Направление «Бизнес-информатика»

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

Решения и ответы

1. Дайте развернутый ответ

1.1.Дайте характеристику моделирования как средства экспериментального исследования.

1.2.Из каких этапов состоит статистическое обследование компьютерной системы?

1.3.Виды и источники угроз информационной безопасности.

1.4.Охарактеризуйте основания ограничения доступа к информации.

2. Решите задачи

2.1.ИТ-предприятие внедряет у себя современные технологии: для банковского обслуживания; для электронного управления доступом на территорию предприятия и в отдельные его зоны; для сбора событий ИБ, связанных с нарушениями режима. Но имеет место быть небрежное отношения к паролям для доступа к корпоративным ресурсам. Предложите конструктивное решение проблемы.

Ответ: перейти на строгую аутентификацию по цифровому сертификату и, чтобы носитель с ним не валялся где-попало, интегрировать на один «пластик» и чип с банковскими приложениями, и электронную метку по управлению доступом на предприятие, и цифровой сертификат для управления доступом к корпоративным информационным ресурсам. Такая универсальная карточка будет всегда с собой, а факт ее оставления где-то будет быстро обнаружен самим хозяином. На рынке такие решения появляются.

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

Ответ:

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

Литература: В.Ф.Шаньгин. Комплексная защита информации в корпоративных системах.

2.3.Дано: шифр гуммирования. Отправитель отправил получателю, шифрованный текст длиной 1000 знаков. Но при шифровании открытого текста ключом-гаммой был пропущен 99-й знак гаммы. Получатель не смог расшифровать текст после 99 знака. Он попросил передающего передать информацию заново. Передающий зашифровал открытый текст тем же ключом заново без ошибок и передал шифр текст получателю. Как противник смог дешифровать часть переданной информации, подключившись к каналу связи?

Решение

Пусть I={0,1,…N-1} алфавит (номера букв) открытого и шифрованного текстов. Ключ для шифрования открытого текста $о_1,о_2,\ldots,о_{1000}$ имеет вид $г_1,г_2,\ldots,г_{1000}$

Уравнения шифрования имеют вид

$о_к+г_к=ш_к \bmod(N)$ при шифровании без ошибки и

$о_к+г^*_к=ш^*_к \bmod(N)$ при шифровании с шибкой.

Уравнения для к от 99 и далее имеют вид

$о_{99}+г_{99}=ш_{99} \bmod(N)$ (1)

$о_{100}+г_{100}=ш_{100} \bmod(N)$ (2)

$о_{101}+г_{101}=ш_{101} \bmod(N)$ (3)

и т.д. при шифровании без ошибки и

$о_{99}+г_{100}=ш^*_{100} \bmod(N)$ (4)

$о_{100}+г_{101}=ш^*_{101} \bmod(N)$ (5)

$О_{101}+г_{102}=ш^*_{102} \bmod(N)$ (6)

и т.д. при шифровании с ошибкой.

Опробуются все N значений $г_{99}$. Для каждого опробуемого варианта г из уравнения (1) находим $о_{99}$ и подставляем в (4) и находим $г_{100}$, подставляем его в(2) находим $о_{100}$, подставляем его в (5) находим $г_{101}$, подставляя его в (3) находим $о_{101}$. И так далее находим текст соответствующий опробуемому варианту г. Если текст нечитаемый (не содержательный) опробуем следующий вариант $г_{99}$. Опробуя все возможные варианты $г_{99}$ (а их всего N) находим открытый содержательный текст.

2.4.Зашифровать текст при помощи шифра простой замены, при имеющемся ключе. Пропуски не шифруются. Текст: «КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ». Ключ: 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

Решение

При помощи ключа зашифровываем текст. В соответствии с ключом первая буква текста «К» перейдет в «В», «Р» перейдет в «Г» и так далее. В итоге получим **зашифрованный текст:**

«ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

Для задачи

2.5.Устройство состоит из 10000 элементов, работающих независимо один от другого. Вероятность отказа любого элемента в течении времени Т равна 0,02. Найти вероятность того, что за время Т откажут ровно два элемента.

Ответ:

По условию дано: n= 10 000; p= 0,02; λ= 200

Искомая вероятность

$$P_{10000}(2)=\frac{\lambda^2}{2!}e^{-\lambda}=\frac{200^2}{2!}e^{-200}$$

3. Выберите один или несколько правильных ответов среди предложенных и заштрихуйте соответствующий овал в бланке ответов на пересечении номера вопроса и номера ответа

3.1. К аспектам информационной безопасности относятся: 1) дискретность; 2) воспроизводимость; 3) конфиденциальность; 4) полезность; 5) целостность; 6) доступность.

Ответ:

3, 5, 6

3.2.При зашифровке текста «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА» при помощи шифра перестановки при имеющемся ключе: 1 2 3 4 5 6 5 3 4 1 6 2 Получается зашифрованный текст: 1) «ПОРИКТФЧРАГИА СКЕЯИААЩЗТ» 2) «АВДОТЬББАРАГ КАВЗЗАЛИ» 3) «ДОТРОТМТМТЖ КАДОМАР»

Ответ:

1

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»

3.3.В устройстве 500 элементов. Вероятность повреждения 0,004. Найти вероятность того, что за время Т повреждено меньше трех элементов 1) 0.68 2) 0.27 3) 1.15 4) 0.0014

Ответ:

1

Решение:

При большом числе испытаний n и малой вероятности p для вычисления вероятности того, что в n испытаниях (n – велико) событие произойдет k раз, используют ***формулу Пуассона***:

$P_n(k) = \frac{\lambda^k}{k!} e^{-\lambda}, \ \lambda = np$ – среднее число появлений события в n испытаниях.

По условию дано: $n = 500, \ p = 0,004, \lambda = np = 2$.

По теореме сложения вероятностей

$$P = P_{500}(0) + P_{500}(1) + P_{500}(2) =$$

$$= e^{-2} + \frac{2}{1!}e^{-2} + \frac{4}{2!}e^{-2} = 5e^{-2} = 0,68.$$

3.4. Носители сведений, составляющих государственную тайну, это: 1) материальные объекты, в том числе физические поля 2) лица, допущенные к сведениям, составляющим государственную тайну 3) документы, содержащие информацию из интернета

Ответ:

1

Источник:

Закон РФ № 5485-1 «О государственной тайне»

3.5. Под конфиденциальностью информации следует понимать: 1) запрет просмотра, записи или хранения, а также других способах вмешательства или наблюдения за сообщениями 2) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя 3) необходимость предотвращения утечки (разглашения) информации за пределы расположения предприятия

Ответ:

2

Источник:

Федеральный Закон № 149 «Об информации, информационных технологиях и о защите информации»

4. Прочитайте статью и сделайте ее критический анализ на русском языке

In order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject

to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons.

Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association. From: Directive 95/46/EC Of The European Parliament And Of The Council

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

5.1.Информационная безопасность как следствие общего взгляда на безопасность и ее зависимость от цели существования системы.

5.2.Возможные методы и оценки рисков в сфере информационной безопасности.

5.3.Государственная, конкурентная разведка и промышленный шпионаж.