Олимпиада НИУ ВШЭ для студентов и выпускников – 2019 г.

Направление: «Бизнес-информатика»

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

Время выполнения задания - 240 мин.

Задание 1. Дайте развернутый ответ (5 вопросов)

Вопрос 1.

Предприятию надо обеспечить устойчивый обмен электронными юридически значимыми документами большого объема. Сформулируйте мотивированно основные требования ИБ к необходимым для этого техническим решениям.

Вопрос 2.

Часто отмечают, что информационная безопасность ситуации или системы состоит в обеспечении конфиденциальности (к), целостности (ц), доступности (д).построить, предложить . описать систему (ситуацию), в которой безопасность информации требует только:

1. целостности и доступности
2. конфиденциальности и целостности
3. конфиденциальности и доступности

Вопрос 3.

Что означает «многократное шифрование» применительно к блочным шифрам?

Вопрос 4.

Охарактеризуйте значение электронного документа при совершении электронных сделок.

Вопрос 5

Охарактеризуйте различные виды электронных подписей

1. простая
2. усиленная
3. усиленная квалифицированная

Задание 2. Решите задачи (5 задач)

Задача 1 .

Расшифровать криптограмму, полученную с помощью метода случайного гаммирования, считая, что буквы алфавита пронумерованы от 0 до 32, соответственно. Зная определенную гамму.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Криптограмма: КММУТГЦНЕЩРК

Гамма (ключ):

11	1	17	1	14	19	9	14	19	17	15	11

Задача 2.

В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я – на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось АААЯАНМШСЧЕИИИТФМРСРМТИСЕ. Найдите исходный текст

Задача 3.

Пароль состоит из ***к*** буквенных символов русского алфавита, использующего 32 буквы. «Хороший» пароль образуется в результате выбора каждого его значения случайным, независимым от других знаков способом, равновероятным 32 возможных значений. Какова вероятность того, что в пароле из к букв будет хотя бы одно повторение, если к=5, к=8?

Задача 4

Какова вероятность P(n) того, что в группе из n человек дни рождения всех людей будут различными?

Задача 5

В группе 30 студентов, даты рождения которых образуются как реализация из 30 независимых случайных величин с равномерным распределением каждой в течение 365 дней года. Сколько пар студентов в среднем будут иметь общий день рождения?

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. (5 заданий)

Вопрос 1.

2 человека играют в игру, подбрасывая симметричную монету и просчитывая количество выпавших "орлов" и "решек". Правила игры: каждый бросок выигрывает тот игрок, у которого после этого броска было больше выпавших сторон монеты. Играют очень долго. Каков результат игры? Почему?

Варианты ответа:

1) каждый из игроков выиграет примерно одинаковое количество бросков;
2) один из игроков будет существенно обыгрывать другого;
3) игрок, бросающий монету первым, выиграет у другого игрока.

Вопрос 2.

Персональные данные это:

Варианты ответа:

1) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
2) любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
3) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Вопрос 3.

Расшифровать криптограмму, полученную с использованием шифра простой замены, при имеющемся ключе шифрования.

Текст: ЭДГЖХЪЦЬАЦАЬЯБГЫЖРАБЬЬБАЗЦЛБДЖЕЬБЕЮЩН

Ключ-подстановка:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

Варианты ответов:

1) СПОСОБЗАЩИТЫИНФОРМАЦИИЭТОКРИПТОГРАФИЯ
2) УПРАВЛЕНИЕИНФОРМАЦИОННОЙБЕЗОПАСНОСТЬЮ
3) УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Вопрос 4

Будет ли каждое из множеств A, B, C, D подмножеством другого, если A – множество действительных чисел, B – множество рациональных чисел, C – множество целых чисел, D – множество натуральных чисел:

Варианты ответа:

1) да;

2) нет;

3) лишь некоторые из множеств являются подмножествами перечисленных множеств.

Вопрос 5

Какова вероятность того, что случайном pin-коде платежной карты встретятся хотя бы 2 повторяющиеся цифры.

Варианты ответа:

1) ≈0,02
2) ≈ 0,50
3) ≈ 0.17
4) ≈0, 63

Задание 4.

Прочитайте положение **General Data Protection Regulation**, сделайте критический анализ на русском языке, определите соотнесение указанных положений с правовыми нормами Российской Федерации.

The GDPR (Regulation (EU) 2016/679) (European Parliament and Council of the European Union, 2016b) strengthens the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It came into force on 24 May 2016 and applied from 25 May 2018. Some Member States have already adopted this legislation, others are working on its preparation, but this does not affect the binding nature of the regulation itself.
Under Article 6.1 a) of the GDPR, the processing of personal data, including IP addresses, is permitted for a specific, necessary and proportionate purpose (purpose of legitimate interest pursued by the CSIRTs, s specified on Article 6.1 f) if the data subject (the person concerned, the person whose personal data are processed) gives consent. In the event of an IT incident, there is no consent from the data subject (e.g. IP address holder) who caused the incident. However, according to the GDPR (see Article 13.3) and to Recital 49 it can be considered that the personal information, under certain circumstances, can be processed by the CSIRT even without consent. Recital 49 indeed provides that 'The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), CSIRTs, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" [DoS] attacks and damage to computer and electronic communication systems.'

Задание 5.

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

1. Особенности обеспечения информационной безопасности в негосударственных предприятиях.

2. Проблемы обеспечения информационной безопасности на предприятиях критической информационной инфраструктуры.

3. Обеспечение информационной безопасности в условиях построения цифровой экономики.