|  |  |
| --- | --- |
| **Национальный**  **исследовательский университет**  **«Высшая школа экономики»**  **Лицей** | **Приложение 414**  УТВЕРЖДЕНО  педагогическим советом  Лицея НИУ ВШЭ  протокол №11 от 23.08.2021г |

**Рабочая программа учебного предмета (курса)**

**«Криптография и информационная безопасность»**

**10 класс**

**Автор:**

Воронцова Татьяна Дмитриевна

**1.Планируемые результаты освоения учебного предмета**

В соответствии с Федеральным государственным образовательным стандартом среднего общего образования (10-11 кл.) освоение учебного предмета «Криптография и информационная безопасность» предполагает достижение личностных, метапредметных и предметных результатов.

Личностные результаты

* сформированность познавательных интересов, интеллектуальных и творческих способностей;
* развитие интеллектуальных и творческих способностей на основе опыта самостоятельного приобретения новых знаний, анализа и оценки новой информации по информационной безопасности;
* сознательное самоопределение ученика относительно профиля дальнейшего обучения или профессиональной деятельности;
* мотивация образовательной деятельности учащихся как основы саморазвития и совершенствования личности.

Метапредметные результаты

Регулятивные универсальные учебные действия

* целеполагание как постановка учебной задачи на основе соотнесения того, что уже известно и усвоено учащимися, и того, что еще неизвестно;
* умение самостоятельно планировать пути достижения целей, в том числе альтернативные, осознанно выбирать наиболее эффективные способы решения учебных, познавательных и проектных задач;
* умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата, определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией и в случае получения результата, отличного от ожидаемого;
* умение оценивать правильность выполнения учебной задачи, собственные возможности ее решения;
* владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности.

Познавательные универсальные учебные действия

* умение устанавливать аналогии, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;
* владение основными алгоритмами решения задач криптоанализа, различными методами и инструментарием;

Коммуникативные универсальные учебные действия

* умение организовывать учебное сотрудничество и совместную деятельность с преподавателем и сверстниками;
* умение работать индивидуально и в группе: находить общее решение на основе согласования позиций;
* умение формулировать, аргументировать и отстаивать свое мнение;
* умение осознанно использовать речевые средства в соответствии с задачей коммуникации для выражения своих мыслей, планирования и регуляции своей деятельности, проговаривать вслух решение задачи;

**Предметные результаты**

* Сформированность у учеников общего представления о видах и областях применения методов и средств криптографии и информационной безопасности;
* Сформированность у учеников общего представления о методах анализа простейших шифров;
* Сформированность у учеников базовых навыков криптоанализа простейших шифров;
* Сформированность у учеников общего представления о методах кодирования.

**2.Содержание учебного предмета**

Изучение курса по выбору «Криптография и информационная безопасность» способствует повышению уровня грамотности школьника в сфере информационных технологий и присущих данной сфере деятельности угроз. Обучение базовым принципам противодействия данным угрозам способствует повышению уровня личной ответственности, организованности школьника и его заинтересованности в изучении новейших информационных технологий.

Курс по выбору «Криптография и информационная безопасность» структурируется на основе различных аспектов информационной безопасности: криптографические средства ИБ, техническая защита информации, разработка защищенного ПО, обнаружение компьютерных атак. Курс по выбору Криптография и информационная безопасность предназначен для учащихся 10 классов, рассчитан на 78 часов.

**Тема 1. Информационная безопасность**

Информация, ее свойства, виды. Информационные процессы. Понятие информационной безопасности. Модель объекта информатизации. Модель уязвимости. Модель угрозы. Модель нарушителя. Модель атаки. Построение политики безопасности.

**Тема 2. Основы теории информации**

Базовые элементы теории вероятности: понятие вероятности, математическое ожидание, дисперсия, функция распределения и плотности, условные вероятности.

Количество информации. Энтропия источника информации: понятие энтропии, применение, расчет.

**Тема 3. Кодирование**

Преобразования информации. Канал связи. Кодирование, его виды: физическое, канальное, кодирование источника, криптография.

Матрицы, назначение, арифметические действия. Допустимые операции. Ранг, определитель. Применение для решения систем линейных уравнений.

Назначение кода, его параметры: скорость кода, коэффициент сжатия. Информативность, потери при кодировании. Однозначность восстановления информации, условие Фано.

Энтропийное кодирование: назначение, виды, алгоритмы (код Хаффмана, код Шеннона-Фано, код Шеннона). Оптимальность сжимающего кода.

Канальное кодирование: назначение, виды, алгоритмы (код кратных повторений, код Хемминга). Минимальное расстояние кода. Корректирующая способность.

**Тема 4. Криптография**

Понятие науки, назначение, основные задачи: защита конфиденциальности, защита целостности, аутентификация, невозможность отказа от авторства.

Основные виды шифров: подстановка и перестановка.

Критерии оценивания шифров: стойкость (теоретическая, практическая, временная).

Основы теории множеств. Отображения, их виды. Математическая модель шифра. Модель шифра простой замены. Модель шифра перестановки.

Первые исторические шифры: шифр Цезаря (шифр сдвига), Атбаш, сцитала. Шифры многоалфавитной замены. Диски Альберти. Абсолютная стойкость шифров. Гаммирование. Шифр Вернама (шифр «одноразовый блокнот»). Лозунговые шифры. Книжные шифры. Коммунистические шифры.

Стеганография, ее виды

**Тема 5. Криптоанализ**

Назначение. Методы классического криптоанализа: атака по шифртексту, атака по открытому тексту, другие вариации атак.

Частотный анализ: метод, назначение, противодействие.

**Тема 6. Криптографические протоколы**

Криптографические протоколы: назначение, виды.

Основы теории групп, колец и полей: понятие группы, кольца, поля. Порядок, характеристика. Арифметические действия: поиск противоположного, сложение, умножение, деление, возведение в степень. Функция Эйлера: назначение, расчет. Примитивный элемент. Алгоритм Евклида. Диофантовы уравнения. Поиск обратного элемента.

Виды шифрования: симметричное и асимметричное. Отличие в математической модели и на практике. Понятие сеансового ключа, ключевой пары.

Протоколы генерации сеансового ключа: назначение, алгоритмы и их преимущества (протокол Диффи-Хеллмана, схема Блома с участием доверенного лица).

Протоколы асимметричного шифрования: назначение, алгоритмы и их преимущества (протокол RSA, трехэтапный протокол Шамира).

Протоколы разделения секрета: назначение, алгоритм (протокол разделения секрета по Шамиру). Пороговые схемы.

Протоколы электронно-цифровой подписи: назначение, алгоритмы и их преимущества (протокол ЭЦП RSA, схема Эль-Гамаля, протокол ЭЦП с арбитром). Понятие хеш-функции, коллизий.

Протоколы нулевого разглашения: назначение, алгоритмы (модель пещеры нулевого разглашения, протокол подбрасывания монетки по телефону, ментальные покер, задачи миллионеров-социалистов на равенство и преимущество).

**3. Тематическое планирование**

Тематическое планирование курса

«Криптография и информационная безопасность»

|  |  |  |  |
| --- | --- | --- | --- |
| № | Тема | Количество аудиторных часов | Примечание |
|  | Информационная безопасность | 8 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
|  | Основы теории информации | 8 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
|  | Кодирование | 12 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
|  | Криптография | 14 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
|  | Криптоанализ | 12 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
|  | Криптографические протоколы | 24 | Лекция и дискуссия по обозначаемой преподавателем проблематике. Практические занятия |
| **Итого:** | | 78 |  |

В воспитании обучающихся приоритетом является создание благоприятных условий для приобретения обучающимися опыта осуществления социально значимых дел:

— опыт дел, направленных на заботу о своей семье, родных и близких;

— трудовой опыт, опыт участия в производственной практике;

— опыт дел, направленных на пользу своему родному городу или селу, стране   
в целом, опыт деятельного выражения собственной гражданской позиции;

— опыт природоохранных дел;

— опыт разрешения возникающих конфликтных ситуаций в школе, дома   
или на улице;

— опыт самостоятельного приобретения новых знаний, проведения научных исследований, опыт проектной деятельности;

— опыт изучения, защиты и восстановления культурного наследия человечества, опыт создания собственных произведений культуры, опыт творческого самовыражения;

— опыт ведения здорового образа жизни и заботы о здоровье других людей;

— опыт оказания помощи окружающим, заботы о малышах или пожилых людях, волонтерский опыт;

— опыт самопознания и самоанализа, опыт социально приемлемого самовыражения и самореализации.

Выделение данного приоритета связано с особенностями обучающихся юношеского возраста: с их потребностью в жизненном самоопределении, в выборе дальнейшего жизненного пути, который открывается перед ними на пороге самостоятельной взрослой жизни.

**Учебно-методическое и материально-техническое обеспечение образовательной деятельности**

**Программно-методическое обеспечение**

1. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации: учебник для академического бакалавриата – М.: Юрайт, 2016. – 473 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. - М.: Астрель, 2007.
3. Кабанов А. С., Лось А. Б., Першаков А. С. Теоретические основы компьютерной безопасности. – М.: МГИЭМ, 2012
4. Кабанов А. С., Лось А. Б., Трунцев В. И. Основы информационной безопасности. – М.: МГИЭМ, 2012

**Материально–техническое обеспечение**

**1. Мультимедийное оборудование**

1.1 Персональный компьютер;

1.2. Экран;

1.3. Проектор;

**2. Лабораторное оборудование**

2.1 Программные эмуляторы шифровальных машин

2.2 Индикатор поля SEL SP-77/2M "Ловец"

**3. Контрольно-измерительные материалы**

4.1 Раздаточный материал для индивидуальной работы

4.2 Дидактические материалы по темам