

ПОДГОТОВКА БУДУЩИХ УЧИТЕЛЕЙ МАТЕМАТИКИ И ИНФОРМАТИКИ К ОБУЧЕНИЮ ШКОЛЬНИКОВ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ

О. Н. Троицкая¹, Е. Д. Вохтомина¹

¹ *Северный (Арктический) федеральный университет имени М. В. Ломоносова*
163002, Россия, г. Архангельск, наб. Северной Двины, д. 17

Аннотация

Активное развитие отрасли кибербезопасности привело не только к необходимости разработки специализированного программного обеспечения, повышения уровня квалификации сотрудников крупных компаний, но и к формированию у будущих учителей умений и навыков грамотного поведения в киберпространстве. Анализ нормативной документации свидетельствует о том, что на первый план выходит проблема подготовки будущих учителей математики и информатики к обучению учащихся школы основам кибербезопасности. Статья посвящена описанию возможного способа решения выявленных проблем. Представлены четыре уровня сформированности знаний, умений и навыков студентов педагогических направлений подготовки в области кибербезопасности, средства и методы их достижения, структурные компоненты кибербезопасности и дисциплины учебного плана (бакалавриат), позволяющие овладеть содержанием этих компонентов, описаны методические особенности проведения лекционных и практических занятий. Авторы статьи полагают, что предлагаемый подход позволяет реализовать идею непрерывного обучения кибербезопасности по схеме: учащиеся школ — студенты бакалавриата — студенты магистратуры — действующие педагоги.

Ключевые слова: непрерывное обучение, кибербезопасность, киберугроза, уровни готовности.

DOI: 10.32517/0234-0453-2019-34-8-24-31

Для цитирования:

Троицкая О. Н., Вохтомина Е. Д. Подготовка будущих учителей математики и информатики к обучению школьников основам кибербезопасности // Информатика и образование. 2019. № 8. С. 24–31.

Статья поступила в редакцию: 15 августа 2019 года.

Статья принята к печати: 17 сентября 2019 года.

Сведения об авторах

Троицкая Ольга Николаевна, канд. пед. наук, доцент, зав. кафедрой экспериментальной математики и информатизации образования, Высшая школа информационных технологий и автоматизированных систем, Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск, Россия; o.troitskaya@narfu.ru; ORCID: 0000-0002-7885-9435

Вохтомина Ева Дмитриевна, студентка 1-го курса, Высшая школа информационных технологий и автоматизированных систем, Северный (Арктический) федеральный университет имени М. В. Ломоносова, г. Архангельск, Россия; eva.vohtomina@yandex.ru; ORCID: 0000-0002-0144-432X

1. Введение

Необходимость подготовки будущих учителей математики и информатики к обучению школьников основам кибербезопасности обусловлена рядом факторов. Прежде всего, это постоянное использование подрастающим поколением возможностей киберпространства и, как следствие, необходимость формирования у них навыков принятия правильных решений в ситуациях встречи с киберугрозами. Далее, это введение в действие ряда документов и нормативно-правовых актов. Так, в 2010 году закон «О защите детей от информации, причиняющей вред их здоровью и развитию» на официальном уровне определил понятие «информационная безопасность детей» [1]. Принятая в 2015 году правительством Российской Федерации «Концепция информационной безопасности детей» [2] обозначила основные принципы, задачи и механизмы реализации государственной политики в области обеспечения информационной безопасности подрастающего поколения. В докумен-

те подчеркнута необходимость приобретения детьми навыков «безопасного существования в современном информационном пространстве» [2, с. 6]. Их формирование можно осуществить путем разработки и внедрения «специальных образовательных и просветительских программ, содержащих информацию об информационных угрозах, о правилах безопасного пользования детьми сетью Интернет» [2, с. 8].

В этот же период времени наряду с понятием «информационная безопасность» в сфере информационных технологий и в области законодательства начинают использовать понятие «кибербезопасность». В проекте Концепции стратегии кибербезопасности Российской Федерации выделено два понятия — киберпространство как элемент информационного пространства и кибербезопасность как составная часть информационной безопасности: «киберпространство — сфера деятельности в информационном пространстве, образованная 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)», «кибербезопасность — совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [3]. Данный подход согласуется с подходом, представленным в международном стандарте ISO/IEC 27032:2012. Согласно стандарту, киберпространство — это «комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет посредством соответствующих сетевых и коммуникационных технологий» [4].

Таким образом, кибербезопасность, обеспечивая защиту данных в цифровом виде, является составным компонентом информационной безопасности и обеспечивает безопасность программного обеспечения (отсутствие вредоносного кода, уязвимостей, угроз проникновения и т. д.), безопасность доступа к сетевым ресурсам и сервисам и безопасность использования глобальной сети Интернет.

Следствием развития такого подхода явилось обоснование внедрения в образовательный процесс методических рекомендаций «Основы кибербезопасности», которые 17 апреля 2017 года были представлены в Совете Федерации на парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве». Согласно им обучение кибербезопасности должно осуществляться непрерывно в течение всего обучения в школе на таких предметах, как «Окружающий мир», «Основы безопасности жизнедеятельности», «Технология», «Обществознание». При этом авторы методических рекомендаций отмечают, что «наиболее очевидной является возможность дополнения вопросами кибербезопасности уроков информатики» [5].

Вопросы методики обучения кибербезопасности школьников затрагиваются многими авторами. Так, например, Т. В. Рихтер, Т. С. Шумейко предлагают организацию школы кибербезопасности, участниками которой станут школьники и их родители [6]. Главная задача школы, состоящая в повышении уровня подготовки учащихся в сфере информационной безопасности, может быть достигнута за счет целенаправленного обучения детей и привлечения их родителей к участию в организации данного процесса. Т. Ю. Денщикова с соавторами считают необходимым включить в образовательный процесс серию взаимосвязанных уроков, контекст которых приближен к реальной действительности: деловая игра, круглый стол, защита проектов, дискуссия, дебаты [7]. Е. В. Данильчук с соавторами в работе [8] рассматривают компонентный состав методики формирования понятия «информационная безопасность» на различных этапах обучения информатике в школе.

Ряд авторов исследуют вопрос обучения информационной безопасности студентов вузов. Так, А. А. Кравцов в статье [9] рассматривает особенности преподавания дисциплины «Гуманитарные аспекты

информационной безопасности», цель которой состоит в том, чтобы научить студентов противостоять информационному воздействию и манипуляции массовым сознанием с применением информационных и коммуникационных технологий. В качестве специального средства обучения студентов П. И. Алексеевский и А. И. Разумова в [10] предлагают использовать электронный интерактивный учебник. И. А. Рахманенко описывает в работе [11] возможности применения электронной образовательной среды Moodle в процессе обучения студентов основам информационной безопасности.

Вопросам обучения кибербезопасности уделяют внимание и зарубежные исследователи. Н.-Ж. Кам и Р. Катараттанакул в работе [12] утверждают, что образование в области кибербезопасности является междисциплинарным, оно охватывает психологию, социологию, политику, юриспруденцию, информатику, вычислительную технику и управление. По их мнению, такая междисциплинарная природа отражается в реальной жизни. Студенты сталкиваются с кибератаками, порой становясь жертвами киберпреступлений (кража их персональных данных, интеллектуальной собственности и т. п.). Н.-Ж. Кам и Р. Катараттанакул считают, что именно внеклассный подход к обучению позволит подготовить учащихся к реальным задачам, побуждая выходить их за рамки формальной обстановки в классе, студии или лаборатории за счет вовлечения в различные проекты по исследованию реальных случаев взлома информационных систем совместно с профессионалами в области кибербезопасности. В качестве средства обучения основам кибербезопасности R. Beuran и др. в работе [13] предлагают обучающую систему с открытым исходным кодом CyRIS (Cyber Range Instantiation System). Она позволяет осуществлять выбор типа кибератаки, ее ключевых характеристик, отслеживает действия, предпринимаемые обучающимся, и т. д.

Анализ учебных планов для направления подготовки 44.03.05 «Педагогическое образование» (профили «Математика и информатика», «Математическое образование», «Информационное образование» и др.) показал, что сегодня большинство из них не содержит ни специальной информационной дисциплины (например, «Информационная безопасность» или «Кибербезопасность»), ни специальной методической дисциплины. В самом ФГОС (Приказ Минобрнауки России № 91 от 09.02.2016) для данного направления подготовки выделена лишь одна компетенция ОК-7, формирование которой так или иначе связано с информационной безопасностью: «способность использовать базовые правовые знания в различных сферах деятельности» [14].

Проведенное нами в сентябре 2017 года тестирование студентов первого—третьего курсов направления подготовки 44.03.05 «Педагогическое образование», профили «Математика» и «Информатика» (всего 60 человек), показало, что они распознают ситуации встречи с киберугрозой, но принять соответствующее решение и дать рекомендации по поведению в сложившейся ситуации многие не могут.

Таким образом, перед нами возникли две задачи, решение которых обусловлено современными тенденциями развития образовательной отрасли кибербезопасности:

- 1) повышение уровня сформированности умений и навыков в области кибербезопасности студентов педагогических направлений подготовки;
- 2) подготовка будущих учителей математики и информатики к обучению учащихся школы основам кибербезопасности.

2. Анализ существующих подходов, позволяющих решить поставленные задачи

С целью определения способов решения поставленных задач был проведен анализ психолого-педагогической и методической литературы.

Еще в 2009 году П. С. Ломаско защитил диссертацию «Методическая система подготовки учителя информатики в области информационной безопасности» [15]. Он предложил ввести в предметную подготовку студентов отдельную дисциплину «Информационная безопасность» и использовать созданный им портал по информационной безопасности для организации их проектно-исследовательской деятельности в данной области. При этом П. С. Ломаско выделил четыре предметных составляющих компетентности в области информационной безопасности: юридический (информационно-правовой), программно-технический, административный и социально-культурный.

Н. А. Бушмелева и Е. В. Разова в статье [16] с целью становления у студентов педагогических направлений подготовки целостного представления о понятии «информационная безопасность» предлагают включить в учебные планы дисциплину «Информационная безопасность и защита информации». Конкретизация этой цели через выделение семи задач позволяет сформировать у студентов представления о принципах и средствах обеспечения информационной безопасности как отдельной личности, так и государства в целом. Особое внимание авторы уделяют взаимосвязи дисциплины «Информационная безопасность и защита информации» с дисциплинами информационного цикла и смежных с ними. По мнению авторов, «межпредметные и внутрипредметные связи дисциплины “Информационная безопасность и защита информации” должны быть направлены на углубление знаний и навыков в области информационной безопасности» [16]. К сожалению, авторы не рассматривают такие дисциплины, как «Методика преподавания информатики», «Психология», которые в значительной мере позволяют формировать у студентов навыки безопасного поведения в киберпространстве.

Ю. И. Богатырева в работе [17] описывает особенности обучения магистрантов направления «Педагогическое образование» за счет включения в учебный план дисциплины «Информационная безопасность в образовательных организациях»

(ТГПУ имени Л. Н. Толстого). Как уточняет автор, цель изучения дисциплины состоит в приобретении студентами «теоретических сведений, практических умений и навыков применения современных информационных технологий для использования их в профессиональной деятельности по защите информации и организации безопасной информационно-образовательной среды образовательной организации» [там же]. Несмотря на то что Ю. И. Богатырева затрагивает проблему «непрерывной подготовки личности к обеспечению информационной безопасности на этапе вузовского и послевузовского образования» [там же], особенности ее решения она не раскрывает. Автор не представляет реализацию непрерывного обучения в системе «школьник — студент бакалавриата — студент магистратуры — действующий педагог».

Таким образом, проведенный анализ свидетельствует о том, что исследователи делают акцент либо на внедрении специального курса по информационной безопасности в учебный план педагогических направлений подготовки, либо на использовании специально разработанных средств обучения. Однако на сегодняшний день в связи с переходом на новые образовательные стандарты такой подход реализовать достаточно сложно.

3. Авторский подход к решению поставленных задач

Анализ нормативно-правовой информации и психолого-педагогической литературы позволил нам выделить четыре уровня сформированности знаний, умений и навыков студентов педагогических направлений подготовки в области кибербезопасности (табл. 1).

С целью достижения первых трех уровней мы в соответствии с выделенными компонентами кибербезопасности определили дисциплины учебного плана бакалавров, позволяющие овладеть содержанием этих компонентов (табл. 2).

Методика проведения лекционных и практических занятий предполагает постановку перед студентами контекстных задач. Например, при изучении темы «Планирование и управление Active Directory» дисциплины «Сети и сетевые технологии» студенты должны решить задачу: «Вы являетесь администратором школьной компьютерной сети. С использованием Active Directory настройте политику безопасности, обеспечивающую выполнение следующих требований:

- создание организационной структуры, учитывающей различный функционал сотрудников и обучающихся;
- ведение списка пользователей сети;
- соблюдение принципов безопасного формирования паролей пользователей;
- периодическая принудительная смена паролей;
- ограничение времени доступа в сеть пользователей разных групп;

Таблица 1

Уровни сформированности знаний, умений и навыков в области кибербезопасности

Уровень	Характеристика уровня по выполняемым действиям
I. Знания-представления	Студент способен определить наличие киберугрозы, распознать возможные риски работы в киберпространстве
II. Знания-копии	Студент способен описать возможные средства и методы нивелирования киберугрозы в соответствии с ее видом
III. Знания-умения	Студент способен применить освоенные средства и методы для нивелирования киберугрозы в <i>стандартных</i> ситуациях, способен <i>ознакомить</i> учащихся с понятием киберугрозы, видами киберугроз, средствами и методами борьбы с ними
IV. Знания-трансформация	Студент способен применить освоенные средства и методы для нивелирования киберугрозы в <i>нестандартных</i> ситуациях, способен <i>сформировать</i> у учащихся <i>умения и навыки</i> безопасной работы в киберпространстве

- ограничение на возможность самостоятельной установки пользователями программного обеспечения;
- выделение общих сетевых ресурсов и ограничение доступа к ним».

Решение ряда задач дисциплины «Базы данных» предполагает изучение студентами федерального закона «О персональных данных» [18]. Так, например, на его основе они определяют структуру базы данных информационной системы медицинского учреждения для хранения информации о пациентах, историях их болезни, назначенном лечении, лечащих докторов и т. д. Созданную базу данных студенты заполняют тестовой информацией и накладывают ограничения различным группам пользователей на доступность персональных данных.

Знакомство с нормативной документацией в области кибербезопасности продолжается и в процессе изучения методических дисциплин. Данный процесс

сопровождается рассмотрением особенностей формирования информационных понятий, суждений и умозаключений, относящихся к кибербезопасности. Например, студентам может быть дано следующее задание: «Опираясь на трехэтапную схему формирования информационных понятий, представьте методику формирования понятия “киберугроза”. Разработайте фрагмент сценария урока». На практических занятиях студенты разрабатывают сценарии учебных занятий и интерактивных игр по кибербезопасности для учащихся основной школы. Будущие учителя учитывают тот факт, что у большинства школьников есть опыт работы в киберпространстве и, возможно, они уже сталкивались с киберугрозами. Именно поэтому студенты разрабатывают методические материалы с опорой на теорию И. С. Якиманской, которая доказала необходимость учета субъектного опыта детей в процессе обучения [19].

Таблица 2

Соответствие компонентов кибербезопасности и дисциплин учебного плана

Компонент кибербезопасности	Содержание компонента кибербезопасности	Дисциплины учебного плана
Безопасность программного обеспечения	Защита от несанкционированного доступа. Защита от утери, повреждения данных. Незаконное распространение программного обеспечения. Компьютерные вирусы: виды, особенности внедрения и воздействия. Антивирусные программы	Информатика. Архитектура ЭВМ. Базы данных. Операционные системы. Цифровые технологии в образовании
Безопасность доступа к сетевым ресурсам и сервисам	Виды преступлений в киберпространстве. Средства и методы защиты от киберугроз. Программы-фильтры. Сети Wi-Fi. Социальные сети. Сетевые игры. Опасная информация в сети. Безопасность сервисов общения (электронная почта, скайп и т. д.). Цифровое правительство	Основы правовых знаний. Сети и сетевые технологии. Операционные системы
Безопасность использования глобальной сети Интернет	Общение в сети, его особенности и возможные последствия. Агрессия в сети и способы противодействия ей. Психологическое воздействие через интернет. Интернет-зависимость. Собственность в интернете. Авторское право. Интеллектуальная собственность. Технологии анализа цифрового следа.	Теоретические основы обучения информатике. Методика обучения информатике и ИКТ учащихся основной школы. Методика обучения информатике и ИКТ в старшей школе. Педагогическая и социальная психология

Однако для формирования уровня «знания-трансформация» будущих учителей необходимо включать в деятельность творческого характера. С этой целью студенты, обучающиеся по направлению подготовки 44.03.05 «Педагогическое образование» (с двумя профилями подготовки), профили «Математика» и «Информатика», участвуют в подготовке областного мероприятия «Неделя кибербезопасности». Они разрабатывают и проводят классные часы с учащимися V—IX классов, родительские собрания, составляют задания для конкурса задач по кибербезопасности и критерии их оценивания. Особенности задач данного вида подробно описаны в статье [20]. Студенты являются членами комиссии по проверке работ учащихся. Вместе с преподавателями кафедры они подводят итоги конкурса.

Начиная с 2017 года студенты активно участвуют в различных всероссийских и международных конкурсах. Так, диплом лауреата VIII Международной конференции-конкурса «Инновационные информационно-педагогические технологии в системе ИТ-образования» (29 ноября — 2 декабря 2018 года, МГУ имени М. В. Ломоносова) получила студентка Евгения Федорова за представленный ею проект «Симулятор “Поисковичок” как средство подготовки учащихся к безопасному поведению в сети Интернет». В начале 2019 года две студентки Татьяна Золотарева и Анна Лебедева приняли участие в конкурсе методических разработок по внеурочной деятельности в рамках проекта «Страна

невыученных уроков» (корпорация «Российский учебник») с работой «Кибербезопасность» (для VII класса). В процессе написания выпускной квалификационной работы в 2019 году под руководством доцента кафедры экспериментальной математики и информатизации образования Т. С. Шириковой студенты разработали сборник задач по кибербезопасности в дополнение к УМК Л. Л. Босовой. После соответствующей доработки он будет опубликован.

К исследованиям в области методики обучения основам кибербезопасности подключились и студенты направления подготовки 44.04.01 «Педагогическое образование», магистерская программа «Информационные технологии в образовании». Они исследовали такие вопросы, как обучение основам кибербезопасности родителей школьников, разработка симуляторов для формирования у школьников навыков безопасного поведения в глобальной сети, создание дидактических игр по кибербезопасности.

Подготовка магистрантов к обеспечению информационной безопасности образовательного процесса реализована за счет введения в основную образовательную программу отдельной профессионально-специализированной компетенции (ПСК-2 — способность обеспечивать информационную безопасность образовательного процесса), которая формируется через соответствующие дисциплины (табл. 3).

В 2019/2020 учебном году на базе кафедры экспериментальной математики и информатизации

Таблица 3

Реализация ПСК-2 в учебном плане магистратуры

Дисциплина учебного плана	Развитие компетенции	
Технологии создания образовательных сайтов и порталов	Знать/ понимать	Распознавать риски использования глобальной сети учащимися в школе и дома, описывать средства и методы снижения данных рисков
	Уметь/применять	Создавать на сайтах образовательных организаций и на персональных сайтах педагогов страницы, адресованные всем участникам образовательного процесса, с информацией о средствах и методах снижения рисков использования глобальной сети учащимися
Технические и программные средства информатизации образования	Знать/ понимать	Описывать программы, обеспечивающие информационную безопасность образовательного процесса
	Уметь/применять	Выбирать и устанавливать программы-фильтры и детские поисковые системы на компьютеры образовательной организации для обеспечения информационной безопасности образовательного процесса
Проектирование, развертывание и администрирование компьютерных сетей образовательной организации	Знать/ понимать	Описывать системные средства безопасности локального компьютера образовательной организации, способы создания учетных записей пользователей компьютерной сети образовательной организации с целью обеспечения информационной безопасности образовательного процесса
	Уметь/применять	Использовать системные средства безопасности локального компьютера образовательной организации, создавать учетные записи пользователей компьютерной сети образовательной организации, ограничивать их с целью обеспечения информационной безопасности образовательного процесса

образования САФУ имени М. В. Ломоносова будет организовано обучение учителей школ по профессиональной программе повышения квалификации «Обучение основам кибербезопасности в образовательных организациях» с применением дистанционных образовательных технологий.

4. Заключение

Дальнейшее развитие данного исследования предполагает расширение спектра проводимых мероприятий. Например, на базе САФУ имени М. В. Ломоносова планируется проведение конкурса «Кибербезопасность в современном мире» для студентов педагогических направлений подготовки (март 2020 года). Он будет включать несколько номинаций: «Лучшее внеучебное занятие по кибербезопасности», «Лучший видеоролик “Киберпространство — в чем его опасность?”», «Социальная реклама “Как ты можешь противостоять киберугрозе?”», «Лучший веб-квест по кибербезопасности».

Предлагаемый нами подход позволяет решить не только задачи повышения уровня сформированности умений и навыков в области кибербезопасности студентов педагогических направлений подготовки, подготовки будущих учителей математики и информатики к обучению учащихся школы основам кибербезопасности, но и организовать непрерывное обучение кибербезопасности по схеме: учащиеся школ — студенты бакалавриата — студенты магистратуры — действующие педагоги.

Список использованных источников

1. Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». http://www.consultant.ru/document/cons_doc_LAW_108808/
2. Распоряжение Правительства Российской Федерации от 02 декабря 2015 года № 2471-р «Об утверждении Концепции информационной безопасности детей». http://www.consultant.ru/document/cons_doc_LAW_190009/
3. Концепция стратегии кибербезопасности Российской Федерации. <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>
4. Марков А. С., Цирлов В. Д. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1. С. 28–35. <http://cyberrus.com/wp-content/uploads/2014/03/28-35.pdf>
5. Тонких И. М., Комаров М. М., Ледовской В. И., Михайлов А. В. Основы кибербезопасности. Описание курса для средних школ, 2–11 классы. <https://toipkro.ru/content/files/documents/podrazdeleniya/orodo/ciber%20bezopasnost.pdf>
6. Рихтер Т. В., Шумейко Т. С. Школа кибербезопасности как эффективное средство обеспечения информационной безопасности подрастающего поколения // Современные тенденции естественно-математического образования: школа — вуз. Материалы Международной научно-практической конференции. Соликамск: СГПИ, 2018. С. 43–45.
7. Денищикова Т. Ю., Аров Х. Н., Должикова М. В., Глушенко И. А., Петьков В. А. Технология обучения школьников основам информационной безопасности // Вестник Адыгейского государственного университета. Серия 3: Педагогика и психология. 2017. № 4. С. 117–123. <http://vestnik.adygnet.ru/files/2017.4/4992/117-123.pdf>
8. Данильчук Е. В., Лукичева А. В., Касьянов С. Н. Методические особенности формирования понятия «информационная безопасность» на разных этапах обучения информатике в школе // Известия Волгоградского государственного педагогического университета. 2018. № 8. С. 8–14. <http://izvestia.vspu.ru/files/publics/131/8-14.pdf>
9. Кравцов А. А. Значение дисциплины «Гуманитарные аспекты информационной безопасности» при овладении студентами общекультурными и профессиональными компетенциями // Вестник МГЛУ. Гуманитарные науки. 2015. № 18. С. 67–75.
10. Алексеевский П. И., Разумова А. И. Разработка электронного интерактивного учебника по теме «Основы информационной безопасности» // Актуальные вопросы преподавания математики, информатики и информационных технологий. 2018. № 3. С. 131–134.
11. Рахманенко И. А. Обучение в области информационной безопасности в электронной информационно-образовательной среде вуза // Современное образование: повышение профессиональной компетентности преподавателей вуза — гарантия обеспечения качества образования. Материалы международной научно-методической конференции. Томск: ТУСУР, 2018. С. 169–170.
12. Kam H.-J., Katerattanakul P. Enhancing student learning in cybersecurity education using an out-of-class learning // Journal of Information Technology Education: Innovations in Practice. 2019. Vol. 18. P. 029–047. DOI: 10.28945/4200
13. Beuran R., Pham C., Tang D., Chinen K., Tan Y., Shinoda Y. Cybersecurity education and training support system: CyRIS // IEICE Transactions on Information and Systems. 2018. Vol. E101.D. Is. 3. P. 740–749. DOI: 10.1587/transinf.2017EDP7207
14. Приказ Министерства образования и науки Российской Федерации от 9 февраля 2016 года № 91 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (уровень бакалавриата)». http://www.consultant.ru/document/cons_doc_LAW_194939/
15. Ломаско П. С. Методическая система подготовки учителя информатики в области информационной безопасности: автореф. дис. ... канд. пед. наук. Красноярск, 2009. 25 с.
16. Бушмелева Н. А., Разова Е. В. Формирование компетенций в области информационной безопасности в системе высшего педагогического образования // Научно-методический электронный журнал «Концепт». 2017. Т. 2. С. 537–544. <https://e-koncept.ru/2017/570106.htm>
17. Богатырева Ю. И. Информационная безопасность будущих педагогов в образовательных организациях как условие обеспечения национальной безопасности // Гуманитарные чтения «Свободная стихия». Материалы III Международной научно-практической конференции (г. Севастополь, 13–15 сентября 2018). Севастополь: СевГУ, 2018. С. 186–189.
18. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». http://www.consultant.ru/document/cons_doc_LAW_61801/
19. Якиманская И. С. Концепция личностно ориентированного образования // Ученые записки Петрозаводского государственного университета. 2010. № 5. С. 36–40.
20. Троицкая О. Н., Безумова О. Л., Ширикова Т. С. Конкурс задач по кибербезопасности как средство подготовки школьников к безопасному поведению в киберпространстве // Актуальные проблемы методики обучения информатике и математике в современной школе. Международная научно-практическая интернет-конференция (г. Москва, 22–26 апреля 2019). <http://news.scienceland.ru/2019/04/23/> <http://news.scienceland.ru/2019/04/23/конкурс-задач-по-кибербезопасности-к/>

TRAINING OF FUTURE TEACHERS OF MATHEMATICS AND INFORMATICS TO TEACHING SCHOOLCHILDREN TO THE BASES OF CYBERSECURITY

O. N. Troitskaya¹, E. D. Vohtomina¹

¹ Northern (Arctic) Federal University named after M. V. Lomonosov
163002, Russia, Arkhangelsk, nab. Severnoy Dviny, 17

Abstract

The active development of the cybersecurity industry has led not only to the need to develop specialized software, improve the skills of employees of large companies, but also to the formation of future teachers' skills and abilities of competent behavior in cyberspace. The analysis of the normative documentation indicates that the problem of training future teachers of mathematics and computer science for teaching schoolchildren the basics of cybersecurity comes to the fore. The article is devoted to the description of a possible way to solve the identified problems. The article presents four levels of formation of knowledge, skills of students of pedagogical areas of training in the field of cybersecurity, means and methods of their achievement, structural components of cybersecurity and the disciplines of the curriculum (bachelor's degree), allowing to master the content of these components, describes the special features of lecture and practical lessons. The authors of the article believe that the proposed approach allows us to implement the idea of lifelong cybersecurity education according to the scheme: schoolchildren — undergraduate students — graduate students — acting teachers.

Keywords: lifelong learning, cybersecurity, cyber threat, levels of readiness.

DOI: 10.32517/0234-0453-2019-34-8-24-31

For citation:

Troitskaya O. N., Vohtomina E. D. Podgotovka budushhikh uchitelej matematiki i informatiki k obucheniyu shkol'nikov osnovam kiberbezopasnosti [Training of future teachers of mathematics and informatics to teaching schoolchildren to the bases of cybersecurity]. *Informatika i obrazovanie — Informatics and Education*, 2019, no. 8, p. 24–31. (In Russian.)

Received: August 15, 2019.

Accepted: September 17, 2019.

About the authors

Olga N. Troitskaya, Candidate of Sciences (Education), Docent, Head of the Department of Experimental Mathematics and Informatization of Education, Higher School of Information Technologies and Automated Systems, Northern (Arctic) Federal University named after M. V. Lomonosov, Arkhangelsk, Russia; o.troitskaya@narfu.ru; ORCID: 0000-0002-7885-9435

Eva D. Vohtomina, 1st year student, Higher School of Information Technologies and Automated Systems, Northern (Arctic) Federal University named after M. V. Lomonosov, Arkhangelsk, Russia; eva.vohtomina@yandex.ru; ORCID: 0000-0002-0144-432X

References

1. Federal'nyj zakon ot 29 dekabrya 2010 goda № 436-ФЗ "O zashchite detej ot informatsii, prichinyayushhej vred ikh zdorov'yu i razvitiyu" [Federal Law dated December 29, 2010 No. 436-ФЗ "On the Protection of Children from Information Harmful to Their Health and Development"]. (In Russian.) Available at: http://www.consultant.ru/document/cons_doc_LAW_108808/
2. Rasporyazhenie Pravitel'stva Rossijskoj Federatsii ot 02 dekabrya 2015 goda № 2471-r "Ob utverzhdenii Kontseptsii informatsionnoj bezopasnosti detej" [Decree of the Government of the Russian Federation dated December 2, 2015 No. 2471-r "On approval of the Concept of children's information security"]. (In Russian.) Available at: http://www.consultant.ru/document/cons_doc_LAW_190009/
3. Kontseptsiya strategii kiberbezopasnosti Rossijskoj Federatsii [The concept of the cybersecurity strategy of the Russian Federation]. (In Russian.) Available at: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>
4. Markov A. S., Tsirlov V. D. Rukovodyashhie ukazaniya po kiberbezopasnosti v kontekste ISO 27032 [Guidelines for cybersecurity in the context of ISO 27032]. *Voprosy kiberbezopasnosti — Cybersecurity Issues*, 2014, no. 1, p. 28–35. (In Russian.) Available at: <http://cyberrus.com/wp-content/uploads/2014/03/28-35.pdf>
5. Tonkikh I. M., Komarov M. M., Ledovskoy V. I., Mikhailov A. V. Osnovy kiberbezopasnosti. Opisanie kursa dlya srednikh shkol, 2-11 klassy [The basics of cybersecurity. Course description for secondary schools, grades 2–11]. (In Russian.) Available at: <https://toipkro.ru/content/files/documents/podrazdeleniya/orodo/ciber%20bezopasnost.pdf>
6. Richter T. V., Shumeiko T. S. Shkola kiberbezopasnosti kak ehffektivnoe sredstvo obespecheniya informatsionnoj bezopasnosti podrastayushhego pokoleniya [School of cybersecurity as an effective means for ensuring information security of the understanding generation]. *Sovremennyye tendentsii estestvenno-matematicheskogo obrazovaniya: shkola — vuz. Materialy Mezhdunarodnoj nauchno-prakticheskoy konferentsii [Modern trends in natural-mathematical education: school — university. Proc. Int. Scientific and Practical Conf.]*. Solikamsk, SSPI, 2018, p. 43–45. (In Russian.)
7. Denshchikova T. Yu., Arov H. N., Dolzhikova M. V., Glushchenko I. A., Petkov V. A. Tekhnologiya obucheniya shkol'nikov osnovam informatsionnoj bezopasnosti [Technology of training of school students in bases of information security]. *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya 3: Pedagogika i psikhologiya — The Bulletin of the Adyge State University. Series 3: Pedagogy and Psychology*, 2017, no. 4, p. 117–123. (In Russian.) Available at: <http://vestnik.adygnet.ru/files/2017.4/4992/117-123.pdf>
8. Danilchuk E. V., Lukicheva A. V., Kasyanov S. N. Metodicheskie osobennosti formirovaniya ponyatiya «informatsionnaya bezopasnost'» na raznykh etapakh obucheniya informatike v shkole [Methodological features of the concept "information security" at different stages of teaching computer science at school]. *Izvestiya Volgogradskogo gosudarstvennogo pedagogicheskogo universiteta — Izvestia of the Volgograd State Pedagogical University*, 2018, no. 8, p. 8–14. (In Russian.) Available at: <http://izvestia.vspu.ru/files/publics/131/8-14.pdf>
9. Kravtsov A. A. Znachenie distsipliny "Gumanitarnyye aspekty informatsionnoj bezopasnosti" pri ovladenii studentami obshhekul'turnymi i professional'nymi kompetentsiyami [The importance of the course "Humanitarian aspects of information security" in students' acquirement of common cultural and professional competences]. *Vestnik MGLU. Gumanitarnyye nauki — Bulletin of MSLU. Humanitarian Sciences*, 2015, no. 18, p. 67–75. (In Russian.)
10. Alekseevsky P. I., Razumova A. I. Razrabotka ehlektronnoho interaktivnogo uchebnika po teme "Osnovy

informatsonnoy bezopasnosti” [The development of electronic interactive textbook on the subject of “Fundamentals of information security”]. *Aktual'nye voprosy prepodavaniya matematiki, informatiki i informatsonnykh tekhnologij* — *Actual issues of teaching mathematics, computer science and information technology*, 2018, no. 3, p. 131–134. (In Russian.)

11. Rakhmanenko I. A. Obuchenie v oblasti informatsonnoy bezopasnosti v ehlektronnoy informatsonno-obrazovatel'noj srede vuza [Teaching information security in information-educational environment of higher educational institution]. *Sovremennoe obrazovanie: povyschenie professional'noj kompetentnosti prepodavatelej vuza — garantiya obespecheniya kachestva obrazovaniya. Materialy mezhdunarodnoy nauchno-metodicheskoy konferentsii* [Modern education: increasing the professional competence of university teachers is a guarantee of ensuring the quality of education. Proc. Int. Scientific-Methodological Conf.]. Tomsk, TUSUR, 2018, p. 169–170. (In Russian.)

12. Kam H-J., Katerattanakul P. Enhancing student learning in cybersecurity education using an out-of-class learning. *Journal of Information Technology Education: Innovations in Practice*, 2019, vol. 18, p. 029–047. DOI: 10.28945/4200

13. Beuran R., Pham C., Tang D., Chinen K., Tan Y., Shinoda Y. Cybersecurity education and training support system: CyRIS. *IEICE Transactions on Information and Systems*, 2018, vol. E101.D, is. 3, p. 740–749. DOI: 10.1587/transinf.2017EDP7207

14. Prikaz Ministerstva obrazovaniya i nauki Rossijskoj Federatsii ot 9 fevralya 2016 goda № 91 “Ob utverzhdenii federal'nogo gosudarstvennogo obrazovatel'nogo standarta vysshego obrazovaniya po napravleniyu podgotovki 44.03.05 Pedagogicheskoe obrazovanie (s dvumya profilyami podgotovki) (uroven' bakalavriata)” [Order of the Ministry of Education and Science of the Russian Federation dated February 9, 2016 No. 91 “On approval of the federal state educational standard of higher education in the field of training 44.03.05 Pedagogical education (with two specialization profiles) (undergraduate level)”]. (In Russian.) Available at: http://www.consultant.ru/document/cons_doc_LAW_194939/

15. Lomasko P. S. Metodicheskaya sistema podgotovki uchitelya informatiki v oblasti informatsonnoy bezopasnosti: avtoref. dis. ... kand. ped. nauk [Methodical system of train-

ing a teacher of computer science in the field of information security. Cand. ped. sci. diss. author's abstract]. Krasnoyarsk, 2009. 25 p. (In Russian.)

16. Bushmeleva N. A., Razova E. V. Formirovanie kompetentsij v oblasti informatsonnoy bezopasnosti v sisteme vysshego pedagogicheskogo obrazovaniya [Formation of competencies in the field of information security in the system of higher pedagogical education]. *Nauchno-metodicheskij ehlektronnyj zhurnal “Kontsept”* — *Scientific and Methodological Electronic Journal “Concept”*, 2017, vol. 2, p. 537–544. (In Russian.) Available at: <https://e-koncept.ru/2017/570106.htm>

17. Bogatyreva Yu. I. Informatsonnaya bezopasnost' budushhikh pedagogov v obrazovatel'nykh organizatsiyakh kak uslovie obespecheniya natsional'noj bezopasnosti [Information security of future teachers in educational organizations as a condition for ensuring national security]. *Gumanitarnye chteniya “Svobodnaya stikhiya”. Materialy III Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Humanitarian readings “Free element”. Proc. III Int. Scientific and Practical Conf.]. Sevastopol, SevSU, 2018, p. 186–189. (In Russian.)

18. Federal'nyj zakon ot 27 iyulya 2006 goda № 152-ФЗ “O personal'nykh dannykh” [Federal Law dated July 27, 2006 No. 152-ФЗ “On Personal Data”]. (In Russian.) Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/

19. Yakimanskaya I. S. Kontseptsiya lichnostno orientirovannogo obrazovaniya [The concept of personality-oriented education]. *Uchenye zapiski Petrozavodskogo gosudarstvennogo universiteta — Proceedings of Petrozavodsk State University*, 2010, no. 5, p. 36–40. (In Russian.)

20. Troitskaya O. N., Bezumova O. L., Shirikova T. S. Konkurs zadach po kiberbezopasnosti kak sredstvo podgotovki shkol'nikov k bezopasnomu povedeniyu v kiberprostranstve [Cybersecurity challenge competition as a means of preparing students for safe behavior in cyberspace]. *Aktual'nye problemy metodiki obucheniya informatike i matematike v sovremennoj shkole. Mezhdunarodnaya nauchno-prakticheskaya internet-konferentsiya* [Actual problems of teaching computer science and mathematics in a modern school. Proc. Int. Scientific and Practical Internet Conf.]. (In Russian.) Available at: <http://news.scienceland.ru/2019/04/23/konkurs-zadach-po-kiberbezopasnosti-k/>

НОВОСТИ

В 41 российском вузе открываются «Точки кипения»

19 октября 2019 года в 41 вузе России открываются «Точки кипения». Что это такое? Пространства коллективной работы, воспользоваться которыми смогут ученые, бизнесмены, госслужащие, общественные деятели, студенты. Здесь они будут делиться опытом, итогами работы, прорабатывать новые модели развития и сотрудничества — «кипеть идеями».

— Сегодня мы наблюдаем, как формируется запрос общества на дополнительные компетенции, современные образовательные программы, — сообщил министр науки и высшего образования РФ М. М. Котюков. — Университеты должны активно участвовать в запуске новых моделей обучения, которые можно получить в разных формах. «Точки кипения» как раз могут стать площадками для апробации таких моделей, для обмена лучшими образовательными практиками между вузами.

По мнению Котюкова, вузы с помощью новой инициативы могут задавать новые стандарты городской среды, технологий и досуга молодежи.

Чем займутся на «точках»? Основная работа, конечно, — это обмен образовательными практиками, запуск сетевого «акселератора», внедрение в учебную деятельность современных цифровых технологий. Студенты и преподаватели получают доступ к цифровой платформе Университета Национальной технологической инициативы «20.35», а также к различным его сервисам, работающим на базе искусственного интеллекта.

— Мы надеемся, что каждый университет сможет использовать «Точку кипения» не только как дополнительное пространство для проведения мероприятий, но и как сервис для формирования у каждого студента новой образовательной траектории, — прокомментировал старт проекта специальный представитель президента РФ по вопросам цифрового и технологического развития Д. Н. Песков. — В 2020 году мы ставим себе задачу «загрузить» сеть «точек» качественными мероприятиями.

(По материалам «Российской газеты»)