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

По структуре олимпиадного задания:

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.

Ответ должен содержать следующие элементы:

- строгая аутентификация;
- применение усиленной ЭП;
- высоко надежные каналы связи (чтобы механизм проверки ЭП не переводил канал в постоянный переспрос очередной посылки)

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

Ответ должен содержать следующие элементы:

Раскрыть термины «целостность», «доступность» и «конфиденциальность» согласно положений стандарта ISO 27001 «Информационные технологии.

Охарактеризовать методы обеспечения информационной безопасности и системы управления защитой информации.

Далее следует связать отсутствие одного из компонентов с характеристикой информационных активов предприятия с учетом потребностей бизнеса в обработке информации, её хранении и передаче.

Следует также описать характер потенциальных угроз информационной безопасности в каждом конкретном случае и характер возможных негативных влияний инцидентов в сфере информационной безопасности.

Вопрос 3.

Что означает «многократное шифрование» применительно к блочным шифрам?

Ответ должен содержать следующие элементы:

1) повторное применение алгоритма шифрования к шифртексту с теми же ключами;
2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
3) увеличение числа этапов шифрования открытого текста.

Вопрос 4.

Охарактеризуйте значение электронного документа при совершении электронных сделок

Ответ должен содержать следующие элементы:

1. понятие электронного документа;
2. значение электронного документа при решении проблемы авторизации
3. электронный документ и скорость сделки;
4. юридическая значимость электронного документа

Вопрос 5

Охарактеризуйте различные виды электронных подписей

1. простая
2. усиленная
3. усиленная квалифицированная

Ответ должен содержать следующие элементы:

1. Понятие электронной подписи
2. Понятие и отличительные признаки каждого из вида подписей
3. Условия использования простой электронной подписи
4. Особенности использования усиленных электронных подписей

2. Решите задачи (5 задач)

Задача 1 (Ч).

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

Решение:

Y	К	М	М	У	Т	Г	Ц	Н	Е	Щ	Р	К
	11	13	13	20	19	3	23	14	5	26	17	11
К	11	1	17	1	14	19	9	14	19	17	15	11
X	0	12	29	19	5	17	14	0	19	9	2	0
	А	Л	Ь	Т	Е	Р	Н	А	Т	И	В	А

Первая строка - зашифрованный текст.

Вторая строка – номера букв зашифрованного текста.

Третья строка – гамма.

Четвертая строка – номера букв открытого текста в алфавите.

Пятая строка – открытый текст, в соответствии с номерами.

Вычитаем из номера буквы алфавита соответствующий компонент ключа, если разность меньше 0, то прибавляем 33. Например первая буква А (11-11=0), а шестая буква Р (3-19=-

16; -16+33=17). Затем записываем **расшифрованный текст** в соответствии с номерами букв в алфавите: АЛЬТЕРНАТИВА

Ответ: АЛЬТЕРНАТИВА

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 ААЯАНМШСЧЕИИИТФМРСРМТИСЕ. Найдите исходный текст

Решение. По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Ответ:

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте: 1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→1 → … То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: 7→14→21→7→… Следовательно, после 21 преобразования текст будет совпадать с исходным. Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ АСИММЕТРИЧНАЯ ШИФРСИСТЕМА

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

Ответ. $P_{к\ -}$ вероятность наличия повторений, а 1- $P_к$ - вероятность отсутствия повторений тогда:

$$\frac{32*31*\ldots(32-к+1)}{32^к} = \frac{32^{[к]}}{32^к}$$

$$P_{к=\ 1-}\frac{32^{[к]}}{32^к};$$

$$P_{к=}\ 0{,}3$$

$$P_8 ==0{,}62$$

Задача 4

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

Решение. Если *n* > 365, то вероятность равна нулю. Если же n ≤ 365, то будем рассуждать следующим образом. Возьмём наугад одного человека из группы и запомним его день рождения. Затем возьмём наугад второго человека, при этом вероятность того, что у него день рождения не совпадёт с днем рождения первого человека, равна 1 — 1/365. Затем возьмём третьего человека, при этом вероятность того, что его день рождения не совпадёт с днями рождения первых двух, равна 1 — 2/365. Рассуждая по аналогии, мы дойдём до последнего человека, для которого вероятность несовпадения его дня рождения со всеми предыдущими будет равна 1 — (*n* — *1*)/365. Перемножая все эти вероятности, получаем вероятность того, что все дни рождения в группе будут различными:

$$P(n)=(1-\frac{1}{365})(1-\frac{2}{365})(1-\frac{n-1}{365})=\frac{364}{365}\frac{363}{365}\ldots\frac{365-(n-1)}{365}=$$

$$\frac{364!}{365^{n-1}(365-n)!}=\frac{365!}{365^{n}(365-n)!}$$

Ответ $\frac{365!}{365^{n}(365-n)!}$.

Задача 5

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

Решение. Пусть $\xi_1,\ldots,\xi_n$- даты рождения студентов, $n=30$. Число пар одинаковых дней рождения есть величина

$$R=\sum_{1\le i<j\le n} J(\xi_i=\xi_j),\ J(A)=\begin{cases}1, \text{если А имеет место}\\ 0, \text{если А не имеет место'}\end{cases}$$

т.е. $J(A)$ – индикатор события A.

Тогда среднее от R и есть требуемая в задаче величина

$$ER=\sum_{1\le i<j\le n} EJ(\xi_i=\xi_j)=\frac{n(n-1)}{2}\cdot P(\xi_1=\xi_2),$$

поскольку $\xi_1,\ldots,\xi_n$ – независимы и одинаково распределены.

Т.к. $P(\xi_1=\xi_2)=\frac{1}{365}$, получаем при $n=30$.

Ответ: $\frac{30\cdot 29}{2}\cdot\frac{1}{365}=1{,}2$

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)

Варианты ответов

Вопрос 1	Вопрос 2	Вопрос 3	Вопрос 4	Вопрос 5
2	3	2	2	2

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.'

При решении задания следовало сделать перевод текста, критический анализ текста.
Соотнести предлагаемый текст с положениями ФЗ РФ «О персональных данных», "О безопасности критической информационной инфраструктуры Российской Федерации"
Сделать выводы о возможности применения (неприменения)указанных положений в РФ.