Олимпиада НИУ ВШЭ для студентов и выпускников – 2018 г.

Направление: «Бизнес-информатика»

Профиль: «Управление информационной безопасностью» **КОД – 172**

РЕШЕНИЯ И ОТВЕТЫ

Литература:

1. Яглом А.М., Яглом И.М. Вероятность и информация. — М.: ДомКнига, 2007. — 512 с.
2. Кноп К.А. Взвешивания и алгоритмы: от головоломок к задачам. – М.: МЦНМО, 2011. – 104 с.
3. Бабаш А.В., Шанкин Г.П. Криптография. / Под редакцией В.П.Шерстюка, Э.А. Применко. – М.: СОЛОН-Р, 2002. – 512 с.
4. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. Лабораторный практикум: учеб.пособие (+CD-ROM) – М.: КНОРУС, 2015. . – 200 с.
5. Зубов А. Ю. Криптографические методы защиты информации. – М.: Гелиос АРВ, 2005. – 192 с.
6. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.
7. Смарт Н.Криптография. – М.: Техносфера, 2006. – 528 с.
8. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.
9. Щербаков А.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Издательско-торговый дом “Русская редакция”, 2003.
10. Фомичев В.М. Дискретная математика и криптология. Курс лекций. – М.: Диалог-МИФИ, 2003.
11. Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. Монография. Под редакцией Баранова А.П., М., 2016. 182 с. (9.5 а.л.)

По структуре олимпиадного задания:

1. Дайте развернутый ответ (5 вопросов)

Вопрос 1.

БАВ

Ваня и Петя используют следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задаётся в табл.2.

Таблица 2

1	2	3	4	5	6	7	8	9	10
7	9	8	1	3	2	4	10	6	5

То есть, первая буква каждой части ставится на 7 место, вторая – на 9 место и т.д. Однажды Ваня собрался отправить сообщение Пете. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 333 раза. В результате Петя получил вот такое сообщение:

«СЬТУЕМНСЕЯИКЛЕОНКАСО».

Помогите Пете его прочитать.

Ответ
Заметим, что буквы переставляются по правилу
1→7→4→1,
2→9→6→2,
3→8→10→5→3.
Значит, каждая буква из первой и второй цепочки встанет на свое место после 3-х шифрований, а из третьей цепочки – после 4-х шифрований. Стало быть, все буквы встанут на свое место через $12 = 3 \cdot 4$ шифрований. Таким образом, через каждые 12 шифрований снова будет появляться исходный текст. Ваня зашифровывал свое сообщение 335 раз. Поделим с остатком 335 на 12:
$335 = 12 \cdot 27 + 11$
Значит, если зашифровать текст, который получил Петя еще раз, то получим 336 шифрований, где число 336 кратно 12, и получится исходное сообщение:
«УМЕНЯЕСТЬСЕНОКОСИЛКА».
Ответ: У МЕНЯ ЕСТЬ СЕНОКОСИЛКА.

Вопрос 2.
ЛМВ

Опасно ли использовать мобильный банк? Что нужно сделать, чтобы снизить возникающие риски?

Ответ: опасно, так как в него бывает упрощенный вход и компрометация (например, вирусная) устройства может привести к хищению денег. Лучше его вообще не использовать, применять только полноценный интернет банк. Но, если использовать, то применять хороший антивирус и не заходить с устройства на опасные сайты.
Источник: моя статья в НБЖ, 2016, 10.

Вопрос 3.
ЕВМ
Охарактеризуйте Мошенничество в сфере компьютерной информации как категорию противоправного деяния

Ответ: хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей

Вопрос 4.
ЛМВ
Что такое Agile и как его реализуют сейчас?

Ответ: 1) серия подходов к разработке программного обеспечения, ориентированных на использование итеративной разработки, динамическое формирование требований и обеспечение их реализации в результате постоянного взаимодействия внутри самоорганизующихся рабочих групп, состоящих из специалистов различного профиля.
2) Сейчас это часто реализуют слишком "усердно" и в тех областях, где это изначально (см. п. 1) не предусматривалось. При этом в протоколах реализации появляются элементы секты.
Источник: Википедия и мои собственные наблюдения.

Вопрос 5

Сколько в среднем бит передаваемой информации оказывается искаженной в эфирной части передаваемой сотовой телефонной связи от телефона до радиовышки во время типичного грозового разряда, если скорость передачи *V*=13 Кбит/с?

Ответ. Не более одного-двух или без искажений.

Решение. Длительность грозового разряда по результатам наблюдений составляет $t = 50 \cdot 10^{-6}$ сек. = 50 мкс. Во время грозового разряда все S бит, передаваемые за его течение можно считать искаженными. Следовательно,

$$S = t \cdot V = 5 \cdot 10^{-5} \cdot 1{,}3 \cdot 10^{4} = 0{,}6.$$

Следовательно, искажений либо не будет, либо их будет мало (1 или 2).

2. Решите задачи (5 задач)

Задача 1 (Ч).

81 раз бросается монета, при этом 60 раз выпал орел. Можно ли сказать, что монета правильная т.е. вероятность выпадения орла или решки одинакова и равна $\frac{1}{2}$?

Ответ. Нет, монета неправильная, орел выпадает чаще чем надо.

Решение. 81 бросание модулируется последовательностью независимых 0,1-случайных величин $\xi_1, \dots, \xi_{81}$, где 0 – орел, 1 – решка. Среднее число орлов для правильной монеты $81 \cdot \frac{1}{2} \cdot \frac{1}{2} = 40{,}5$.

Дисперсия числа орлов равна

$$\sigma^2 = 81 \cdot \frac{1}{2} \cdot \frac{1}{2} = 20{,}25.$$

Тогда величина отклонения $\sigma = \sqrt{20{,}25} \approx 4{,}5$.

По правилу «трех сигм» вероятность отклонения больше, чем на $3\sigma = 13{,}5$ меньше, чем 10^{-3}. Следовательно, орлов более, чем $40{,}5 + 13{,}5 = 54$ быть не должно. У нас наблюдается 60 выпадений орлов, т.е. это чрезвычайно редкое событие, которое не случается практически никогда. Следовательно, монета не может быть правильной.

Задача 2.

БЕК

Расшифровать текст, зашифрованный шифром перестановки, имея ключ

Текст: «ПОРИКТФЧРАГИА СКЕЯИААЩЗТ»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Решение:

Составим **ключ-обратной подстановки**:

1	2	3	4	5	6
4	6	2	3	1	5

Разобьём текст в соответствии с длинной ключа и запишем в столбик

П	О	Р	И	К	Т
Ф	Ч	Р	А	Г	И
А		С	К	Е	Я
И	А	А	Щ	З	Т

Переставим столбцы в соответствии с этим ключом. Первый столбец станет четвертым, второй – шестым, и так далее. После перестановки получим таблицу:

К	Р	И	П	Т	О
Г	Р	А	Ф	И	Ч
Е	С	К	А	Я	
З	А	Щ	И	Т	А

Затем выпишем строки по порядку и получим **расшифрованный текст:**
«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА»

Задача 3.
БАВ

Найти все натуральные числа, оканчивающиеся на 2006, которые после зачеркивания последних четырех цифр уменьшаются в целое число раз.

Решение
Пусть натуральные числа n имеют вид n= x•10000 + 2006, где x принадлежит множеству натуральных чисел N. После вычеркивания последних цифр получим число x.
По условию, где n € N. Отсюда имеем, что должно быть натуральным и x. Следовательно, x - делитель числа 2006.
Число 2006 имеет делители: 1; 2; 17; 34; 59; 118; 2006. Следовательно, имеются числа, отвечающие условию задачи: 12006; 22006; 172006; 342006; 592006; 1182006; 20062006.
Ответ: 12006; 22006; 172006; 342006; 592006; 1182006; 20062006.

Задача 4
БПА

Сколько в среднем бит передаваемой информации может быть искажено в эфирном тракте Wi-Fi при типичном грозовом разряде, если скорость V передачи данных составляет V = 1 Mbit/s?
Решение. Длительность грозового разряда составляет в среднем величину 50 мкс. Поэтому искажено может быть $50 \cdot 10^{-6} \cdot 10^{6} = 50$ бит информации.

Задача 5

БПА
В пин-коде платежной карточки 4 цифры, каждая из которых выбирается случайно из множества $0,1,\ldots,9$ и независима друг от друга. Сколько в среднем будет одинаковых цифр в пин-коде?
Ответ. $\frac{4\cdot 3}{2} \cdot \frac{1}{10} = 0{,}6.$
Решение. Пусть $(\xi_1, \xi_2, \xi_3, \xi_4)$ – пин-код, как реализация 4-х независимых случайных величин. Тогда число совпадающих пар R равно

$$R = J(\xi_1 = \xi_2) + J(\xi_1 = \xi_3) + J(\xi_1 = \xi_4) + J(\xi_2 = \xi_3) + J(\xi_2 = \xi_4) + J(\xi_3 = \xi_4),$$

где $J()$ – индикатор совпадения.

Поскольку

$$P\{J(\xi_1 = \xi_2) = 1\} = P(\xi_i = \xi_2) = \frac{1}{10},$$

то $ER = 6 \cdot \frac{1}{10} = 0{,}6$.

3.

Выберите один или несколько правильных ответов среди предложенных и заштрихуйте соответствующий овал в бланке ответов на пересечении номера вопроса и номера ответа. Дополнительно можете привести обоснование ответа . (5 заданий)

Вопрос 1.

1. Как принято оформлять политику безопасности в организации:
   а) в виде приказа о назначении ответственных лиц;
   б) в виде отчетов обо всех действиях пользователей в АИС;
   г) как документ, включающий описание проблемы, область применения, позиции руководства организации, санкции за не выполнение и пр.;
   д) в виде инструкции о действиях в критических ситуациях.

   Ответ – в)

   См «Защита информации в компьютерных системах» В.Шаньгин.

Вопрос 2

В технологии электронной подписи используется пара ключей – открытый и закрытый. Каким ключом делается подпись:

а) открытым ключом отправителя;
б) открытым ключом получателя;
в) закрытым ключом отправителя;
г) закрытым ключом получателя.

Ответ – подписание закрытым ключом отправителя.
См «Защита информации в компьютерных системах» В.Шаньгин.; http://dic.academic.ru

Вопрос 3

Перехват сетевых пакетов, передаваемых по линиям передачи данных в сети это:

а) Dos-атака;
б) Спуфинг;
в) «Man-in-the-middle»;
г) Сниффинг.

Ответ – г)
См «Защита информации в компьютерных сетях» В. Шаньгин

Вопрос 4

1. Какая модель управления доступом является групповой:
   а) на основе идентификации;
   б) мандатная;

в) ролевая;
г) дискреционная.

Ответ – в).
См «Защита информации в компьютерных системах» В. Шаньгин.

Вопрос 5

Основой построения большинства поточных шифров являются:

1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
2) схемы суммирования по mod 16;
3) таблицы подстановок.

Правильный ответ (1.)

4. Прочитайте раздел **Federal Information Security Management Act of 2002**, сделайте критический анализ на русском языке, определите соотнесение указанных положений с правовыми нормами Российской Федерации.

SEC. 203. COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE note. AND ACCEPTANCE OF ELECTRONIC SIGNATURES.
PURPOSE.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.
(b) ELECTRONIC SIGNATURES.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105-277;
112 Stat. 2681-749 through 2681-751), each Executive agency (as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.
(c) AUTHORITY FOR ELECTRONIC SIGNATURES.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.
(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federed bridge certification authority for digital signature compatibility, and for other activities consistent with this section, $8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

5. Выберите одну из предложенных тем и напишите эссе по этой теме:
1. Угрозы и риски в системе обеспечения информационной безопасности.
2. **Флаги идентификаторов сессий (cookies) httponly и secure.**
Ответ: Флаг httponly запрещает обращение к cookies исполняемому JavaScript коду, что не позволяет украсть сессию жертвы, в случае эксплуатации уязвимости межсайтовое исполнение сценариев (Cross-Sote Scripting).
Флаг secure запрещает передачу cookies от клиента к серверу по не зашифрованному протоколу HTTP, что не позволяет украсть сессию жертвы, в случае проведения атаки человек по середине.
Книга: The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, Second Edition

3. Какие на ваш взгляд должны быть основные принципы безопасной работы в интернете?