здоровья (аутисты, ДЦП и др.) различных возрастных групп (с 2 по 9 класс). Следует отметить, что погружение студентов-будущих педагогов в непосредственное общение с детьми с различными нарушениями зрения, с их родителями и педагогами является одним из мощных стимулов к дальнейшему развитию навыков softskils и педагогического потенциала будущих специалистов.

Данная серия мероприятий отличалась высоким уровнем включения будущих педагогов в организационные вопросы социальных проектов. Они вместе с руководителями проектов разрабатывали план фестивалей, готовили раздаточные материалы, продумывали мини-квесты по выставочным зонам, собирали демонстрационный материал (роботов, 3d модели и др.).

Во время проведения фестивалей студенты максимально быстро включались в решение возникших педагогических ситуаций, например, когда к студенты, отвечающему за демонстрацию робота Ботли в сопровождении тьютора подошла абсолютно слепая ученица школы-интерната. Будущий педагог сориентировался на возможности коммуникации с учеником посредством сопровождающего тьютора, затем самостоятельно вел диалог со слепой девочкой, посредством включения тактильных рецепторов обучающейся.

И во время подготовки мероприятия у студентов и во время его проведения у них формировались такие навыки как критическое мышление; креативность; коммуникация; координация, которые были реализованы на примере образовательных активностей.

Подводя итоги данных мероприятий, студенты отмечали, что они с огромным удовольствием работали с детьми с ОВЗ. Студенты данной группы сплотились, сдружились, они научились совместной организации педагогических активностей.

Литература

1. Ананьева, Т. Десять компетенций, которые будут востребованы в 2020 году [Электронный ресурс]. Режим доступа: http://www.tananyeva.com/single-post/ (Дата обращения: 11.02.2017).
2. Ивонина А.И., Чуланова О.Л., Давлетшина Ю.М. Современные направления теоретических и методических разработок в области управления: роль soft-skills и hardskills в профессиональном и карьерном развитии сотрудников // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №1 (2017) http://naukovedenie.ru/PDF/90EVN117.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ. КиберЛенинка: https://cyberleninka.ru/article/n/sovremennye-napravleniya-teoreticheskih-i-metodicheskih-razrabotok-v-oblasti-upravleniya-rol-soft-skills-i-hard-skills-v-professionalnom.
3. Данилова Е. Что такое обучение 4К, зачем оно вашему ребенку и где учиться по такой системе // Блог МЭЛ https://mel.fm/blog/yekaterina-danilova/3492-chto-takoye-obucheniye-4k-zachem-ono-vashemu-rebenku-i-gde-uchitsya-po-takoy-sisteme?utm_source=fb&utm_medium=share

ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СОВРЕМЕННЫХ ИНЖЕНЕРНЫХ СПЕЦИАЛЬНОСТЕЙ

Асмыкович И.К. (asmik@tut.by), Ловенецкая Е.И. (e_blinova@mail.ru)

Белорусский государственный технологический университет (БГТУ), г. Минск

Аннотация

Работа посвящена анализу содержания, методического обеспечения и использования инфорационных технологий при изучении курса «Математические основы криптографии» для студентов специальности «Программное обеспечение информационной безопасности мобильных систем».. Подчеркивается необходимость включения в курс основных понятий и алгоритмов теории чисел, алгебраических структур, включая группы точек эллиптических кривых над конечными полями.Отмечена возможность научно-исследовательской работы студентов по данной тематике, перспективы расширения программы курса с учетом новейших достижений в криптографии. Обсуждаются возможности использования системы дистанционного обучения для методического обеспечения такой динамично изменяющейся дисциплины, какой в настоящее время является курс «Математические основы криптографии».

Бурное развитие информационных технологий, их стремительное внедрение во все сферы жизни общества породило в начале XXI века огромный спрос на специалистов IT-профиля.Одной из

важнейших дисциплин для таких специалистов является математика[1,2], «Математику уже затем учить надо, что она ум в порядок приводит» говорил М.В. Ломоносов..Программы подготовки по математике для студентов этих специальностей должны отличаться от традиционных программ для технических университетов с некоторым сокращением разделов непрерывной и увеличением доли дискретной математики. Это соотвествует фразе К.Ф. Гаусса «Математика — царица наук, арифметика — царица математики.»

Учитывая вовлеченность в сферу современной практической криптографии и защиты информации теоретико-числовых и алгебраических структур, мы включили в программу дисциплины «Математические основы криптографии» следующие разделы: элементы теории дифантовых уравнений и модульной арифметики,.основныеалгебраические структуры, поля Галуа, эллиптические кривые над конечными полями..

Первый раздел включает теорию делимости целых чисел, сравнения и классы вычетов, алгоритм Евклида для нахождения НОД целых чисел и решения линейных сравнений, свойства функции Эйлера, теорему Эйлера, понятие о первообразных корнях и индексах (дискретных логарифмах) в классах вычетов, применение символов Лежандра и Якоби для проверки разрешимости квадратичных сравнений. Дается представление о математических задачах факторизации целых чисел и дискретного логарифмирования, трудноразрешимость которых лежит в основе современных криптосистем с открытым ключом.

В разделе «Алгебраические структуры» рассматриваются группы, кольца, поля, дается понятие о теории делимости в кольце и о факториальных кольцах, достаточно подробно изучаются свойства кольца многочленов над полем, в частности, над конечным полем Zp, обсуждаются понятия и свойства неприводимых многочленов, применимость алгоритма Евклида для нахождения НОД многочленов.

Третий раздел посвящен описанию полей Галуа, т. е. полей конечного порядка. Обсуждаются различные способы построения таких структур и описания их элементов, дается понятие об изоморфизме полей одного порядка, упоминаются существующие алгоритмы дискретного логарифмирования в конечных полях.

В разделе «Эллиптические кривые» описываются правила сложения элементов в группах точек эллиптических кривых над конечными полями, что иллюстрируется с помощью аналогичных кривых над полем действительных чисел. Кроме этого, обсуждается задача дискретного логарифмирования в группе точек эллиптической кривой над конечным полем.

Необходимость обеспечения курса учебно-методической литературой и отсутствие подходящих пособий, освещающих все перечисленные вопросы на доступном для студентов технических вузов уровне, привели к созданию электронного учебно-методического комплекса (ЭУМК) по дисциплине [3]. ЭУМК «Математические основы криптографии» представляет собой один pdf-документ, доступный студентам через систему дистанционного обучения (СДО) БГТУ [3] . Используя панель навигации, можно видеть всю структуру документа и перемещаться по его разделам. ЭУМК имеет четыре раздела: в теоретическом разделе представлены тесты лекций, содержание которых можно видеть ; практический раздел объединяет материалы для проведения практических занятий и выполнения индивидуальных расчетных заданий по теории чисел и теории полей Галуа; раздел контроля знаний содержит материалы для текущей и итоговой аттестации, а именно примерные варианты контрольных работ и перечень теоретических вопросов для подготовки к зачету по дисциплине.

Наличие ЭУМК вносит коррективы также и в процесс чтения лекций. Появляется возможность более детального обсуждения наиболее значимых моментов и краткого упоминания остального, поскольку нет необходимости записывать подробно всю информацию. Современная молодежь, привыкшая к постоянному использованию всевозможных гаджетов и получению ответов на любые вопросы из интернета в режиме реального времени, вообще не стремится вести полноценный конспект лекций. Однако приходится констатировать, что для незаинтересованного студента и наличие ЭУМК не способствует формированию целостного восприятия изучаемого курса.

Бурное развитие криптографических алгоритмов, использующих теоретико-числовые и алгебраические структуры, открывает заинтересованным студентам широкие возможности для изучения различных существующих методов и пробы своих сил в научно-исследовательской работе[4,5].

Необходимость методического обеспечения столь динамично меняющегося курса весьма удачно реализуется с использованием системы дистанционного обучения [2,3], где имеется возможность своевременно вносить изменения в представленные материалы. На наш взгляд, основной функцией дистанционных курсов, включаемых как часть традиционных учебных курсов, является именно предоставление студентам хорошо структурированной тщательно отобранной информации, необходимой и достаточной для изучения соответствующей дисциплины, что обеспечивает качественную основу и руководство для освоения предмета.

Литература

1. Асмыкович И.К., Борковская И.М., Пыжкова О.Н. О роли математики в формировании творческих навыков студентов технических университетов НауковийвісникЛьотноїакадемії. Серія: Педагогічні науки. Збірникнауковихпраць / Гол.ред. Т.С. Плачинда. Кропивницький: ЛАНАУ, 2019. Вип. 5.. С. 29 – 33
2. Асмыкович И.К. Реалии и перспективы дистанционного обучения математике в технических университетах // Научно-методическое издание Материалы XXIX международной конференции «Современные информационные технологии в образовании» 26июня 2018 г. Троицк – Москва С. 451 – 452.
3. Ловенецкая Е.И., Бочило Н.В. Первые результаты использования систем дистанционного обучения в учебном процессе кафедры высшей математики // Высшее техническое образование. Минск: БГТУ, 2018. Т. 2, №1. С. 90-94.
4. Лашкевич Е.М., Ковалевич Д.А. Векторная схема разделения секрета// 69-я научно-техническая конференция учащихся, студентов и магистрантов: сб. науч. работ : в 4-х ч. – Минск : БГТУ, 2018. – Ч. 4. с.286 – 288
5. Марчук К.С., Использование теории групп точек на эллиптической кривой для создания электронной подписи // Молодость. Интеллект. Инициатива: материалы VII Межд. научно-практ.конф. студентов и магистрантов, Витебск, 18 апреля 2019 г. / Витеб. гос. ун-т ; редкол.: И.М. Прищепа (гл. ред.) [и др.]. – Витебск : ВГУ имени П.М. Машерова, 2019. с.27 – 28.

ПРИМЕНЕНИЕ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ В УЧЕБНОМ ПРОЦЕССЕ ГБПОУ НАВАШИНСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ, КАК ОДИН ИЗ МЕТОДОВ ПОВЫШЕНИЕ КАЧЕСТВА, ДОСТУПНОСТИ И ВОСТРЕБОВАННОСТИ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ

Бирюкова Л.С. (nsmt-birukova@yandex.ru)

Государственное бюджетное профессиональное образовательное учреждение «Навашинский политехнический техникум», городской округ Навашинский

Аннотация

В данной работе представлен опыт применения электронного обучения и дистанционных образовательных технологий в образовательном процессе ГБПОУ Навашинский политехнический техникум» .

Под электронным обучением (ЭО) понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников.

Под дистанционными образовательными технологиями (ДОТ) понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Целью применения электронного обучения и дистанционных образовательных технологий в учебном процессе государственного бюджетного профессионального образовательного учреждения «Навашинский политехнический техникум» является повышение качества, доступности и востребованности образовательных услуг.