МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

УТВЕРЖДАЮ

Проректор по учебной работе

_____/Г.Х. Шарипзянова/

«01» марта 2021 г.

Дополнительная профессиональная программа (повышение квалификации)

«Обучение дисциплине «Математические основы шифрования» учащихся ИТ-классов»

Авторы-разработчики
Тимошина Елена Сергеевна

Либерман Даниил Александрович

Утверждено на заседании учебно-методического совета
инженерной школы (факультета)
Протокол № 6 от 25.02.2021

Декан инженерной школы (факультета) _____/Н.А. Кобиашвили/

Москва - 2021 г.

Аннотация

Практико-ориентированный курс «Математические основы шифрования» направлен на обеспечение кадровых условий предпрофессионального инженерного образования в рамках проекта «Инженерный класс в московской школе» и « ИТ-класс в московской школе». Слушатели курсов познакомятся со схемами проведения практической части предпрофессионального экзамена. Будут представлены методические рекомендации по подготовке обучающихся инженерных классов к предпрофессиональному экзамену. В рамках курса будут рассмотрены фундаментальные теоретические и практические задачи в таких областях информатики как математические основы шифрования, информационная безопасность, технологии защиты данных, основы криптографии. Примеры включают задания, сопроводительные тексты и руководства, варианты тестов и критерии оценки. Программа предусматривает выполнение слушателями ряда практических работ, раскрывающих практические задания предпрофессионального экзамена. Слушателям будут предложены методические рекомендации по подготовке обучающихся инженерных классов и ИТ-классов к предпрофессиональному экзамену.

Раздел 1. Характеристика программы

1.1. Цель реализации программы

Целью программы является совершенствование профессиональных компетенций, обучающихся в области подготовки, учащихся к практической части предпрофессионального экзамена по ряду направлений: математические основы шифрования; информационная безопасность; технологии защиты данных; основы криптографии.

Совершенствуемые компетенции

№ п/п	Компетенция	Направление подготовки 44.03.01, Педагогическое образование
		Бакалавриат
		Код компетенции
1	Способен осуществлять контроль и оценку формирования результатов образования обучающихся, выявлять и корректировать трудности в обучении	ОПК-5
3	Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК-8

1.2. Планируемые результаты обучения

№ п/п	Знания- умения	Направление подготовки 44.03.01,
		Педагогическое образование
		Бакалавриат
		Код компетенции
1	**Знать:** Критерии оценки знаний и умений учащихся на основе решения инженерных задач по направлениям: «математические основы шифрования»; «информационная безопасность»; «технологии защиты данных»; «основы криптографии». . **Уметь:** Разрабатывать систему объективной оценки знаний изучаемого учащимися теоретического и практического материала. Решать практические задачи в рамках подготовки учащихся к предпрофессиональному экзамену по направлениям: «математические основы шифрования»; «информационная безопасность»; «технологии защиты данных»; «основы криптографии».	ОПК-5
3	**Знать:** Область информатики, относящуюся к информационной безопасности; технологиям защиты данных; криптографии. **Уметь:**	ОПК-8

	Решать задачи администратора систем информационной безопасности, относящиеся к шифрованию, криптографии и защите данных.	

1.3. Категория обучающихся (слушателей): уровень образования - ВО, направление подготовки - «Педагогическое образование», область профессиональной деятельности: обучение информатике в инженерных и ИТ-классах.

1.4. Форма обучения: заочная с применением дистанционных образовательных технологий.

1.5. Режим занятий: Круглосуточный доступ к системе дистанционного обучения, дистанционные очные консультации 2 ак. ч. один раз в неделю.

1.6. Трудоемкость программы. 18 ак. ч.

Раздел 2. *Содержание программы*

2.1. Учебный (тематический) план

№	Наименование	Всего	В том числе		
п/п	Разделов	час.	Лекции	Практич занятия	Формы контроля
0.Введение в курс					
0.1	Вводная лекция. Преподавание курса «Математические основы шифрования» Направленность курса. Особенности преподавания курса. Методы мотивации учащихся.	1	1		тест
1. Введение в криптографию					
1.1	Введение в криптографию. Вводные знания о криптографии, алгоритмах шифрования. Знакомство с терминами. История шифрования. Первые шифраторы.	1	1		тест
1.2	Знакомство с шифрами. Исторические примеры простых шифров. Шифр сдвига. Расшифровывание. Криптоанализ.	1	1		тест
1.3	3. Важные исторические шифры. Разбор исторических шифров. Шифр замены и шифр Рихарда Зорге.	1		1	тест
2. Математические основы шифрования					
2.1	Математическое описание шифра замены. Математическое описание перестановки букв в открытом	1		1	тест

	тексте, используемое в шифре замены.				
2.2	Шифр Вернама. Подробный разбор шифра Вернама. Ключ. Расшифрование. Криптоанализ.	1		1	тест
2.3	Абсолютно стойкий шифр. Разбор результатов исследований К. Шеннона о существовании абсолютно стойкого шифра.	1	1		тест
2.4	Шифровальные машины. Принципы работы и сравнение шифровальных машин Энигма, Сигаба, Purple.	1	1		тест
3. Криптографические ключи					
3.1	Симметричное и асимметричное шифрование. Вопросы распределения ключей. Специальная терминология. Сравнение алгоритмов симметричного и асимметричного шифрования.	1	1		тест
3.2	Криптостойкость ключа. Что такое криптостойкость ключа и от чего она зависит. Возможные атаки по шифротексту.	1		1	тест
3.3	Алгоритмы распределения ключей. Разбор методов надежного и защищенного от перехвата способов обмена ключами. Протокол широкоротой лягушки.	1		1	тест
3.4	Инфраструктура открытых ключей (PKI)	1	1		тест
	Знакомство с PKI (Public Key Infrastructure). Изучение протокола аутентификации Kerberos. Важность выбора метода распределения ключей.				
4. Современные шифры					
4.1	Сеть Фейстеля. Разбор метода блочного шифрования, разработанный Хорстом Фейстелем, как основа современных криптографических протоколов.	1	1		тест
4.2	Современные отечественные шифры. Знакомство с новыми направлениями в криптографии на примере отечественного шифра ГОСТ 28147—89, «Кузнечик».	1	1		тест
4.3	Современные зарубежные шифры. Что такое, как работают и в чем разница между 3DES, AES, Blowfish, IDEA, Threefish от Брюса Шнайера.	1	1		тест
4.5	Электронная подпись. Виды электронных подписей, как они работают и как их использовать.	1	1		тест

4.6	Квантовая криптография. Что такое квантовая криптография, где используется и как помогает в распределении секретных ключей, генерации случайных чисел и электронной подписи.	1	1		тест
5. Заключение					
5.1	Итоговое тестирование	1		1	тест
	Итого:	**18**	**12**	**6**	**18**

Раздел 3. «Формы аттестации и оценочные материалы»

3.1. Текущий контроль:

Текущий контроль осуществляется за счет проверки самостоятельных работ слушателей и на основании результатов промежуточного тестирования.

Теоретические знания проверяются с помощью контрольных тестов.

Тест 1. Методика оценивания теоретического материала курса.

- Дистанционное прохождение всех тестов теоретического материала (прохождение соответствующего теста к каждому из 16 уроков для учащихся).

Тест 2. Методика разработки системы оценивания.

1. Назовите основные подходы к построению системы оценивания знаний и умений учащихся на основе курса «Математических основ шифрования».
2. Как строится шкала оценки практических умений по процессу решения инженерной задачи из курса «математические основы шифрования»?
3. Как строится шкала оценки умений по письменному оформлению результатов построения проекта с использованием технологий защиты данных?

Сформированные навыки проверяются за счет выполнения всех практических работ.
Требования к выполнению практических работ:

Сценарий занятий по математическим основам шифрования должен состоять из:

- исходного текста задания (с указанием ПО, которое необходимо для решения задачи);
- нормативного решения задачи;
- последовательности исполнений действий учащихся, приводящей к решению задачи администрирования;
- пошагового описания действий учителя и учеников в ходе занятия;
- варианты способов самоконтроля обучающихся по пройденной теме.

Критерии объективной оценки знаний и умений учащихся должны учитывать:

- Оценку процесса решения задачи администрирования;
- Оценку оформления результатов решения;

По каждому пункту выставляется от 0 до 3 баллов:

0 баллов – данный элемент не представлен;
1 балл – дано частичное описание или в общих чертах;
2 балла – описание недостаточно, содержит некоторые обоснования;
3 балла – описание полное, обоснованное, логичное.

3.2. Итоговая аттестация:

Итоговая аттестация проводится на основании совокупности, выполненных на положительную оценку работ и результатов промежуточного тестирования.

Раздел 4. «Организационно-педагогические условия реализации программы»

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

1. Электронное учебное пособие в МЭШ «Математические основы шифрования»;
2. Сценарии уроков в МЭШ серия «Математические основы шифрования»;
3. Учебник Введение в криптографию под редакцией В.В.Ященко. Издание четвертое, дополненное. Москва, издательство МЦНМО, 2012. ISBN 978-5-4439-0026-1
4. Оценочные средства – контрольные тесты в МЭШ – электронное учебное пособие в МЭШ «Математические основы шифрования» и в сценарии уроков в МЭШ серия «Математические основы шифрования»;

4.2. Материально-технические условия реализации программы

Аудитория с возможностью демонстрации презентаций и организации групповой работы. Лаборатория для практической отработки инженерных задач предпрофессионального экзамена.

Работа на платформе https://lms.mospolytech.ru/ (для дистанционной формы обучения или с частичным применением дистанционной формы).