Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

Университетский лицей № 1523
Предуниверситария НИЯУ МИФИ

Утверждаю
Руководитель Университетского лицея
№1523 Предуниверситария НИЯУ МИФИ

_____А.Б. Пастухов
«_27_» _августа_____2021г.

РАБОЧАЯ ПРОГРАММА
Информационная безопасность
10-11 класс

Москва

Рабочая программа
среднего общего образования по дисциплине
Информационная безопасность

Пояснительная записка

Данная программе предназначена для организации процесса обучения информационной безопасности в 10-11 классах Предуниверситария НИЯУ МИФИ.

Программа опирается на широкие фундаментальные и методические наработки российской высшей школы в области обучения начальным профессиональным навыкам в ИТ-сфере. Программа направлена на формирование у школьников начальных практических навыков в области информационной безопасности через изучения основ сетевого и системного администрирования, криптографии, стеганографии, основных способов защиты web- и мобильных приложений.

С учётом быстрорастущих потребностей рынка, широкого проникновения в повседневную жизнь информационных технологий, формируется значительный спрос на специалистов, которые способны решать различные цифровые задачи. Данный запрос наиболее явно сформулирован в Национальной технологической инициативе. Одной из основных задач такого типа является задача обеспечения информационной безопасности. Изучение информационной безопасности требует изучение информатики и математики в качестве базовых предметов, а также дополняет их изучение специфичными для себя навыками и знаниями.

Обучение информационной безопасности позволяет учащемуся с раннего возраста получить начальные профессиональные навыки, на практике понять, что входит в работу ИТ-специалиста и совершить осознанный выбор при поступлении в университет. Более того, какой бы выбор не был совершён в итоге учащимся, знание информационной безопасности лишь усилит его привлекательность на рынке труда в любой области.

Обучение подразумевает постоянно участие в практических мероприятиях и соревнованиях, характерных для области информационной безопасности.

Общая характеристика учебного предмета

Начальные профессиональные навыки являются обязательными элементами подготовки школьников, в том числе к поступлению в университет. Обучение информационной безопасности в средней школе направлено на достижение следующих целей:

1) В направлении личностного развития:
- развитие начальных профессиональных навыков в области информационной безопасности и информационных технологий;
- развитие логического и критического мышления, способности к умственному эксперименту;
- развитие алгоритмической культуры и интуиции;
- воспитание качеств личности, обеспечивающих социальную мобильность, способность принимать самостоятельные решения;
- формирование качеств мышления, необходимых для адаптации в современном информационном обществе;
- развитие критичности мышления на уровне, необходимом для будущей профессиональной деятельности, а также последующего обучения в высшей школе;
- формирование этических принципов в области использования информационных технологий

2) В метапредметном направлении
- формирование представлений об информационной безопасности, как о необходимом элементе любой деятельности;
- развитие представлений о математике как форме описания и методе познания действительности, создание условий для приобретения первоначального опыта математического моделирования
- формирование общих способов интеллектуальной деятельности, характерных для математики и являющихся основой познавательной культуры, значимой для различных сфер человеческой деятельности;
- развитие навыков практического программирования в конкретных областях;

3) В предметном направлении
- овладения навыками программирования на уровне достаточном для решения практических задач в области информационной безопасности;
- создание фундамента для математического развития, формирования механизмов мышления, характерных для математической деятельности;

Содержание подготовки по информационной безопасности в средней школе формируется на основании фундаментального математического образования, навыков программирования, а также практического опыта

специалистов из индустрии информационной безопасности. В программе оно представлено в виде совокупности содержательных разделов, конкретизирующих соответствующие блоки информационной безопасности применительно для изучения в средней школе.

Содержание подготовки по информационной безопасности включает в себя следующие разделы: введение, определение базовых качеств, основы ИБ, изучение правового поля и области применения навыков, основы тестирования на проникновение, практика использования прикладного ПО для тестирования.

В рамках целостной подготовки в области информационной безопасности через освоение указанных выше разделов решаются следующие задачи:

- формирование системного представления об области информационной безопасности;
- выработка практических навыков, достаточных для решения стандартных и нестандартных задач в области информационной безопасности.

Требование к результатам обучения и освоению содержания курса

Изучение информационной безопасности в средней школе дает возможность обучающимся достичь следующих результатов развития:

1) в личностном направлении:
- получить практические навыки работы в области информационных технологий и информационной безопасности;
- развить критическое мышление и работы с логическими объектами;
- получить представление об информационной безопасности с практической и теоретической точек зрения;

2) в метапредметном направлении:
- получить представление о том, как применять технологии из области информационной безопасности в высокотехнологично сфере;
- сформировать умение использовать алгоритмические схемы для реализации собственных проектов;
- сформировать умение выдвигать гипотезы при решении учебных задач и понимать необходимость их проверки;
- сформировать умение применять индуктивные и дедуктивные способы рассуждений, видеть различные стратегии решения задач;
- сформировать умение самостоятельно ставить цели, выбирать и создавать алгоритмы для решения учебных математических проблем

3) в предметном направлении:
- овладеть базовым понятийным аппаратом в области информационных технологий;
- овладеть соответствующим математическим аппретом для решения задач в области информационной безопасности;
- получить практические навыки в области информационной безопасности;
- получить опыт участия в соревнованиях в области практической информационной безопасности.

Место учебного предмета в учебном плане образовательного учреждения

Согласно учебному плану ИТ-классов Предуниверситария НИЯУ МИФИ на изучение информационной безопасности отводится от 1 до 2 лет в зависимости от выбора обучающегося. Количество часов на изучение представлено в таблице:

Класс	Предмет	Количество учебных часов в неделю	Общее количество учебных часов за год обучения
10	Основы информационной безопасности	2	68
11	Информационная безопасность	2	68

Содержание предмета основы информационной безопасности

Введение, определение базовых качеств (4 часов)

Определение текущего уровня навыков и знаний.

Основы ИБ, изучение правового поля и области применения навыков (8 часов)

Нормативное регулирование в сфере ИБ. Основные понятия ИБ. Области развития в сфере ИБ.

Основы тестирования на проникновение. (28 часов)

Методология тестирования на проникновение. Основные цели, задачи и этапы. Разбор OWASP TOP 10 с углубление в технологии и области применения.

Практика использования прикладного ПО для тестирования. (28 часов)

Разбор OWASP TOP 10 и используемого ПО для каждого вида уязвимостей. Применение практических навыков для решения олимпиадных заданий.

Содержание предмета информационная безопасность

Введение, определение базовых качеств (4 часов)

Определение текущего уровня навыков и знаний.

Основы ИБ, изучение правового поля и области применения навыков (8 часов)

Нормативное регулирование в сфере ИБ. Основные понятия ИБ. Области развития в сфере ИБ.

Продвинутое тестирования на проникновение. (28 часов)

Методология тестирования на проникновение. Разбор OWASP TOP 10 с углубление в технологии и области применения.

Практика использования прикладного ПО для тестирования. (28 часов)

Разбор OWASP TOP 10 и используемого ПО для каждого вида уязвимостей. Применение практических навыков для решения олимпиадных заданий.

Учебно-методическое и материально-техническое обеспечение образовательного процесса

Учебно-методическое обеспечение

1) https://edu.cyberschool.msu.ru/ (сайт)

2) https://owasp.org (сайт)

3) https://tryhackme.com/ (сайт)

4) https://picoctf.org/ (сайт)

5) https://overthewire.org/ (сайт)

Технические средства обучения

- мультимедийный компьютер;
- мультимедиапроектор;
- интерактивная доска.

Информационные средства

- соответствующие программные средства для решения практических задач;
- база материалов для самостоятельного изучения.

Планируемые результаты изучения учебного предмета

Результаты обучения представлены в Требованиях к уровню подготовки и задают систему итоговых результатов обучения, которых должны достигать все учащиеся, оканчивающие основную школу, и достижение которых является обязательным условием положительной аттестации ученика за курс основной школы. Эти требования структурированы по трем компонентам: «знать/понимать», «уметь», «использовать приобретенные знания и умения в практической деятельности и повседневной жизни». При этом последние два компонента представлены отдельно по каждому из разделов содержания.

В результате изучения курса информационной безопасности ученик должен

знать/понимать

1) Основы ИБ

2) Основные направления ИБ

3) Базовые принципы анализа защищенности

4) Основные инструменты для проведения анализа защищенности

уметь

1) Оценивать безопасность информационных систем

2) Оценивать уровень защищенности информационных систем

3) Программировать на языке Python для написания базовых скриптов

использовать приобретенные знания и умения в практической деятельности и повседневной жизни для

1) Защиты своей личной информации

2) Повышения уровня знаний для обеспечения собственной безопасности в информационном поле

Формы и методы контроля

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Содержание и объем материала, подлежащего проверке, определяется программой. При проверке усвоения материала нужно выявлять полноту, прочность усвоения учащимися теории и умения применять ее на практике в знакомых и незнакомых ситуациях.

Основными формами проверки знаний и умений учащихся по информационной безопасности являются практическое решение задач на время и устный опрос.

Рекомендации по оценке знаний и умений учащихся

Опираясь на эти рекомендации, учитель оценивает знания и умения учащихся с учетом их индивидуальных особенностей.

При оценке ответов учитель в первую очередь учитывает показанные учащимися знания и умения. Оценка зависит также от наличия и характера погрешностей, допущенных учащимися. Среди погрешностей выделяются ошибки и недочеты. Погрешность считается ошибкой, если она свидетельствует о том, что ученик не овладел основными знаниями, умениями, указанными в программе. К недочетам относятся погрешности, свидетельствующие о недостаточно полном или недостаточно прочном усвоении основных знаний и умений или об отсутствии знаний, не считающихся в программе основными. К недочетам относятся: нерациональное решение, описки, недостаточность или отсутствие пояснений, обоснований в решениях.

Недочетами также считаются: погрешности, которые не привели к искажению смысла полученного учеником задания или способа его выполнения; неаккуратно и небрежно выполненный программный код. Граница между ошибками и недочетами является в некоторой степени условной. При одних обстоятельствах допущенная учащимися погрешность может рассматриваться учителем как ошибка, в другое время и при других обстоятельствах — как недочет.

Оценка ответа проводится по пятибалльной системе, т.е. за ответ выставляется одна из отметок: 1 (плохо), 2 (неудовлетворительно), 3(удовлетворительно), 4 (хорошо), 5 (отлично).

- Ответ/решение оценивается отметкой «5», если ученик полно раскрыл содержание материала в объеме, предусмотренном программой, а также проявил творческие способности в процессе поиска ответа.
- Ответ оценивается отметкой «4», если он удовлетворяет в основном требованиям на оценку «5», но при этом имеет ряд недостатков, в первую очередь связанных с отказом творчески подойти к решению задачи, если это возможно, а также в случае небрежного выполнения поставленного задания.
- Ответ оценивается отметкой «3», если он удовлетворяет оценки «4», но при этом отсутствует практическое понимание способа получения ответа. Допущены ошибки, указывающие на то, что ученик частично не понимает содержание используемой технологии.
- Ответ оценивается отметкой «2» если обучающийся не может получить ответ на поставленную задачу или не понимает полностью содержание используемой технологии.
- Ответ оценивается отметкой «1» если обучающий не может решить задачу в принципе, допускает неэтичное поведение в процессе решения задачи.