2072-9014.2020.53.3.06

Г. Ю. Яламов

О современном состоянии обучения кибербезопасности

В статье рассмотрено современное состояние обучения кибербезопасности в общеобразовательных учреждениях и учреждениях высшего профессионального образования, основные направления его развития и совершенствования.

Ключевые слова: информационная безопасность; кибербезопасность; киберпространство; киберугроза; защита информации; информационно-психологическая безопасность.

Основной тренд развития современного общества связан с новым этапом развития технологий — четвертой промышленной революцией. Процесс перехода на новый уровень автоматизации и обмена данными, включающий в себя киберфизические системы, интернет вещей и облачные вычисления, вызывает существенные перемены в политической, экономической и социальной сферах, в том числе и в образовании. Резкий скачок объемов данных, развитие информационных и коммуникационных технологий, Интернета и других телекоммуникационных сетей оказывают преобразующее воздействие на информационную деятельность обучающихся, в процессе которой они постоянно используют возможности киберпространства, являющегося составляющей информационного пространства.

Под киберпространством мы здесь понимаем сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства). Киберпространство как сфера деятельности подвержено киберугрозам, которые существуют везде, где применяются информационные и коммуникационные технологии. Как следствие, возникла необходимость формирования у обучающихся навыков принятия правильных решений в ситуациях встречи с такими угрозами, систематизации понятий в этой области знания.

Кибербезопасность как понятие было сформулировано не так давно. Кибербезопасность рассматривается как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного

числа угроз и воздействий с нежелательными последствиями»[1]. Эти условия подразумевают, например, борьбу с компьютерными вирусами, спамом, удаленным взломом, утечкой данных и др.

В настоящее время молодые люди много времени проводят в социальных сетях, которые, по мнению специалистов, представляют собой инструмент вовлечения и способны формировать определенные алгоритмы поведения.

Не должны оставаться без внимания и проблемы, связанные с обеспечением информационно-психологической безопасности [7] пользователей информационных систем, Интернета и других телекоммуникационных сетей. Деятельность в киберпространстве подвержена факторам риска, способным оказать деструктивные воздействия на развитие познавательных или когнитивных качеств личности, на ее психоэмоциональное состояние [8]. К таким факторам можно отнести информационные перегрузки, «обманчивость природы» объектов виртуального мира, внешнюю агрессивность информации, информацию неэтичного характера или информацию, оскорбляющую мораль и чувства пользователя, сетевую информационную зависимость пользователя, информацию, не соответствующую эргономическим требованиям, и др.

На современном этапе государство через различные свои институты, в том числе и систему образования, обеспечивает противодействие угрозам информационной безопасности для всех субъектов образовательного процесса. Особое внимание уделяется вопросам кибербезопасности. Основные принципы, задачи и механизмы реализации государственной политики в области обеспечения информационной безопасности подрастающего поколения отражены в целом ряде документов[2].

Кроме того, для педагогов начального, общего и полного среднего образования были разработаны методические рекомендации «Основы кибербезопасности», которые на парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве» (Совет Федерации 17 апреля 2017 года) были рекомендованы для использования в образовательном процессе.

Эти методические рекомендации направлены на внедрение учебного материала по информационной безопасности в процесс изучения таких предметов, как «Информатика», «Окружающий мир», «Основы безопасности жизнедеятельности», «Технология», «Обществознание», «Биология» и других учебных дисциплин. Согласно данным рекомендациям, обучение кибербезопасности

---

[1] Концепция стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 16.03.2020).

[2] Распоряжение Правительства Российской Федерации от 02 декабря 2015 года № 2 2471-р «Об утверждении Концепции информационной безопасности детей // КонсультантПлюс. URL: http://www.consultant.t-u/document/cons_doc_LAW_190009/ (дата обращения: 16.03.2020); Федеральный закон от 29 декабря 2010 года М 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 16.03.2020).

должно осуществляться непрерывно в течение всего времени учебы в школе. Такой подход позволит преподавателям различных школьных предметов самостоятельно, с учетом своего учебного плана, использовать представленную информацию для расширения кругозора обучающихся в области информационной безопасности, сформировать у них ключевые компетенции и навыки безопасной работы в цифровой среде.

Анализируя описание курса «Основы кибербезопасности»[3], мы видим, что он включает в себя 8 модулей для разных возрастных категорий обучающихся со 2-го по 11-й классы. Каждый модуль содержит название раздела, предлагаемые для изучения темы и понятия кибербезопасности, структурированные по классам. Модули дидактически взаимосвязаны и могут рассматриваться параллельно, они обеспечивают преемственность знаний по информационной безопасности с предыдущими уровнями обучения. Некоторые цели обучения этого курса могут быть достигнуты при изучении информатики в 7–9-х классах.

Содержание курса соответствует Стандарту основного общего образования по информатике, что позволяет реализовать метапредметные результаты и предметные умения дисциплины «Информатика» при изучении вопросов информационной безопасности. В частности, имеются следующие возможности:

– формирование навыков и умений безопасного и целесообразного использования киберпространства, а также умения следовать нормам информационной этики и права;

– формирование умения использовать средства ИКТ при решении когнитивных, коммуникативных и организационных задач с соблюдением норм информационной безопасности, этико-социальных и правовых норм, здоровьесберегающих условий, требований техники безопасности и эргономики;

– понимание юридических аспектов использования программного обеспечения и работы в Интернете и т. п.

Кроме того, в методических рекомендациях предложены примеры уроков, которые можно проводить в рамках изучения школьных дисциплин «Информатика», «Окружающий мир» и «Основы безопасности жизнедеятельности». Также материалы курса могут эффективно использоваться на открытых уроках, а некоторые из них — в начальной школе на классном часе. Для оценки уровня усвоения образовательного материла обучающимся предложены различные оценочные средства.

Упомянутый выше учебный материал имеет несомненную педагогическую целесообразность. Вместе с тем он носит рекомендательный характер, эффективность его использования в учебном процессе во многом зависит от желания и готовности педагогов рассматривать вопросы кибербезопасности на своих уроках.

---

[3] *Тонких И. М., Комаров М. М., Ледовской В. И., Михайлов А. В.* Основы кибербезопасности: Описание курса для средних школ, 2–11 классы. М., 2016. 113 с. URL: http://vestnik.apkpro.ru/doc/osnovi_kiberbezopasnosti.pdf (дата обращения: 27.02.2020).

Хотелось бы видеть в программе общеобразовательной школы отдельный предмет по информационной безопасности, но современная программа настолько плотная, что для него просто нет места. Тем не менее по инициативе Общественной палаты в школьный курс по основам безопасности жизнедеятельности будет включен раздел по кибербезопасности. Министерство просвещения РФ поддержало эту идею, и программа учебного курса будет изменена после утверждения новых образовательных стандартов [2].

Анализ содержания школьных учебников на предмет отражения в них требований стандарта и примерных образовательных программ в области обучения кибербезопасности в основной и средней школе показывает, что в их содержание включены почти все понятия стандарта, но многие из них, к сожалению, не включают понятия информационной безопасности и кибербезопасности.

Если говорить об учебниках по предмету «Информатика», то понятие «информационная безопасность» упоминается в них достаточно редко и, как правило, только в узком его смысле, не соответствующем масштабам киберпространства. Так, к примеру, в учебнике «Информатика и ИКТ» информационная безопасность определяется как «состояние защищенности информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений, имеющих место в рамках данной информационной системы» [1].

А в учебнике «Информатика и ИКТ» для 11-го класса можно прочитать следующее: «Информационная безопасность — это совокупность мер по защите информационной среды общества и человека» [3]. И в том, и в другом случае в определениях киберпространство ограничено рамками информационной системы или среды, речь идет только о защите информации, а не о киберпространстве в целом со всеми его составляющими. Кроме того, в этих учебниках никак не отражена защита государства и человека как личности в рамках их информационной деятельности в киберпространстве. Не затронуты вопросы информационно-психологической безопасности, связанные с интернет-зависимостью, стрессами и переутомлением пользователей информационных систем, Интернета, других телекоммуникационных сетей.

Следует отметить учебник И. Г. Семакина и Е. К. Хеннера для 10–11-х классов «Информатика и ИКТ (базовый уровень)» [5], в котором авторами систематизированы основные понятия в области защиты цифровой информации и представлены они в виде иерархической схемы под названием «Система основных понятий».

Заслуживает внимания авторский учебно-методический комплекс (УМК) Л. Л. Босовой, который многие учителя используют в своей работе. УМК включает в себя учебники по информатике с 5-го по 9-й класс, методические пособия, сборник задач и упражнений, рабочие тетради и другие методические материалы по информатике. В учебниках раскрываются некоторые вопросы кибербезопасности, однако есть и недостатки [6]:

1) без внимания остались вопросы, связанные с понятиями киберпространства, кибербуллинга и киберпреступлений;

2) при раскрытии вопросов нет описания возможных киберугроз и, соответственно, не даны рекомендации по действиям и правилам поведения при встрече с ними;

3) для 6-х и 8-х классов учебный материал по кибербезопасности практически не представлен. Заметим, что именно у этой возрастной категории обучающихся проявляется активный интерес к социальным сетям и сервисам, а в школе увеличивается количество изучаемых предметов, что вызывает необходимость все чаще обращаться к Интернету за информацией для выполнения учебных заданий;

4) не рассмотрены вопросы: необходимости сохранения персональных данных; законодательства, действующего в Интернете; о зонах информационного риска для его пользователей; сетевой информационной зависимости и др.

Важно заметить, что подготовке будущих учителей в области кибербезопасности, на наш взгляд, не уделяется должного внимания. Так, учебные планы по направлению «Педагогическое образование» не содержат специальных информационных или методических дисциплин по изучению кибербезопасности, или информационной безопасности. Сам же ФГОС для данного направления подготовки включает в себя лишь одну компетенцию, формирование которой можно с большой натяжкой отнести к информационной безопасности, — способность использовать базовые правовые знания в различных сферах деятельности [6].

Сегодня вопросы обучения информационной безопасности студентов вузов затрагиваются многими авторами. Анализ научно-методической литературы, посвященной проблемам формирования и развития у студентов культуры безопасного поведения в киберпространстве, использования его возможностей, умения противостоять киберугрозам, показал следующее.

Целый ряд авторов (П. С. Ломаско, Н. А. Бушмелева, Е. В. Разова, Ю. И. Богатырева и др.) предлагают ввести в предметную подготовку студентов отдельную дисциплину, посвященную изучению информационной безопасности. По мнению этих авторов, данная дисциплина должна быть направлена на формирование у студентов представления о понятии «информационная безопасность», принципах и средствах обеспечения информационной безопасности отдельной личности, государства и общества в целом. Авторы схожи в одном: целью изучения дисциплины должно быть приобретение студентами теоретических сведений, практических умений и навыков применения современных ИКТ для использования их в профессиональной деятельности по защите информации и организации собственной безопасной информационной среды, т. е. личной информационной безопасности.

Несомненный интерес в аспекте исследуемой проблемы представляет коллективная монография [4]. Этот труд, на наш взгляд, может быть хорошей опорой при разработке учебников, методических пособий и курсов,

так или иначе связанных с обучением как информационной безопасности в целом, так и кибербезопасности в частности.

В монографии обобщены результаты научно-педагогических исследований авторов в области информатизации отечественного образования в контексте информационной безопасности, а также обоснованы и описаны перспективные направления фундаментальных и прикладных научных исследований в данной области в условиях конвергенции педагогической науки и современных ИКТ, взаимного влияния и проникновения их методов в методы других наук. В центре внимания авторов находится ***информационная безопасность субъектов образовательного процесса***, использующих в своей деятельности средства ИКТ, которая определена как условия, при которых действие или бездействие по отношению к субъектам образовательного процесса со стороны внешних информационных источников не влекут за собой негативные последствия для физического и психического здоровья пользователя [6]. Негативные последствия в данном контексте, по мнению авторов, могут вызывать:

– информация, запрещенная законодательством, или агрессивная, нелегитимная, неэтичная информация, а также информация, оскорбляющая моральные ценности и чувства пользователя, в том числе представленная в СМИ, Интернете, при сетевых взаимодействиях;

– использование некачественной педагогической продукции, разработанной с использованием ИКТ, не отвечающей педагогико-эргономическим требованиям;

– потеря авторских прав разработчика на результаты интеллектуальной собственности, представленной в электронном виде.

Кроме того, в монографии выделены и описаны содержательные аспекты информационной безопасности субъектов образовательного процесса, обоснована необходимость создания межпредметной программы формирования культуры их личной информационной безопасности. Что особенно ценно — в монографии уделено внимание подготовке учителей и студентов педагогических вузов в области информационной безопасности личности, а в приложении к монографии представлен каталог электронных ресурсов по теме подготовки обучающихся в школе и будущих учителей в области информационной безопасности и даны соответствующие ссылки на терминологические словари.

Вопросам обучения кибербезопасности уделяют внимание и зарубежные исследователи. Так, например, в работе [10] показано, что обучение в области кибербезопасности имеет междисциплинарный характер и тесно связано с информатикой, психологией, социологией, политикой, юриспруденцией, вычислительной техникой и управлением. По мнению авторов, междисциплинарность кибербезопасности как предмета для изучения отражается в реальной жизни (кибератаки, киберпреступления, кибербуллинг и др.). Поэтому авторы предлагают внеклассный подход к обучению кибербезопасности, выходящей за рамки формальной обстановки класса, студии или лаборатории.

Подобный подход позволяет подготовить обучающихся к решению реальных задач по противодействию киберугрозам или вообще избежать встречи с ними. Предлагается вовлекать обучающихся в различные проекты по исследованию реальных случаев взлома информационных систем совместно с профессионалами в области кибербезопасности. Некоторые зарубежные исследователи [9] советуют также использовать информационные системы как средства обучения основам кибербезопасности, например обучающую систему с открытым исходным кодом CyRIS (Cyber Range Instantiation System). Данная система позволяет выбрать тип кибератаки, ее ключевые характеристики, отследить действия, предпринимаемые обучающимся, и т. д.

Таким образом, можно сказать, что исследования проблем обучения студентов в области кибербезопасности идут по следующим основным направлениям:

1) создание и внедрение специализированного курса по информационной безопасности в учебные планы подготовки, в том числе и педагогических направлений;

2) разработка и реализация межпредметных программ [6], направленных на формирование культуры личной информационной безопасности субъектов образовательного процесса средствами метапредметных компонентов дисциплин «Информатика», «Технология», «Русский язык», «Литература», «Обществоведение», «История», «География» и др., которые в рамках разработки данной программы являются опорными;

3) использование специально разработанных средств и форм обучения, способствующих повышению компетентности студентов в области кибербезопасности, а также культуры их безопасного поведения в киберпространстве, т. е. способности и готовности противостоять преднамеренным или непреднамеренным воздействиям, которые могут нанести вред, независимо от естественного или искусственного характера таких воздействий.

Однако на сегодняшний день в связи с переходом на новые образовательные стандарты такие подходы реализовать достаточно сложно. Данное положение вещей выглядит не только грустно, но и небезопасно.

Реализация мер эффективной кибербезопасности в настоящее время является весьма сложной задачей, так как сегодня существует множество киберустройств, от которых могут исходить киберугрозы, а злоумышленники становятся все более изобретательными. Подрастающее поколение особенно подвержено информационным рискам в условиях глобальной массовой сетевой коммуникации, чем и характеризуется современный этап развития информационного общества. Поэтому в заключение хотелось бы сказать, что все участники образовательного процесса должны быть компетентны в области кибербезопасности, а учителя-предметники и преподаватели должны как минимум владеть ее основами, ведь педагоги сами могут столкнуться и со спамом, и с вирусами, и со взломом компьютера, и со многими другими киберугрозами; кроме того, они должны быть примером для обучающихся.

Литература

1. *Гейн А. Г., Сенокосов А. И.* Информатика и ИКТ. 11 класс. М.: Просвещение, 2012. 336 с.

2. *Костенко Я., Сидоренко Е.* Зададут курсор: Школьников научат безопасности в Сети // Известия. 2020. 9 янв. (№ 1). С. 1–5.

3. *Макарова Н. В., Николайчук Г. С., Титова Ю. Ф.* Информатика и ИКТ: 11 класс. СПб.: Питер, 2012. 223 с.

4. Развитие информатизации образования в школе и педагогическом вузе в условиях обеспечения информационной безопасности личности / С. А. Бешенков [и др.]. М.: ИУО РАО, 2018. 107 с.

5. *Семакин И. Г., Хеннер Е. К.* Информатика и ИКТ. Базовый уровень: учебник для 10–11 классов. 5-е изд. М.: БИНОМ. Лаборатория знаний, 2009. 246 с.

6. *Троицкая О. Н., Вохтомина Е. Д.* Подготовка будущих учителей математики и информатики к обучению школьников основам кибербезопасности // Информатика и образование. 2019. № 28. С. 24–31.

7. *Яламов Г. Ю.* Методические подходы к обеспечению информационно-психологической безопасности пользователей интеллектуальных обучающих систем // Педагогическая информатика. 2019. № 4. С. 176–182.

8. *Яламов Г. Ю.* Условия интеллектуализации цифровой образовательной среды // Грани познания. 2019. № 2 (61). С. 115–118.

9. *Beuran R. at al.* Cybersecurity education and training support system: CyRIS // IEICE Transactions on Information and Systems. 2018. Vol. E101-D. № 3. P. 740–749.

10. *Kam H. J., Katerattanakul P.* Enhancing student learning in cybersecurity education using an out-of-class learning // Journal of Information Technology Education: Inovations in Practice. 2019. Vol. 18. P. 029–047.

Literatura

1. *Gejn A. G., Senokosov A. I.* Informatika i IKT. 11 klass. M.: Prosveshhenie, 2012. 336 s.

2. *Kostenko Ya., Sidorenko E.* Zadadut kursor: Shkol`nikov nauchat bezopasnosti v Seti // Izvestiya. 2020. 9 yanv. (№ 1). S. 1–5.

3. *Makarova N. V., Nikolajchuk G. S., Titova Yu. F.* Informatika i IKT: 11 klass. SPb.: Piter, 2012. 223 s.

4. Razvitie informatizacii obrazovaniya v shkole i pedagogicheskom vuze v usloviyax obespecheniya informacionnoj bezopasnosti lichnosti / S. A. Beshenkov [i dr.]. M.: IUO RAO, 2018. 107 s.

5. *Semakin I. G., Xenner E. K.* Informatika i IKT. Bazovy`j uroven`: uchebnik dlya 10–11 klassov. 5-e izd. M.: BINOM. Laboratoriya znanij, 2009. 246 s.

6. *Troiczkaya O. N., Voxtomina E. D.* Podgotovka budushhix uchitelej matematiki i informatiki k obucheniyu shkol`nikov osnovam kiberbezopasnosti // Informatika i obrazovanie. 2019. № 28. S. 24–31.

7. *Yalamov G. Yu.* Metodicheskie podxody` k obespecheniyu informacionno-psixologicheskoj bezopasnosti pol`zovatelej intellektual`ny`x obuchayushhix sistem // Pedagogicheskaya informatika. 2019. № 4. S. 176–182.

8. *Yalamov G. Yu.* Usloviya intellektualizacii cifrovoj obrazovatel`noj sredy` // Grani poznaniya. 2019. № 2 (61). S. 115–118.

9. *Beuran R. at al.* Cybersecurity education and training support system: CyRIS // IEICE Transactions on Information and Systems. 2018. Vol. E101-D. № 3. P. 740–749.

10. *Kam H. J., Katerattanakul P.* Enhancing student learning in cybersecurity education using an out-of-class learning // Journal of Information Technology Education: Inovations in Practice. 2019. Vol. 18. P. 029–047.

G. Yu. Yalamov

About the Current State of Cybersecurity Education

In the article aspects of the current state of cybersecurity education, the main directions of its development and improvement.

Keywords: information security; cybersecurity; cyberspace; cyber threat; information protection; information and psychological security.