МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАДАНИЙ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационная безопасность

Направление подготовки
09.03.03«Прикладная информатика»

Профиль подготовки
«Прикладная информатика в экономике»

Квалификация выпускника
«Бакалавр»

Разработчик:
к.т.н, доцент Овсяницкая Л.Ю.

Оглавление

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Целями (целью) изучения дисциплины являются (является).

Цель:

Сформировать знания о принципах опасностей и угроз, возникающих в процессе развития современного информационного общества и овладение навыками противодействия опасностям.

Задачи:

- сформировать у студентов практические навыки использования различных способов правовой охраны существующих и вновь создаваемых объектов интеллектуальной собственности;
- освоить основные аспекты интеграции права и информационных технологий, общих вопросов правового регулирования информационных технологий.

1.1 Планируемые результаты обучения по дисциплине.

Освоение дисциплины направлено на формирование у студентов следующих компетенций:

Общекультурных:

ОК-4 - способен использовать основы правовых знаний в различных сферах деятельности;

Общепрофессиональных:

ОПК-4 - способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Профессиональных:

ПК-18 - способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.

1.2 Результаты освоения образовательной программы:

В результате изучения дисциплины студент должен:

ОК-4 - способен использовать основы правовых знаний в различных сферах деятельности.

В результате освоения компетенции ОК- 4 студент должен:

знать:

- законодательство об информационных технологиях (ИТ);
- структуру информационного законодательства;
- законодательство об ИТ в системе законодательства России;

– понятие объектов права ИТ;
– понятие субъектов права ИТ.

уметь:

– анализировать правовую ситуацию в информационной сфере, выделяя область информационных технологий;
– уметь разбираться в простейших правовых ситуациях;
– составлять и анализировать авторские договоры.

владеть/ быть в состоянии продемонстрировать:

– навыками анализа правовых ситуаций в области информационных технологий;
– навыками составления и анализа авторских договоров и лицензий к программному обеспечению.

ОПК-4 - способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

В результате освоения компетенции ОПК-2 студент должен:

знать:

– значение информации в развитии современного информационного общества и возникающие, в связи с этим;
– опасности и угрозы;
– стандарты информационной безопасности;

уметь:

– соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;
– ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу информационной безопасности;
– использовать правовые нормы в профессиональной и общественной деятельности;

владеть/ быть в состоянии продемонстрировать:

– методы обеспечения информационной безопасности;
– навыки поиска необходимых нормативных и законодательных документов;
– навыки работы с нормативными и правовыми документами в профессиональной деятельности.

ПК-18: способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью;

В результате освоения компетенции ПК-1 студент должен:

знать: методы и средства обеспечения информационной безопасности;

уметь: анализировать и выбирать методы и средства обеспечения информационной безопасности;

владеть/ быть в состоянии продемонстрировать: навыки и умения обеспечения информационной безопасности информационных систем.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ;

Содержание дисциплины (модуля)

Раздел 1. Опасности и угрозы в информационном обществе

Тема 1. Актуальность информационной безопасности, понятия и определения. Виды нарушений информационной системы.

Тема 2. Угрозы информации. Видоизменяющиеся атаки и видоизменяющаяся защита. Хешированные пароли. Социальный инжиниринг.

Тема 3. Вредоносные программы. Аутентификация и идентификация. Проблема выбора пароля.

Тема 4. Защита от компьютерных вирусов. Элементы системы аутентификации. Правила выбора PIN-кодов и паролей.

Раздел 2. Методы и средства защиты компьютерной информации

Тема 1. Использование защищенных компьютерных систем. Основы криптографии.

Тема 2. Программные и аппаратные методы криптографии. Симметричное и несимметричное шифрование.

Тема 3. Биометрические методы и средства защиты информации – принципы, преимущества, недостатки и место применения каждого средства.

Занятие в интерактивной форме предполагает проведение деловой игры, посвященной обоснованию и практическому внедрению биометрических средств аутентификации пользователей.

Раздел 3. Криптографические методы информационной безопасности.

Тема 1. RSA-алгоритм работы с открытыми ключами. Электронная подпись. Сертификаты открытых ключей. № 63-ФЗ от 06.04.2011г. «Об электронной подписи». Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Сертификаты открытых ключей. Удостоверяющие центры.

Раздел 4. Правовые аспекты в области защиты информации

Тема 1. Основные нормативные и руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Тема 2. Разграничение информации на современных предприятиях. Лицензирование и сертификация в области защиты информации.

Тема 3. Перечень сведений конфиденциального характера. Персональные данные; служебная информация; коммерческая тайна; профессиональная тайна

3. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Раздел 1. Опасности и угрозы в информационном обществе

Тема 1. Актуальность информационной безопасности, понятия и определения. Виды нарушений информационной системы.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

Подготовьте сообщения на тему:

1. Виды нарушений информационной системы.
2. Информационная безопасность – предпосылки возникновения, история, современная ситуация.

Тема 2. Угрозы информации. Видоизменяющиеся атаки и видоизменяющаяся защита. Хешированные пароли. Социальный инжиниринг.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

1. Что такое социальный инжиниринг?
2. Укажите типы угроз информации.

Тема 3. Вредоносные программы. Аутентификация и идентификация. Проблема выбора пароля.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

1. Дайте определение терминам аутентификация, идентификация, авторизация, мониторинг.
2. Опишите правила выбора паролей.

Тема 4. Защита от компьютерных вирусов. Элементы системы аутентификации. Правила выбора PIN-кодов и паролей.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

Задача: рассчитайте энтропию и битовое пространство пароля из четырех латинских букв.

Решение

Количество возможных вариантов считается по формуле:

$$S=A^n,$$

где S – количество возможных паролей,

A – заданное количество допустимых символов

n – заданная допустимая длина пароля в символах.

$$26^4 = \mathbf{456926.}$$

Поэтому, если мы разрешаем использование только 26 различных значений символов (количество букв одного регистра), и все пароли имеют в

длину четыре буквы, то количество альтернатив ограничивается числом менее полумиллиона. Для нахождения энтропии снова вычислим логарифм по основанию два:

$$\log_2(456926) = 18{,}8.$$

Количество = 19 бит, округлено вверх.

Эти расчеты наглядно показывают, как асимметрия может повлиять на диапазон значений базовой секретной информации. Обычный компьютер будет хранить пароль из четырех букв в виде последовательности из четырех восьмибитовых байтов. Таким образом, мы имеем базовую секретную информацию, которая требует 32-битового пространства. Ранее мы определили, что в случае пароля из четырех букв энтропия составляет всего 19 бит. Остальные биты жертвуются, чтобы сделать пароли для пользователей более легкими в обращении и запоминании.

Хотя фактор времени был исключен из нашего способа оценки сопротивляемости атакам, часто необходимо знать, сколько времени в среднем может занимать успешная атака. Выполним оценку среднего времени атаки.

Введем обозначения

T – среднее время атаки,

K - темп, с которым может делаться отдельное предположение (=1000).

V - среднее пространство атаки для четырехбуквенных паролей 19 бит

$$T = \frac{2^V}{R} = 524288/1000 = 524{,}3 \text{ с.}$$

Рассчитайте энтропию и битовое пространство паролей. Заполните таблицу и на основе анализа полученных данных укажите наиболее секретный пароль.

Количество символов пароля	**Допустимые символы**	**Энтропия**	**Битовое пространство**	**Ранг**
4	Латинские (26) буквы			
4	Латинские и русские буквы (33)			
4	Цифры (10), латинские и русские буквы			
4	Цифры, латинские и русские буквы с учетом регистра.			
4	Цифры, латинские и русские буквы с учетом			

	регистра, символы (10 – например, #,* и т.д)			
5	Латинские буквы			
5	Латинские и русские буквы			
5	Цифры, латинские и русские буквы			
5	Цифры, латинские и русские буквы с учетом регистра.			
5	Цифры, латинские и русские буквы с учетом регистра, символы.			
6	Латинские буквы			
6	Латинские и русские буквы			
6	Цифры, латинские и русские буквы			
6	Цифры, латинские и русские буквы с учетом регистра.			
6	Цифры, латинские и русские буквы с учетом регистра, символы.			

Раздел 2. Методы и средства защиты компьютерной информации

Тема 1. Использование защищенных компьютерных систем. Основы криптографии. Программные и аппаратные методы криптографии. Симметричное и несимметричное шифрование. Биометрические методы и средства защиты информации – принципы, преимущества, недостатки и место применения каждого средства.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

1. Укажите существующие методы биометрии.
2. Укажите преимущества и недостатки программных и аппаратных методов криптографии.

Раздел 3. Криптографические методы информационной безопасности.

Тема 1. RSA-алгоритм работы с открытыми ключами. Электронная подпись. Сертификаты открытых ключей. № 63-ФЗ от 06.04.2011г. «Об электронной подписи». Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Сертификаты открытых ключей. Удостоверяющие центры.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

Изучение законов и нормативных актов:

1. № 63-ФЗ от 06.04.2011г. «Об электронной подписи».
2. О видах электронной подписи, использование которых допускается при обращении за получением государственных услуг». Пост. Правительства РФ от 25.06.2012.

Задача:

1. Зашифруйте число закрытым ключом. Передайте кому-либо открытый ключ и предложите расшифровать число. Проверьте результат.

2. Предложите кому-либо зашифровать сообщение для вас вашим открытым ключом. Расшифруйте сообщение. Проверьте результат.

Пример выполнения работы

1. Предположим, нам необходимо подписать сообщение «Привет». Переводим слово в кодировку ANSII: 240210201215197212.
2. Хешируем сообщение. Пусть мы решим разбивать сообщение на блоки длиной 6 символов: 240210, 201215, 197212. По алгоритму эти блоки превращаются в цифры: 646.
3. Для создания ключей выбираем два простых числа: p=17, q=31.
4. Вычисляем их произведение n=p*q=17*31=527.
5. Выбирается произвольное число e (e<n), такое, что наибольший общий делитель НОД(e,(p-1)(q-1))=1. Для нашей задачи возьмем e=7. Действительно, НОД (7, 480)=1.
6. Методом Евклида решаем e*d+(p-1)(q-1)*y=1. Получим результат: y=-5, d=343.
7. Два числа (e,n) – публикуются как открытый ключ и передаются нашим партнерам.
8. Подписываем сообщение:

$$\begin{Bmatrix} c_1 = m_1^{\,d} \bmod(n) = 6^{343} \bmod(527) = 99 \\ c_2 = m_2^{\,d} \bmod(n) = 4^{343} \bmod(527) = 64 \\ c_3 = m_3^{\,d} \bmod(n) = 6^{343} \bmod(527) = 99 \end{Bmatrix}$$

9. Передаем сообщение: «Привет» и подпись: 99 64 99.
10. Получатель при проверке ЭЦП выполняет:
    a) Хеширует сообщение «Привет», получает результат 646.
    b) Расшифровывает полученным от вас открытым ключом и числом **n** сообщение 99 64 99:

$$\begin{Bmatrix} m_1 = c_1^{\,e} \bmod(n) = 99^{7} \bmod(527) = 6 \\ m_2 = c_2^{\,e} \bmod(n) = 64^{7} \bmod(527) = 4 \\ m_3 = c_3^{\,e} \bmod(n) = 99^{7} \bmod(527) = 6 \end{Bmatrix}$$

    c) Сравнивает значение, полученное при хешировании слова «Привет» (пункт 10.a) и значение, полученное при расшифровке

подписи (пункт 10.b). Если они равны, выдаем сообщение: «Подпись верна». Если значения не равны, сообщение: «Подпись поддельная».

11. Зашифруем слово «Привет» открытым ключом получателя. Шифровать будем **отдельно** каждый символ последовательности 240210201215197212.
12. В учебных целях будем шифровать своим открытым ключом.

$$c_1 = m_1^{e} \bmod(n) = 2^{e} \bmod(527) = 128$$

Передаем зашифрованный первый символ.

13. Расшифровка сообщения:

$$m_1 = c_1^{d} \bmod(n) = 128^{343} \bmod(527) = 2$$

Раздел 4. Правовые аспекты в области защиты информации

Тема 1. Основные нормативные и руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

1. Укажите основные законы РФ, регламентирующие вопросы соблюдения государственной тайны.
2. Укажите требования, предъявляемые к информационным системам, содержащим государственную тайну.

Управляющий коммерческого банка «Северный» обратился к управляющим филиалов с вопросами:

1. Необходимо ли проводить дополнительную защиту информации в их филиале банка?
2. На что обратить особое внимание?
3. Провести предварительную оценку стоимости комплекса мер по защите информации в филиале банка.

Технология работы:

Метод анкетного опроса с последующей обработкой его результатов

Для реализации данного метода разработан перечень анкетных вопросов для учредителя фирмы, охватывающий все стороны деятельности фирмы, связанные с циркулирующей на ней информацией. Перечень анкетных вопросов представлен в табл. 1.

1. Создайте электронную книгу **Информационная безопасность.xls**
2. Создайте рабочие листы: **Анализ данных**, **Оценка затрат**.
3. Выделите ячейку **A1** и скопируйте на лист **Анализ данных** в столбцы **A:D** таблицу 1:

Перечень вопросов анкеты

№ п/п	ВОПРОСЫ АНКЕТЫ	Долевые коэффициенты для общих оценок	Долевые коэффициенты для частных оценок
Уровень конкуренции			
1	1) Конкурентоспособна ли Ваша продукция на внутреннем рынке?	3,5	35
	2) Конкурентоспособна ли Ваша продукция на внешнем рынке?	5	50
	3) Монопольна ли Ваша продукция на внутреннем рынке?	1,5	15
Степень конфиденциальности информации, циркулирующей на фирме			
2	1) Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»?	11	55
	2) Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части их касающаяся, с грифом «конфиденциально»?	5	25
	3) Имеется ли информация ограниченной доступности только работникам фирмы?	4	20
Время «старения» конфиденциальности информации			
3	1) Носит ли конфиденциальность долговременный характер (год и более)?	5	50
	2) Носит ли конфиденциальность кратковременный характер (месяц и более)?	4	40
	3) Носит ли конфиденциальность оперативный характер (до месяца)?	1	10
Режимные и организационные мероприятия			
4	1) Учитываются ли интересы сохранения тайны фирмы при кадровом отборе верхнего звена управления?	3,8	13
	2) То же при подборе лиц, допущенных к конфиденциальной информации?	2,7	9
	3) То же при кадровом отборе штатного персонала фирмы в целом?	1,5	5
	4) Налажен ли контроль за сохранением работниками фирмы коммерческой тайны?	1,8	6
	5) Обеспечена ли охрана фирмы и конфиденциальной документации, содержащей коммерческую тайну?	2,2	7,4
	6) Возможен ли доступ «недопущенных» лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности?	2,3	7,6
	7) Возможно ли, по Вашему мнению, проникновение агента конкурирующей фирмы в верхнее звено управления?	6,0	19,7
	8) То же в среднее звено управления?	3,7	12,3
	9) То же в обслуживающий технику персонал?	2,3	7,6
	10) То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией?	1,5	5,0
	11) Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами?	2,2	7,4
Оснащение служебных помещений техническими средствами			

	1) Телефонными аппаратами?	2,5	8,5
	2) Переговорными устройствами?	1,5	5,0
	3) Датчиками пожарной и охранной сигнализаций?	0,6	2,0
	4) Электрическими и электронными часами?	0,8	2,5
	5) Абонентскими громкоговорителями?	0,9	3,0
	б) Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	1,5	5,0
	7) Установками прямой телефонной связи?	1,3	4,5
	8) Радиоприемниками?	1,5	5,0
	9) Телевизорами?	1,5	5,0
	10) Магнитофонами?	0,5	1,5
	11) Диктофонами?	0,5	1,5
	12) Установкой оперативной (директорской) связи?	1,5	5,0
	13) Телефаксами?	2,2	7,5
	14) Персональными ЭВМ?	3,0	10,0
	15) Видеомагнитофонами?	0,9	3,0
	16) Автоматической телефонной станцией?	3,0	10,0
	17) Радиотелефоном?	1,5	5,0
	18) Организована ли техническая защита на фирме?	4,5	1,5

4. Результаты анкетного опроса разместим на листе **Анализ данных**. Выделите ячейку **E1** и скопируйте в столбцы **E:J** таблицу 2:

Результаты анализа ответов на вопросы

Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты для общей оценки	Долевые коэффициенты для частных оценок	Общая оценка	Частные оценки
1	2	3	4	5	6
…					

5. На первом этапе заинтересованная в защите информации сторона в лице учредителя (руководителя) банка заполняет анкету, отвечая на ее вопросы, приведенные в табл. 1. Ответы на вопросы анкеты в форме **«да»** или **«нет»** заносятся в **графу 1 таблицы 2** против соответствующих вопросов. Учитывайте для **пункта 5** задание вашего варианта.

6. На втором этапе с привлечением консультанта проводится анализ результатов опроса. Если ответ на вопрос соответствует увеличению опасности утечки информации, то в **графе 2 табл. 2** проставляется знак **«+»**, в противном случае проставляется знак **«–»**. В **графе 3** расставьте**долевые коэффициенты для общей оценки**, соответствующие знаку «+» по всем вопросам анкеты, а в **графе 4** расставьте **долевые коэффициенты для частных оценок,** используя логическую функцию **ЕСЛИ**.

G4 = =ЕСЛИ(F4="+";C4;0)

	C	D	E	F	G	H	I	J
1			Результаты анализа ответов на вопросы					
2	Долевые коэффициенты для общих оценок	Долевые коэффициенты для частных оценок	Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты для общей оценки	Долевые коэффициенты для частных оценок	Общая оценка	Частные оценки
3			1	2	3	4	5	6
4	3,5	35	да	+	3,5	35		
5	5	50	да	+	5	50		
6	1,5	15	нет	-	0	0		
7	кулирующей на фирме							

7. На третьем этапе производится суммирование долевых коэффициентов **графы 3 табл. 2** «Долевые коэффициенты для общей оценки», соответствующих знаку «+» по всем вопросам анкеты. Результат суммирования записывается в **графу 5 табл.2** и является общей оценкой (**G**) для принятия решения о необходимости защиты конфиденциальной информации на фирме в целом.

При этом:

- ☑ если общая оценка **G** равна или больше **50** (**G ≥ 50**), то защиту необходимо проводить по всем направлениям;
- ☑ если общая оценка **G** больше **20**, но меньше **50** (**50 > G > 20**), то вероятность утечки информации достаточно велика, необходимо провести частные оценки, защита необходима по отдельным направлениям;
- ☑ если общая оценка **G** меньше **20** (**G<20**), то вероятность утечки информации мала и дополнительную защиту информации можно не проводить.

ПРИМЕР

Суммируя долевые коэффициенты графы 3, соответствующие знаку «+», получаем общую оценку необходимости защиты информации, циркулирующей в филиале банка в целом, равную **G=77,2 > 50**, значит, защиту информации необходимо проводить обязательно по всем направлениям.

	C	D	E	F	G	H	I	J
1			Результаты анализа ответов на вопросы					
2	Долевые коэффициенты для общих оценок	Долевые коэффициенты для частных оценок	Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты для общей оценки	Долевые коэффициенты для частных оценок	Общая оценка	Частные оценки
3			1	2	3	4	5	6
4	3,5	35	да	+	3,5	35	8,5	
5	5	50	да	+	5	50		
6	1,5	15	нет	-	0	0		
7	а фирме							
8	11	55	да	+	11	55	20	
9	5	25	да	+	5	25		
10	4	20	да	+	4	20		
11								
12	5	50	да	+	5	50	10	
13	4	40	да	+	4	40		
14	1	10	да	+	1	10		
15								
16	3,8	13	да	+	3,8	13	17,8	

……

27	редставки							
28	2,5	8,5	да	+	2,5	8,5	25,2	84
29	1,5	5,0	да	+	1,5	5		
30	0,6	2,0	да	+	0,6	2		
31	0,8	2,5	да	+	0,8	2,5		
32	0,9	3,0	да	+	0,9	3		
33	1,5	5,0	да	+	1,5	5		
34	1,3	4,5	да	+	1,3	4,5		
35	1,5	5,0	да	+	1,5	5		
36	1,5	5,0	да	+	1,5	5		
37	0,5	1,5	да	+	0,5	1,5		
38	0,5	1,5	да	+	0,5	1,5		
39	1,5	5,0	да	+	1,5	5		
40	2,2	7,5	да	+	2,2	7,5		
41	3,0	10,0	да	+	3	10		
42	0,9	3,0	да	+	0,9	3		
43	3,0	10,0	да	+	3	10		
44	1,5	5,0	да	+	1,5	5		
45	4,5	1,5	нет	-	0	0		
46							G=	81,5
47								
48								

8. На четвертом этапе проводится анализ с помощью частных оценок по всем 5 пунктам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов **графы 4 табл.2 «Долевые коэффициенты для частных оценок»**, помеченных знаком «+» для каждого пункта отдельно. При этом получится пять частных оценок:

- ☑ по пункту 1 – оценка конкурентоспособности продукции (услуг) – **G1**;
- ☑ по пункту 2 – оценка степени конфиденциальности информации – **G2**;
- ☑ по пункту 3 – оценка временных характеристик конфиденциальности информации – **G3**:
- ☑ по пункту 4 – оценка защиты информации режимными и организационными методами – **G4**:
- ☑ по пункту *5* – оценка возможности утечки информации через технические средства – **G5**.

Если частная оценка по каждому из пунктов 1-3 равна или больше **20** (**G1, G2, G3 > 20**), то это подтверждает необходимость защиты информации.

Если частная оценка по каждому из пунктов 4, 5 равна или больше 20 (**G4, G5 > 20**), то это указывает на необходимость проведения защиты информации режимными и организационными методами или с помощью технических средств защиты соответственно.

В том случае, если частная оценка по одному из пунктов 1-3 меньше 20 (**G1, G2, G3 < 20**), то защиту информации можно не проводить.

Таким образом, на основе проведенных оценок руководитель фирмы принимает решение о необходимости проведения работ по организации защиты информации.

ПРИМЕР

Суммируя долевые коэффициенты **графы 4 табл.2**, соответствующие знаку «+» по каждому пункту анкеты, получаем пять частных оценок:

частные оценки по пунктам 1, 2, 3 получились равными: **G1 = 85, G2= 100, G3 = 100**. Все они больше 20 и в соответствии с методикой

подтверждают наличие на фирме конфиденциальной информации, которую необходимо защищать.

Частные оценки по пунктам 4 и 5 получились равными: **G4 = 59,5, G5 = 84**. Обе оценки больше 20, следовательно, защита информации необходима как **режимно-организационными мерами**, так и с помощью технических средств защиты.

Выводы: анализ таблиц 1 и 2 позволяет наметить направления, по которым должна совершенствоваться защита информации в банке в нашем примере.

Например, по **пункту 4** необходимо:

наладить кадровый отбор штатного персонала фирмы в интересах обеспечения безопасности информации:

принять меры по предотвращению проникновения агентов конкурирующих фирм в состав персонала, обслуживающего технику, а также в штат, непосредственно не связанный с конфиденциальной информацией;

оборудовать специальное помещение, защищенное от утечки информации, для проведения служебных совещаний и ведения переговоров с деловыми партнерами.

Тема 2. Разграничение информации на современных предприятиях. Лицензирование и сертификация в области защиты информации.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

Тема 3. Перечень сведений конфиденциального характера. Персональные данные; служебная информация; коммерческая тайна; профессиональная тайна.

Список литературы по теме приведен в таблице 4.1

Задания для самостоятельной работы:

Изучение законов и нормативных актов:

1. ФЗ № 152 «О персональных данных» от 08.06.2006.
2. Федеральный закон от 08 июля 2006года N149-ФЗ «Об информации, информационных технологиях и о защите информации».

Подготовка устных сообщений:

1. Проблемы правового регулирования электронного информационного взаимодействия и электронного документооборота.
2. Проблемы формирования системы информационного права.
3. Информационное право как наука: основные научные школы и авторы.
4. Телекоммуникационная деятельность как объект правового регулирования. Правовое регулирование телекоммуникационных услуг.
5. Государственные автоматизированные системы как объект правового регулирования.
6. Информационные технологии как объект правового регулирования.
7. Проблемы правового регулирования отношений в сфере использования сети Интернет. Проблемы правового регулирования деятельности СМИ в сети Интернет.

4. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА, НЕОБХОДИМАЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ);

Основная литература				
	Авторы, составители	Наименование	Издательство, год	Наличие в ЭБС
Л 1.1	Ярочкин В. И.	Информационная безопасность: учебник для вузов	М.: Академический проект, 2008	http://biblioclub.ru/index.php?page=book_red&id=211164&sr=1
Л 1.2.	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации	М., Берлин: Директ-Медиа, 2015	http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1
Л 1.3.	Сычев Ю. Н.	Основы информационной безопасности: учебно-практическое пособие	М.: Евразийский открытый институт, 2010	http://biblioclub.ru/index.php?page=book_red&id=90790&sr=1
Л 1.4.	Галатенко В. А.	Стандарты информационной безопасности	Интернет-Университет Информационных Технологий, 2006	http://biblioclub.ru/index.php?page=book_red&id=233065&sr=1
Дополнительная литература				
Л 2.1.	Загинайлов Ю. Н.	Основы информационной безопасности : курс визуальных лекций	М., Берлин: Директ-Медиа, 2015	http://biblioclub.ru/index.php?page=book_red&id=362895&sr=1

*ЭБС – электронно - библиотечная система

5. РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Интернет ресурс (адрес)	Описание ресурса
1.	http://consultant.ru/	справочно-информационная система Консультант Плюс
2.	http://garant.ru/	справочно-информационная система «Гарант».

6. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Этап формирования компетенций в процессе изучения дисциплины характеризуется следующими типовыми контрольными заданиями

Типовые контрольные вопросы для подготовки к экзамену (зачету) при проведении промежуточной аттестации по дисциплине

1. Понятие угрозы. Виды противников или нарушителей. Виды нарушений информационной системы. Аутентификация и идентификация.
2. Хеширование паролей. Проблема выбора пароля. Парадокс «коврика для мыши». Элементы системы аутентификации. Социальный инжиниринг. Правила выбора PIN-кодов и паролей.
3. Противостояние атакам угадывания. Случайные значения, битовые пространства, ассиметрия базовой секретной информации.
4. Стеганография – история возникновения, назначение, принцип действия, требования, направления и ограничения.
5. Криптография и криптоанализ. Симметричное и несимметричное шифрование
6. RSA-алгоритм работы с открытыми ключами. Алгоритм создания пары ключей.
7. Электронная цифровая подпись. Алгоритм создания (3 этапа).
8. Сертификаты открытых ключей. Назначение, условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Удостоверяющие центры.
9. Три функции систем управления криптографическими ключами. PKI.
10. Носители ключей и сертификатов. Правила хранения ключей. Замок «Соболь», Touch Memory, eToken.
11. Аппаратная криптография. Достоинства и недостатки. Подписывание документов и макросов средствами MS Office.
12. Одиннадцать биометрических методов защиты информации. Достоинства, недостатки и области применения каждого метода.
13. Основные нормативные и руководящие документы, касающиеся государственной тайны. Разграничение информации на современных предприятиях. Грифы секретности. Персональные данные; служебная информация; коммерческая тайна; профессиональная тайна.

14. Средство защиты конфиденциальной информации Secret Disk. Назначение и возможности. Сценарии использования. Одноразовые пароли. Алгоритм работы.
15. Спам. История возникновения слова СПАМ. В чем заключается основная проблема борьбы со спамом. Типы спамерских писем (нигерийские письма, открытки и т.д.). Фильтры. Способы обхода фильтров. Предложения Билла Гейтса по борьбе со спамом.
16. Программы-шпионы и их типы. Межсетевые экраны.
17. Принцип записи информации на винчестер и компакт-диск. Возможность восстановления утерянной информации. Способы защиты CD дисков от копирования.
18. Основные руководящие документы Гостехкомиссии РФ. Классы защищенности автоматизированных систем в РФ. Оранжевая книга.

Критерии оценки изложены в шкале оценки для проведения промежуточной аттестации по дисциплине в п.6.2.