Олимпиада для студентов и выпускников – 2017 г.

Направление: «Бизнес-информатика»

Профиль: «Управление информационной безопасностью» КОД – 172

Время выполнения задания - 240 минут, язык – русский.

Задание 1. Дайте развернутые ответы на следующие вопросы:

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

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

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.

4. Какова роль контейнера в обеспечении стеганографической защиты информации?

5. Охарактеризуйте значение норм уголовного права в системе обеспечения информационной безопасности.

Задание 2. Решите задачи.

Задача 1.

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).

Задача 2.

Задано:
8809=6
7111-0
2172=0
1113=0
5781=2
3333=0
6855=3
Следует найти: 2581=?

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?

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

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.

Задание 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.

1. К аспектам информационной безопасности относятся (несколько верных ответов):

1) дискретность;
2) достоверность;
3) конфиденциальность;
4) актуальность;
5) целостность;
6) доступность.

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).

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.

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?

1) Не менее 8;
2) Не менее 16;
3) Не менее 32;
4) Не менее 64.

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.

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:

1. Проблемы информационной безопасности;
2. Отрасль информационной безопасности в частном секторе;
3. Массовое применение IT –технологий и угрозы информационной безопасности;
4. Угрозы и риски в сфере информационной безопасности.