Олимпиада для студентов и выпускников - 2016

Национальный исследовательский университет «Высшая школа экономики»

Направление: «Бизнес-информатика»

Профиль: «Управление информационной безопасностью» КОД – 172

Время выполнения задания - 240 минут

Литература:

1. Бабаш А.В., Шанкин Г.П. Криптография. / Под редакцией В.П.Шерстюка, Э.А. Применко. – М.: СОЛОН-Р, 2002. – 512 с.
2. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. Лабораторный практикум: учеб.пособие (+CD-ROM) – М.: КНОРУС, 2015. . – 200 с.
3. Зубов А. Ю. Криптографические методы защиты информации. – М.: Гелиос АРВ, 2005. – 192 с.
4. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.
5. Смарт Н.Криптография. – М.: Техносфера, 2006. – 528 с.
6. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.
7. Щербаков А.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Издательско-торговый дом “Русская редакция”, 2003.
8. Фомичев В.М. Дискретная математика и криптология. Курс лекций. – М.: Диалог-МИФИ, 2003.

Общая часть

Задание 1. Открытые вопросы

Дайте развернутый ответ

Вопрос 1. В компьютерную систему поступает 100 запросов в течение одного часа. Вероятность получения ошибочного запроса и его необработки составляет 0,01.

Какова вероятность того, что в течении 2-х часов не будет ни одного ошибочного запроса?

Решение 1 задачи:

В течение 2-х часов будет подано 2*100=200 запросов. Вероятность неошибочного запроса 0,99. Вероятность того, что все запросы будут неошибочны $(0{,}99)^{200} = (1-0{,}01)^{200} = e^{-2} \approx 0{,}135$.

Вопрос 2. В системе установлен парольный доступ и длина пароля, состоящего из цифр 0,1,...,9, равна трем.

а) Какова вероятность угадывания пароля с первого раза?

б) Какова вероятность угадывания пароля с не более чем 10 попыток?

в) Какое ограничение числа попыток надо ввести, чтобы вероятность угадывания была не более 0,01?

Решение 2 задачи:

а) Вероятность угадывания трех цифр с первого раза $\left(\frac{1}{10}\right)^3 = 10^{-3}$.

б) Вероятность неугадывания с первого раза $1-10^{-3} = 0{,}999$. Тогда вероятность угадывания за 10 попыток равна 1 - (вероятность неугадывания за 10 попыток) = 1 - 0,99 = 0,01.

в) Вероятность неугадывания с первого раза $1-10^{-3} = 0{,}999$. При k попытках вероятность неугадывания $\left(1-10^{-3}\right)^k \approx e^{-k\cdot 10^{-3}}$. Вероятность угадывания $1-(1-10^{-3})^k \approx 1-e^{-k\cdot 10^{-3}} \approx 1-1+k\cdot 10^{-3} = 0{,}01.$ Т.е. *k=10.*

Вопрос 3. Что такое CRC в пакете данных протокола Ethernet и для чего он используется?

Решение 3 задачи:

CRC - это циклический проверочный код для Ethernet длины 32. Он используется для проверки целостности (неизменности) данных в пакете.

Вопрос 4. Для чего нужен Удостоверяющий Центр при реализации технологии электронной подписи?

Решение 4 задачи:

Удостоверяющий центр нужен для проверки принадлежности электронной подписи лицу, его использующему.

Вопрос 5. Для чего нужно производить регулярное обновление антивируса?

Решение 5 задачи:

База сигнатур вирусов непрерывно расширяется и пополняется производителями антивирусных средств. Регулярное, по расписанию производителя, обновление позволяет бороться с вновь появившимися новыми вирусами.

Специальная часть (4 блока)

Блок 1. Решите задачи

Задача 1.

Найдите произведение подстановок. $G1 \cdot G2 =?$

$G1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$; $G2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$.

Ответ. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Задача 2.

Датчик случайных 0,1 числе создал бинарную последовательность длиной 100, в которой единиц 75.

Можно ли считать такой датчик хорошим, т.е. что он вырабатывает равновероятные значения 0 или 1, независимо от такта к такту выдачи? Обосновать ответ.

Решение 2 задачи:

Если датчик хороший, то вероятность 0 или 1 равна 1/2. Соответственно Среднее число равно 50, а дисперсия равна 25. Соответственно, среднее отклонение должно быть не более $3\sigma = 3 \cdot \sqrt{25} = 15$. Т.о число единиц *v* должно удовлетворять неравенству $|v - 50| < 15$ с высокой степенью вероятности 0,995. В нашем случае *v*=75 и неравенство не выполняется. Следовательно, датчик плохой.

Задача 3

Расшифровать текст при помощи шифра простой замены, при имеющемся ключе шифрования.

Текст: «ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

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

Решение:

Запишем **ключ-обратной подстановки** на основе ключа-подстановки**:**

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

При помощи этого ключа расшифровываем текст. В соответствии с ключом-обратной подстановки первая буква зашифрованного текста «В» перейдет в «К», «Г» перейдет в «Р» и так далее. В итоге получим **расшифрованный текст:**

«КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ»

Задача 4

Зашифровать текст с помощью шифра 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	

Текст: «КРИПТОГРАФИЯ»

Гамма(ключ):

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

Решение:

Х	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
	11	17	9	16	19	15	3	17	0	21	9	32
К	11	1	17	1	14	19	9	14	19	17	15	11
Y	22	18	26	17	0	1	12	31	19	5	24	10
	Х	С	Щ	Р	А	Б	Л	Ю	Т	Е	Ч	Й

Первая строка - открытый текст.

Вторая строка – номера соответствующих букв в алфавите.

Третья строка – гамма.

Четвертая строка – номера букв зашифрованного текста.

Пятая строка – зашифрованный текст в соответствии с таблицей подстановки

Складываем номер буквы и соответствующий компонент ключа, если сумма больше или равна 33, то вычитаем 33. Например, первая буква (11+11=22), а пятая буква (19+14=33; 33-33=0). Затем записываем в **зашифрованный текст:** «ХСЩРАБЛЮТЕЧЙ»

Задача 5.

Охарактеризуйте общие черты и отличия нормативно-правовых требований защиты персональных данных и информации о частной жизни лица.

Ответ:

В юридической науке под частной жизнью понимается область личных, интимных, семейных, бытовых и иных отношений людей. К сведениям о частной жизни лица относят информацию, непосредственно связанную с конкретным человеком (факты его биографии, номинативные (назывные) данные, национальность, место жительства, сведения о заболеваниях, информация о семейной жизни, привычках, увлечениях, нравственных, политических, сексуальных и религиозных пристрастиях), что составляет большую часть циркулирующей в обществе информации.Задача закона состоит только в том, чтобы исчерпывающим образом зафиксировать процедуру вторжения в частную жизнь человека в интересах борьбы с преступностью, охраны здоровья и безопасности других людей, т.е. в случаях, признаваемых правомерными в цивилизованных демократических государствах.

Параллельно с развитием законодательства о защите частной жизни лица предпринимается комплекс мер по защите персональных данных, что можно связать с положениями Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных". С принятием Закона «О персональных данных» принимается комплекс организационно-техническим и правовых мер, направленных на обеспечение безопасности персональных данных.
В нашей стране механизм защиты персональных данных по компетенциям связан с деятельностью Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства связи и массовых коммуникаций Российской Федерации. Дополнительно можно выделить отраслевые подходы, например Центробанка, ФМС Российской Федерации и т.д. Достаточно свободное определение персональных данных смешивает их со сведениями, относящимися к банковской, налоговой тайне, иным категориям информации ограниченного доступа.

С другой стороны, можно проследить определённое смешение понятий «персональные данные» и «тайна личной жизни» в ряде нормативных актов и в научной литературе.

В качестве примера можно привести Перечень сведений конфиденциального характера, соотносящий понятие сведений о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющих идентифицировать его личность, с понятием персональных данных, определение которых совпадает с конвенциональным, закреплено в Федеральном законе и под которым следует понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Блок 2. Тестовые вопросы

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

Вопрос 1.

В асимметричных криптографических алгоритмах ключи зашифрования и расшифрования всегда:

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

Правильный ответ 1

Вопрос 2.

Безопасность системы RSA основана на:

1) трудности задачи разложения на простые множители;

2) комбинации символов, выбранных случайным образом;

3) использовании секретного ключа для шифрования;

4) использовании простого делителя в качестве открытого ключа.

Правильный ответ 1

Вопрос 3

1. По аспекту информационной безопасности угрозы можно классифицировать на:
2. угрозы нарушения конфиденциальности, секретности
3. угрозы нарушения конфиденциальности, доступности, целостности
4. угрозы нарушения криптографической стойкости

Правильный ответ 2.

(А.А.Малюк, В.С.Горбатов и др. Введение в информационную безопасность. Учебное пособие для высших учебных заведений).

Вопрос 4

Что такое IPS/IDS?

1. группа протоколов стека TCP/IP
2. антивирусная утилита
3. система обнаружения и предотвращения вторжений

Правильный ответ –3.
(В.Ф.Шаньгин. Комплексная защита информации в корпоративных системах).

Вопрос 5

Агрессивное потребление ресурсов является угрозой:

1. конфиденциальности
2. доступности
3. целостности

Правильный ответ – 2.
(В.Ф.Шаньгин. Комплексная защита информации в корпоративных системах).

Блок 3. Прочитайте статью, сделайте ее критический анализ на русском языке

§6802 U.S.Code - Obligations with respect to disclosures of personal information

(a)Notice requirements

Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.

(b)Opt out

(1)In generalA financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2)Exception

This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

(c)Limits on reuse of information

Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(d)Limitations on the sharing of account number information for marketing purposes

A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(e)General exceptionsSubsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information—

(1)as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with—

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B)aintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3) (A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4)to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies (including the Bureau of Consumer Financial Protection [1] a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6) (A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

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

1. Опишите характерные особенности обеспечения информационной безопасности сведений, составляющих коммерческую тайну
2. Особенности обеспечения информационной безопасности в государственных информационных системах
3. Дайте характеристику актуальных угроз безопасности персональных данных при их обработке в информационных системах