Олимпиада для студентов и выпускников – 2017

Направление: «Бизнес-информатика»
Профиль: «Управление информационной безопасностью» КОД – 172

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.

Как Вы понимаете существо атаки типа «человек посередине»? Как эффективно с ней бороться?

Ответ: Этот тип атак используется для нарушения конфиденциальности и целостности сеанса. Злоумышленник использует слабости в ИБ для прослушивания и нелегального захвата трафика. При этом чаще всего он подменяет идентификацию одного из сетевых ресурсов.

Вопрос 2.

Что такое «сертификат ключа электронной подписи и для чего он используется?

Ответ: Это документ в электронном или бумажном виде, который выдается удостоверяющим центром и подтверждает, что ключ подписи действительно принадлежит владельцу сертификата. Используется для аутентификации.

Вопрос 3.

Классифицируйте информационную систему в соответствии со следующей ее характеристикой: нарушение безопасности персональных данных, обрабатываемых в ней, может привести к значительным негативным последствиям для субъектов ПДн.

Ответ: К1

Вопрос 4.

Какова роль контейнера в обеспечении стеганографической защиты информации?

Ответ:

Контейнер осуществляет маскировочную функцию. Соответственно он должен быть достаточно разнообразен и иметь значительный информационный объем. Вариаций контейнеров должно быть много и они должны регулярно пересылаться.

Вопрос 5

Охарактеризуйте значение норм уголовного права в системе обеспечения информационной безопасности

Ответ

Помимо положений гл. 28 (ст.ст.272 -274 УК РФ), Предусмотрена ответственность за мошенничество с использованием компьютерной информации (ст. 159-5 УК РФ, мошенничество с использованием платежных карт (159-4 УК РФ) и т.д.. Кроме того, существует ряд норм, предусматривающих ответственность в сфере нарушений требований по защите информации ограниченного доступа, в т.ч. -гос. тайны, коммерческой ,банковской и налоговой тайны, Личной и семейной тайны, Переписки, почтовой, телеграфной и т.д. сообщений, Объектов авторского и изобретательского права и т.д.

2. Решите задачи (5 задач)

Задача 1 (Ч).

Дано 5 различных по весу монет (a_1, a_2, a_3, a_4, a_5). За сколько взвешиваний (сравнений) можно их упорядочить по весу? Найти минимальное количество взвешиваний (сравнений).

Решение:

Общее количество исходов в этой задаче определяется количество комбинаций расположения монет и равно:

$$\mathbf{5! = 120}$$

Каждое сравнение дает два возможных результата. Тогда количество необходимой информации определяется по формуле Хартли как $\boldsymbol{log_2 120}$.

Запишем следующее неравенство:

$$\mathbf{2^6 = log_2 64 < log_2 120 < log_2 128 = 2^7}$$

Отсюда следует, что упорядочить по весу можно за 7 взвешиваний.

Ответ: 7 взвешиваний (сравнений).

Задача 2.

Задано:

8809=6

7111-0

2172=0

1113=0

5781=2

3333=0

6855=3

Следует найти: 2581=?

Ответ:

Значение зависит от количества кружочков в каждой цифре. В "9" один кружочек, в "8" — два, в "1" — ни одного, а, значит, **2581 = 2.**

Задача 3.

Пароль (пин-код) банковской карточки содержит 4 цифровых символа, каждый из 0,1,2,...,9 - возможных. Злоумышленнику удалось подглядеть 2 первых символа.

Какова вероятность получить доступ к карточному счету с трех попыток, если карточка похищена злоумышленником?

Решение:

Вероятность неугадывания после подглядывания 2-х цифр с одной попытки $(1-10^{-2})$. Вероятность угадывания равна 1 минус вероятность неугадывания с 3-х попыток, т.е.

$$1-(1-10^{-2}) \approx 3 \cdot 10^{-2} = 0{,}03.$$

Задача 4

Зашифровать текст при помощи шифра перестановки при имеющемся ключе.

Текст: «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА»

Ключ:

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

Решение:

Разделим текст в соответствии с длинной ключа и запишем в столбик

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

Затем поменяем столбцы местами в соответствии с ключом. Первый столбец станет пятым, второй – третьим, и так далее. В итоге получим такую таблицу:

П	О	Р	И	К	Т

Ф	Ч	Р	А	Г	И
А		С	К	Е	Я
И	А	А	Щ	З	Т

Затем выпишем строки по порядку и получим **зашифрованный текст:**

«ПОРИКТФЧРАГИА СКЕЯИААЩЗТ»

Задача 5

Какими распределениями вероятностей можно приблизить число выпавших гербов симметричной (p=0,5) / несимметричной (p - мало) монеты при большом n числе бросаний? P - вероятность выпадения герба.

Ответ:

нормальное распределение (если np стремится к бесконечности) и распределение Пуассона, если np - ограничено.

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.

К аспектам информационной безопасности относятся (выберите нужные из вариантов):

а) дискретность;

б) достоверность;

в) конфиденциальность;

г) актуальность;

д) целостность;

е) доступность.

Ответ: №№ в), д), е).

Вопрос 2

Преимуществами асимметричных криптографических алгоритмов являются (несколько верных ответов):

1) скорость выполнения криптографических преобразований;

2) легкость внесения изменений в алгоритм шифрования;

3) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа**;**

4) применение в системах аутентификации (электронная цифровая подпись)**.**

Правильный ответ №№ 3 и 4

Вопрос 3

Кроме алгоритма RSA часто используемыми алгоритмами асимметричного шифрования являются (несколько верных ответов):

1) алгоритм Эль-Гамаля**;**

2) алгоритм шифрования Месси-Омуры**;**

3) алгоритм Вильяма-Шафрама;

4) алгоритм Грищенкова.

Ответ: правильный ответ №№ 1 и 2

Вопрос 4

Противоугонная система автомобиля кодирует возможность доступа к нему случайной цифровой (от 0 до 9) последовательностью. Какой разрядности должен быть код, чтобы при атаке типа Brute Force с компьютера производительностью 1 млн. операций в секунду система «в лучшем» для нее случае устояла бы в течении 10 минут?

Не менее 8

Не менее 16

Не менее 32

Не менее 64

Решение: Brute Force – это атака на пароль путем полного перебора.

Делаем допущение, что 1 млн. операций в секунду – это время проверки одной комбинации цифр.

За 10 мин, т.е. за 600 сек можно перебрать 6 помноженное на 10 в восьмой степени комбинаций. Что дает 8-и разрядный код из заданного по условию алфавита.

Ответ – не менее 8.

Вопрос 5

В асимметричных криптографических алгоритмах ключи зашифрования и расшифрования всегда:

1) разные, хотя и связанные между собой**;**
2) разные, никак не связанные между собой;
3) совпадают;
4) ключ зашифрования представляет собой ключ расшифрования, записанный в обратном порядке.

Правильный ответ: №1

4. Прочитайте раздел International Strategy for Cyberspace (Prosperity, Security, and Openness in a Netwokked World), сделайте ее критический анализ на русском языке, определите соотнесение указанных положений с нормами Доктрины информационной безопасности Российской Федерации.

Military: Preparing for 21st Century Security Challenges

Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:

• **Recognize and adapt to the military's increasing need for reliable and secure networks.** We recognize that our armed forces increasingly depend on the networks that support them, and we will work to ensure that our military remains fully equipped to operate even in an environment where others might seek to disrupt its systems, or other infrastructure vital to national defense Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so;

• **Build and enhance existing military alliances to confront potential threats in cyberspace.** Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation are needed to confront those actors who would seek to disrupt or exploit our

networks This effect begins by acknowledging that the interconnected nature of networked systems of our closest allies, such as those of NATO and its member states, creates opportunities and new risks Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies and partners to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors;

• **Expand cyberspace cooperation with allies and partners to increase collective security.** The challenges of cyberspace also create opportunities to work in new ways with allied and partner militaries By developing a shared understanding of standard operating procedures, our armed forces can enhance security through coordination and greater information exchange; these engagements will diminish misperceptions about military activities and the potential for escalatory behavior Dialogues and best practice exchanges to enhance partner capabilities, such as digital forensics, work force development, and network penetration and resiliency testing will be important to this effrt The United States will work in close partnership with like-minded states to leverage capabilities, reduce collective risk, and foster multi-stakeholder initiatives to deter malicious activities in cyberspace.

5. Выберите одну из предложенных тем и напишите эссе по этой теме:

Проблемы информационной безопасности

Отрасль информационной безопасности в частном секторе

Массовое применение IT –технологий и угрозы информационной безопасности

Угрозы и риски в сфере информационной безопасности