kaspersky

Вероятность и шифрование

Рекомендации по проведению урока

kaspersky

Вероятность и шифрование

Рекомендации по проведению занятий с учащимися:

Цели урока: сформировать связи понятий теории вероятностей с шифрованием, на примере шифра простой замены.

Планируемые результаты:

Личностные: мотивация к учебной деятельности и формирование устойчивого интереса к раскрытию связей между математическими понятиями, информационными технологиями и информационной безопасностью, в том числе с шифрованием;

Предметные: раскрытие прикладного содержания теории вероятностей в рамках информационной безопасности (шифрования);

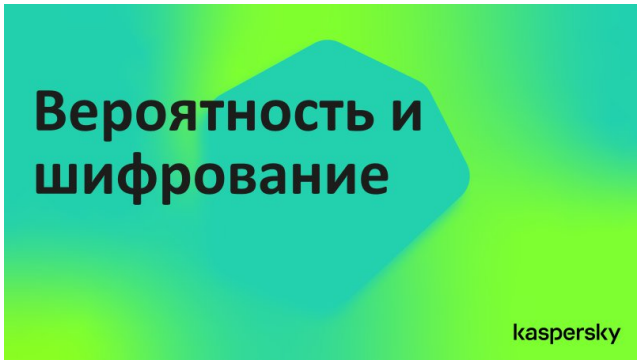
Метапредметные: формирование самостоятельности выполнения конкретной поставленной задачи, формирование навыков анализа, сравнения и обобщения, установление аналогий.

Методическое обеспечение и средства обучения:

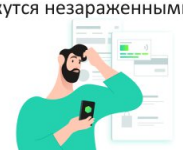
1. Материал для учителя
2. Презентация
3. Рабочие листы учащихся

Методический материал носит рекомендательный характер и учитель, принимая во внимание особенности класса, может изменять вопросы и дополнять задания.

kaspersky

Слайд	Комментарии
	**Слова учителя:** Добрый день ребята, сегодня наше занятия посвящено математическим основам, которые используются в информационной безопасности. Конкретно сегодня остановимся на понятиях и теоремах теории вероятностей. **Вопрос учащимся:** Для чего необходимо шифрование данных? Что уже известно вам о шифровании из школьного курса информатики?
	**Слова учителя:** Очень часто мы стоим перед выбором, когда каждый из вариантов одинаково важен для нас. Что же делать в такой ситуации? Бросить монету - единственное правильное решение! Миллионы людей по всему миру решают важные вопросы подбрасыванием монетки, попробуйте и вы! *Подбрасывать монетки можно по указанному адресу сайта. Следует отметить, что при увеличении количества подбрасывания, вероятность стремится к ½ = 0,5.* **Слова учителя:** Мы рассмотрели монетку, у которой возможно два варианта события, но при бросании выпадает что-то одно, то есть, выпадение орла равновероятно как и выпадение решки. И, если ставить ставки на выпадение конкретного события, то при больших количествах подбрасывания монетки, будет стремиться к ничьей.
	Так как понятие вероятность события (частота события) не является новым для учащихся старшей школы. То следует вспомнить определение вероятности события – отношение количества благоприятных событий к количеству всевозможных. Для независимых событий их совместное наступление означает умножение вероятностей, наступление хотя бы одного из данных независимых событий – сложение вероятностей. *С данными теоремами следует провести аналогию с алгеброй логикой (конъюнкция и дизъюнкция).* **Вопрос:** Как вы считаете, кто изображен на слайде и почему? *Многие узнают Блеза Паскаля из курса физики, некоторые сразу скажут, что в честь*

kaspersky

	него назвали язык программирования и что он, один из первых, кто собрал механический калькулятор, выполняющий элементарные операции. Исторически, оперировать с понятием вероятности события один из первых стал Паскаль. Один из его знакомых увлекался азартными играми и как-то поведал ему свои наблюдения о выигрыше и проигрыше в некоторых играх. Этим только разогрев интерес Паскаля к построению математической модели данного процесса. Из-за этого Паскаля считают одним из основоположников теории вероятностей, который ввел определение вероятности события.
Задачи для актуализации знаний: • На клавиатуре телефона 10 цифр, от 0 до 9. Какова вероятность того, что случайно нажатая цифра окажется четной? • Рассматриваются символьные последовательности длины 5 в шестибуквенном алфавите {У, Ч, Е, Н, И, К}. Сколько существует таких последовательностей, которые начинаются с буквы У и заканчиваются буквой К? • Пользователь владеет четырьмя методами шифрования, среди которых – шифр Цезаря. Какова вероятность, что пользователь не воспользуется данным шифрованием? kaspersky	**Задачи для актуализации знаний:** 1. Всевозможных событий 10 Благоприятных событий 5 По определению 5/10 = 0,5. 2. Если в алфавите M символов, то количество всех возможных «слов» (сообщений) длиной N равно M^N (число размещений с повторением). Первая и последняя буквы пятибуквенного слова фиксированы, значит, задача сводится к нахождению количества возможных слов длиной 3 в шестибуквенном алфавите. Их число равно 6^3 =216. *При выполнении третьего задания, следует уточнить, что шифр Цезаря – шифр простой замены, представляющий сдвиг букв алфавита на определенный шаг.* 3. Всевозможных событий 4 Благоприятных событий 3 По определению 3/4 = 0,75.
• Для создания пароля из пяти символов пользователь использовал цифры 0, 3, 4, 8 и 9. Какова вероятность подобрать установленный пароль? • Вероятность того, что загруженный файл на компьютер с неофициального источника заражен вирусом, равна 0,8. Пользователь загружает два таких файла. Найдите вероятность того, что оба файла окажутся незараженными.  kaspersky	*При выполнении четвертого задания, необходимо вспомнить, что данная задача связана с перестановками без повторений. Из n элементов будет* $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$ *перестановок.* 4. Всевозможных событий 5! = 120 Благоприятных событий 1 По определению 1/120 = 0,008(3). *Следует отметить, что решение четвертой задачи должно подтолкнуть на размышления, тяжело ли подбирать такой пароль вручную или же перебором комбинаций через генератор на компьютере. Помимо этого, как можно защитить аккаунт со*

	стороны разработчиков, если имеется только такая возможность по созданию паролю? 5. Вероятность загрузки незараженного файла равна 1-0,8 = 0,2. Так как это независимые события, то вероятности необходимо перемножить, получаем ответ 0,04. *Для независимых событий их совместное наступление означает умножение вероятностей, наступление хотя бы одного из данных независимых событий – сложение вероятностей.*
	Шифр простой замены – класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Примером могут являться шифр Цезаря – сдвиг букв алфавита на определенный шаг или ROT13 – заменяет каждую букву на парную ей из второй половины латинского алфавита, образовывая два набора по тринадцать символов. *Данные примеры иллюстрируют симметричное шифрование.* *Следует обговорить, в каком случае данные примеры шифрования актуальны.*
	**Практическое задание:** Расшифруйте текст, указав сдвиг алфавита в шифре Цезаря. **Ответы:** • **1 вариант:** Молодец, ты расшифровал! Сдвиг: 6 • **2 вариант:** Бегите, глупцы! Сдвиг: 8 • **3 вариант:** Точно шифр Цезаря! Сдвиг: 7 *Рекомендуется разбить учащихся на группы/пары и провести задание по вариантам. В рабочем листе ученика к данному заданию дана таблица алфавита, чтобы наглядно можно было сопоставить каждой букве соответствующую букву из шифротекста (перебором).*

kaspersky

Вопрос:

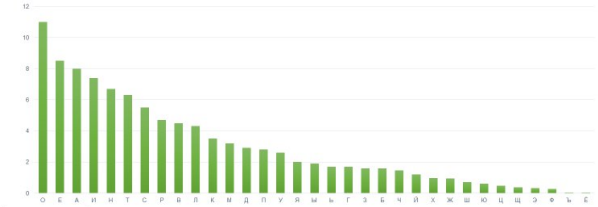
- Сколько существует возможных перестановок букв русского алфавита?

kaspersky

Ответ: если рассматриваем русский алфавит, то 33!

Следует провести дискуссию, тяжело ли все эти комбинации перебирать вручную, либо при помощи алгоритма на компьютере.

Частота встречаемости букв русского алфавита



kaspersky

Частотный анализ в шифровании – один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

На слайде показана диаграмма – распределение частот встречаемости конкретных букв русского алфавита, полученная после анализа практически всех слов русского языка. Чаще используют частоту встречи слогов.

Вопрос: Где вы встречали в реальной жизни такую частоту встречи букв?

Ответ: Расположение букв на клавиатуре.

Если говорить о частоте встречаемости слогов, то пример – клавиатура телефона, при нажатии на конкретную букву вокруг нее показываются возможные следующие буквы в написании слова. Такая технология реализована во многих гаджетах.

Следует отметить, что если текст будет технического направления, то, к примеру, частота буквы «Ф» будет намного больше.

Вопрос: Как вы считаете, если использовать шифр простой замены, что произойдет с частотами встреч букв алфавита замены?

Ответ: Буквы нового алфавита (шифротекста) унаследуют частоту (вероятность встречи) букв исходного алфавита.

Слова учителя: Следует отметить, что данная диаграмма построена при анализе всех слов, на практике же имеем ограниченный текст, тем самым, частота конкретной буквы может немного отличаться от эталонной.

kaspersky

Вопрос:

- В чем плюсы и минусы шифра простой замены?

kaspersky

У учащихся в рабочих листах имеется готовая таблица, в которую необходимо вписать свои варианты ответа.

Примеры возможных вариантов ответов:

+: простота шифрования и расшифровки, если шифровать вручную; много различных комбинаций перестановок; чем меньше слов для шифрования простой замены, тем труднее получить исходный текст, применяя частотный анализ.

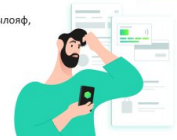
-: легкий взлом при помощи частотного анализа; различные комбинации перестановок легко реализовать на языках программирования.

Задание:

- При помощи частотного анализа расшифруйте текст:

Тяомджфя ф нмяорнмц нуяюя ьуячятц нмяуя;
Я л убыъх рся нудйяуя,
Змр вмр чур ъёъ съ мяф юругжрх олфц:
Уцжг нмрцм чяэънмц Рэфц.
Рэфрэ н пруыбшцсд нъюъ рся ырнмяуя;
Эъомцм Рэфятц мяф ц наф:
Мр ф мътб цй поцштъм, мр цй ся йэрнм сясцшъм,
Мр цй прсбйяъм, мр цй пруцшъм;
Рэфц съ ыъхнмэлбм сцфяф.
«Мгкл порпянмг! — ьрэроцм рся, — ц мрм ылояф,
Фмр нулжяъм убынфцй энъй зояф:
Энщ пор Рэфц уцжг тсъ сяуьяуц;
Я порфл ся-эрурн съм э сцй».
Тяомджфя млм н ырняыд ц н пъзяуц
Р фятъсг мяф йэямцуя цй,
Змр мругфр юодчьц чянэъофяуц.

- Помощь для анализа: https://planetcalc.ru/733/



kaspersky

Задание можно выполнить при помощи частотного анализа онлайн (ссылка указана на слайде). В рабочих листах имеется данный шифротекст и таблица соответствий букв.

Так как текст имеет не особо много символов, то точно будет «размытие» вероятности встречи конкретной буквы. Поэтому необходимо сопоставить условно и после этого провести логический анализ текста. К примеру, если в шифротексте встречается одна отдельная буква, которая не соответствуют по смыслу расшифрованному тексту, то возможно это предлог, союз или местоимение.

Ответ: Басня Крылова «Мартышка и очки».

При шифровании в этом примере исходный алфавит зеркально отражен (А-Я, Б-Ю, В-Э, …, Я-А).

Спасибо за внимание!

kaspersky

Слова учителя: Давайте подведем итог нашего занятия. Сегодня мы рассмотрели шифр простой замены и выявили связь, между теорией вероятностей и шифрованием данного вида, применяли частотный анализ для расшифровки текста.

В качестве обобщения полученных знаний, можно еще раз задать вопрос ученикам:

1. На ваш взгляд, в чем плюсы и минусы шифра простой замены?
2. Помогает ли теория вероятностей на 100% расшифровать зашифрованный текст?

Спасибо за внимание!