Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

9 Семестр

Раздел 1 Первый раздел

1.1 Контроль по итогам (КИ) - 8 Неделя

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ

для оценки уровня знаний студентов по дисциплинам «Информационная безопасность»

УСЛОВИЯ ПРИМЕНЕНИЯ

Контроль проводится письменно во время аудиторного занятия. При проведении экспресс опросов студент получает лист с индивидуальным заданием, включающим 5 вопросов, выбранных преподавателем произвольным образом из приведенного ниже перечня. Перечень включает задания трех видов: ВО (выбор одного правильного ответа), МВ (выбор нескольких правильных ответов), КО (задания с кратким ответом – число, формула). Для ответа студенту отводится 20 минут.

Критерии оценки результатов применения тестов текущего контроля (каждый тест состоит из пяти заданий)

Число правильных ответов	Процент освоения материала	Результат выполнения
0	менее 20%	0 (неуспешно)
1	от 20% до 30%	5 (неуспешно)
2	от 30% до 50%	10 (неуспешно)
3	от 50% до 60%	15 (успешно)
4	от 60% до 75%	20 (успешно)
5	более 75%	25 (успешно)

ЗАДАНИЯ ДЛЯ ТЕСТОВ

Задания типа ВО (выбор одного правильного ответа)

Задание №1

Несанкционированный доступ к информации – это:

1. получение информации пользователем без санкции руководителя;
2. получение информации лицами и процессами, не имеющими на это полномочий;
3. получение информации пользователем без разрешения администратора безопасности;
4. получение информации лицом, являющимся внешним по отношению к автоматизированной системе.

Задание №2

Угроза безопасности информации – это:

1. возникновение на каком либо этапе жизненного цикла автоматизированной системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию;
2. вероятность осуществления несанкционированного доступа к информации;
3. вероятность хищения носителей, запоминания или копирования информации.

Задание №3

Угрозы безопасности информации по видам негативного воздействия могут быть подразделены на:

1. случайные, преднамеренные, объективные, субъективные;
2. случайные, объективные;
3. угрозы техническим средствам, моделям, алгоритмам и программам, внешней среде, людям;
4. угрозы физической целостности, логической структуре, содержанию, конфиденциальности, праву собственности.

Задание №4

Какой из основных принципов защиты информации от несанкционированного доступа требует наличия у пользователя определенной формы допуска?

1. принцип обоснованности доступа;
2. принцип достаточной глубины контроля доступа;
3. принцип разграничения потоков информации;
4. принцип чистоты повторно используемых ресурсов;
5. принцип персональной ответственности;
6. принцип целостности средств защиты.

Задание №5

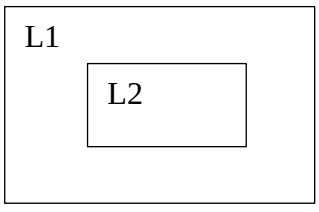
Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Какой из основных принципов защиты информации от несанкционированного доступа должен быть положен в основу принятия решения в данной ситуации?

1. принцип обоснованности доступа;
2. принцип достаточной глубины контроля доступа;
3. принцип разграничения потоков информации;
4. принцип чистоты повторно используемых ресурсов;
5. принцип персональной ответственности;
6. принцип целостности средств защиты.

Задание №6

Какие виды доступа разрешены в модели Белла и Ла Падула для показанного на рисунке взаимодействия уровней безопасности, если L1 – уровень безопасности субъекта доступа, а L2 – уровень безопасности объекта доступа?

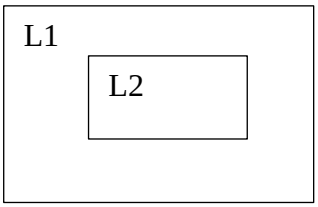
1. ни чтение, ни запись;
2. только чтение;
3. только запись;
4. и чтение, и запись



Задание №7

Какие виды доступа разрешены в модели Белла Ла Падула для показанного на рисунке взаимодействия уровней безопасности, если L1 – уровень безопасности объекта доступа, а L2 – уровень безопасности субъекта доступа?

1. ни чтение, ни запись;
2. только чтение;
3. только запись;
4. и чтение, и запись.



Задание №8

Идентификация пользователей – это:

1. проверка подлинности пользователя;
2. установление полномочий пользователя;
3. присвоение пользователю индивидуальной метки;
4. проверка пароля, предъявленного пользователем.

Задание №9

Аутентификация пользователей – это:

1. установление полномочий пользователя;
2. проверка подлинности пользователя;
3. проверка принадлежности пользователя к лицам, допущенным к защищаемой информации;
4. присвоение пользователю индивидуальной метки.

Задание №10

Какой из приведенных ниже способов аутентификации может быть отнесен к разряду «Пользователь имеет»?

1. аутентификация по предъявленному паролю;
2. аутентификация по пластиковой карте;
3. аутентификация по подписи;
4. аутентификация по отпечаткам пальцев.

Задание №11

Какой из приведенных ниже способов аутентификации является наиболее эффективным?

1. аутентификация по предъявленному паролю;
2. аутентификация по пластиковой карте;
3. аутентификация по геометрии руки;
4. аутентификация по подписи.

Задание №12

Какую роль играет PIN-код, используемый в банковской пластиковой карте?

1. персональный номер пользователя;
2. пароль в системе аутентификации;
3. ключ к расшифровке личного счета пользователя.

Задание №13

Защита информации – это:

1. состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере;
2. состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних информационных угроз;
3. обеспечение защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз;

4. состояние защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз;
5. обеспечение защищенности жизненно важных интересов личности, общества и государства в информационной сфере.

Задание №14

Безопасность информации – это:

1. состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере;
2. состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних информационных угроз;
3. обеспечение защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз;
4. состояние защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз;
5. обеспечение защищенности жизненно важных интересов личности, общества и государства в информационной сфере.

Задание №15

В чем заключается смысл интенсификации процессов защиты информации?

1. ускорение решения задач защиты информации;
2. использование наступательной стратегии защиты информации;
3. организация защиты информации на основе комплексного использования аппаратных и программных средств;
4. обеспечение комплексной защиты информации с опорой на научно обоснованные прогнозы возможных проявлений дестабилизирующих факторов.

Задание №16

Какие из перечисленных вредительских программ относятся к классу саморепродуцирующихся?

1. «Логические бомбы»;
2. «Троянские кони»;
3. «Лазейки»;
4. «Вирусы»;
5. «Бактерии»;
6. «Черви»;
7. «Шпионы».

Задание №17

Элементы матрицы доступа в модели Лэмпсона-Грэхема-Деннинга определяют:

1. привилегии субъекта доступа по отношению к объекту доступа;
2. привилегии объекта доступа по отношению к субъекту доступа;
3. разрешенные виды доступа субъекта к объекту;
4. уровень безопасности субъекта доступа;
5. уровень безопасности объекта доступа.

Задание №18

Для реализации принципа достаточной глубины контроля необходимо, чтобы:

1. механизмы контроля охватывали все информационные массивы, которые должны быть разграничены между пользователями;
2. механизмы контроля охватывали информационные массивы, содержащие конфиденциальную информацию;
3. механизмы контроля охватывали всю конфиденциальную информацию.

Задание №19

Для реализации принципа разграничения потоков информации необходимо, чтобы:

1. информация, предназначенная разным пользователям, передавалась в разных потоках;
2. информация разного уровня конфиденциальности передавалась в разных потоках;
3. информация с ограниченным доступом передавалась по выделенным линиям связи.

Задание №20

Реализация принципа чистоты повторно используемых ресурсов предполагает:

1. очистку ресурсов, содержащих конфиденциальную информацию, в конце рабочего дня;
2. очистку ресурсов, содержащих конфиденциальную информацию, после окончания сеанса связи с пользователем;
3. очистку ресурсов, содержащих конфиденциальную информацию, до их перераспределения другим пользователям;
4. очистку ресурсов, содержащих конфиденциальную информацию, при их переполнении.

Задание №21

Реализация принципа целостности средств защиты предполагает выполнение следующих условий:

1. система защиты информации должна точно выполнять свои функции;
2. система защиты информации должна содержать средства идентификации и аутентификации пользователей;
3. система защиты информации должна быть изолированной от пользователей;
4. система защиты информации не должна существенно влиять на время реализации прикладных программ пользователей;
5. система защиты информации должна позволять осуществлять контроль эффективности защиты.

Задание №22

Суть криптографических методов защиты информации заключается:

1. в кодировании информации при передаче по каналам связи;
2. в передаче конфиденциальной информации по незащищенным каналам связи;
3. в преобразовании информации в форму, непонятную для посторонних;
4. в дешифровании информации, передаваемой по открытым каналам связи.

Задание №23

Криптоанализ – это:

1. кодирование информации при передаче по каналам связи;
2. передача конфиденциальной информации по незащищенным каналам связи;
3. дешифрование информации, передаваемой по каналам связи.

Задание №24

Кодирование как способ криптографического закрытия информации – это:

1. преобразование исходного сообщения с помощью специальной процедуры, использующей систему условных обозначений элементов информации;
2. преобразование исходного сообщения с помощью специальной процедуры, использующей ключ;
3. преобразование исходного сообщения с помощью специальной процедуры, использующей шифрование.

Задание №25

Шифрование как способ криптографического закрытия информации – это:

1. преобразование исходного сообщения с помощью специальной процедуры, использующей систему условных обозначений элементов информации;
2. преобразование исходного сообщения с помощью специальной процедуры, использующей ключ;
3. преобразование исходного сообщения с помощью специальной процедуры, использующей кодирование.

Задание №26

Что представляет собой стеганография?

1. разновидность криптографии, использующая несимметричный алгоритм шифрования;
2. маскировка самого факта скрытной передачи сообщений по незащищенным каналам связи;
3. способ преобразования сообщений в форму, непонятную для постороннего, с использованием специальных символов;
4. один из способов кодирования информации.

Задание №27

В каких из перечисленных ниже случаев используется несимметричный алгоритм шифрования?

1. используется централизованная схема распространения ключей шифрования, каждый абонент имеет два ключа – ключ связи с центром и ключ шифрования данных;
2. используется децентрализованная схема распространения ключей шифрования, каждый абонент имеет два ключа – ключ шифрования ключей и ключ шифрования данных;
3. используется открытая информационная сеть, каждый абонент имеет два ключа – общедоступный ключ и секретный ключ.

Задание №28

Как изменяется стойкость криптосистемы при увеличении сложности алгоритма шифрования?

1. увеличивается;
2. уменьшается;
3. стойкость не зависит от сложности алгоритма.

Задание №29

Как изменяется стойкость криптосистемы при увеличении длины ключа шифрования?

1. увеличивается;
2. уменьшается;
3. стойкость не зависит от длины ключа.

Задание №30

Какой из методов реализации алгоритма шифрования (аппаратный или программный) может обеспечить более высокую стойкость криптосистемы?

1. программный;
2. аппаратный;
3. стойкость не зависит от метода реализации алгоритма.

Задание №31

Какая из двух криптосистем является более стойкой с точки зрения теории вычислительной сложности?

1. у криптоаналитика имеется необходимая информация для восстановления сообщения в заданный срок;

2. у криптоаналитика есть возможность получения дополнительной информации, чтобы восстановить сообщение;
3. обе криптосистемы не удовлетворяют требованиям стойкости в равной степени;
4. обе криптосистемы удовлетворяют требованиям стойкости в равной степени.

Задание №32

К какому классу криптосистем относится известный алгоритм шифрования DES, разработанный фирмой IBM?

1. симметричные криптосистемы;
2. несимметричные криптосистемы;
3. криптосистемы с общедоступным ключом.

Задание №33

Криптосистема с общедоступным ключом использует:

1. симметричный алгоритм шифрования;
2. несимметричный алгоритм шифрования.

Задание №34

Какая криптосистема лежит в основе реализации алгоритма электронной цифровой подписи?

1. симметричная криптосистема;
2. несимметричная криптосистема.

Задание №35

Можно ли использовать криптосистему с общедоступным ключом для доведения до абонентов ключа шифрования ключей в децентрализованной системе распределения ключей?

1. можно;
2. нельзя;
3. можно в отдельных случаях.

Задание №36

Кто вырабатывает ключ данных в централизованной системе распределения ключей шифрования, построенной на основе центра трансляции ключей?

1. вызывающий абонент;
2. вызываемый абонент;
3. центр трансляции ключей.

Задание №37

Кто вырабатывает ключ данных в централизованной системе распределения ключей шифрования, построенной на основе центра распределения ключей?

1. вызывающий абонент;
2. вызываемый абонент;
3. центр распределения ключей.

Задание №38

В чем заключается различие систем распределения ключей шифрования с центром трансляции ключей (ЦТК) и с центром распределения ключей (ЦРК)?

1. в системе ЦРК ключ данных вырабатывает центр, а в системе ЦТК – вызывающий абонент;
2. в системе ЦТК все абоненты имеют индивидуальные ключи связи с центром, а в системе ЦРК ключ связи с центром – общедоступный;
3. в системе ЦТК используется один ключ, а в системе ЦРК – два ключа.

Задание №39

Какие из приведенных ниже вредительских программ относятся к классу саморепродуцирующихся?

1. логические бомбы;
2. лазейки;
3. троянские кони;
4. черви;
5. бактерии;
6. вирусы.

Задание №40

Какая из приведенных ниже последовательностей действий соответствует алгоритму, реализуемому программой-вирусом?

1. проверить условие срабатывания – при выполнении условия осуществить заданные манипуляции, при невыполнении – найти и заразить незараженную программу – передать управление несущей вирус программе;
2. найти и заразить незараженную программу – проверить условие срабатывания – при выполнении условия осуществить заданные манипуляции, при невыполнении – передать управление несущей вирус программе;
3. проверить условие срабатывания – при выполнении условия найти и заразить незараженную программу, при невыполнении – передать управление несущей вирус программе – осуществить заданные манипуляции;
4. проверить условие срабатывания – при выполнении условия найти и заразить незараженную программу, осуществить заданные манипуляции, при невыполнении – передать управление несущей вирус программе.

Задание №41

«Спячка» как фаза существования компьютерного вируса используется его автором:

1. для создания у пользователей уверенности в правильной работе вычислительной системы;
2. для заражения других программ;
3. для многократного самокопирования вируса.

Задание №42

Фаза проявления компьютерного вируса заключается:

1. в заражении других программ;
2. в разрушении программ и данных, предусмотренном автором вируса;
3. в многократном самокопировании вируса.

Задание №43

Какие из перечисленных ниже антивирусных программ имеют основной задачей подсчет контрольной суммы и сравнение ее с заданным значением для защищенных копий программы перед каждым началом ее работы?

1. программы проверки целостности программного обеспечения;
2. программы контроля;
3. программы удаления вирусов.

Задание №44

Какие из перечисленных ниже перспективных методов борьбы с компьютерными вирусами базируются на системах логического вывода? Суть их сводится к определению алгоритма и спецификации программы по ее коду и выявлению, таким образом, программ, осуществляющих несанкционированный доступ.

1. универсальные методы;

2. адаптивные и самообучающиеся методы;
3. интеллектуальные методы;
4. аппаратные методы.

Задание №45

Технический канал утечки информации – это:

1. акустические, виброакустические, электрические и электромагнитные сигналы, представляющие конфиденциальную информацию;
2. совокупность физических полей, несущих конфиденциальную информацию, конструктивных элементов, взаимодействующих с ними, и технических средств злоумышленника для регистрации поля и снятия информации;
3. взаимовлияние цепей с конфиденциальной информацией и цепей вспомогательных средств и систем, выходящих за контролируемую территорию;
4. воздействие опасных сигналов на вспомогательные технические средства и системы.

Задание №46

Какой технический канал утечки информации наиболее часто используется техническими разведками для получения конфиденциальной информации?

1. акустический;
2. виброакустический;
3. проводной и радиосвязи;
4. побочных электромагнитных излучений и наводок.

Задание №47

Что является источником опасных сигналов при съеме конфиденциальной информации с помощью подключения злоумышленника к телефонной линии связи?

1. телефонный аппарат;
2. абоненты, ведущие переговоры;
3. аппаратура АТС.

Задание №48

Электронный контроль речи – это:

1. использование электронных стетоскопов и лазерных детекторов для негласного съема акустической информации;
2. использование радиоканала и линий электропитания для передачи акустической информации;
3. использование записывающих диктофонов для фиксирования акустической информации.

Задание №49

Какой из перечисленных ниже методов не применяется для негласного съема информации в каналах телефонной связи?

1. непосредственное подключение к телефонной линии;
2. негальваническое подключение к телефонной линии;
3. перехват побочного электромагнитного излучения телефонного аппарата;
4. использование микропередатчика с питанием от телефонной линии;
5. прослушивание помещений с помощью кодового микрофонного усилителя;
6. прослушивание помещений с помощью микрофона телефонного аппарата;
7. прослушивание помещений с использованием телефонных аппаратов, содержащих электромагнитный звонок;
8. прослушивание телефонных разговоров, ведущихся по радиотелефонам без применения средств защиты;

9. перехват факсимильных сообщений.

Задание №50
Какой из перечисленных ниже технических каналов наиболее часто используется для перехвата информации, обрабатываемой средствами вычислительной техники?

1. акустический канал;
2. канал проводной и радиосвязи;
3. канал побочных электромагнитных излучений и наводок;
4. канал вторичных источников питания;
5. канал воздействия опасных сигналов на вспомогательные технические средства и системы.

Задания типа МВ (выбор нескольких правильных ответов)

Задание №1
Какие из перечисленных элементов автоматизированной системы могут являться субъектами доступа к информации?

1. пользователь;
2. файл данных;
3. администратор;
4. регистр;
5. программа;
6. задание;
7. процесс;
8. терминал;
9. порт;
10. узел сети;
11. том;
12. устройство;
13. память.

Задание №2
Какие из перечисленных элементов автоматизированной системы могут являться объектами доступа к информации?

1. память;
2. устройство;
3. пользователь;
4. узел сети;
5. том;
6. процесс;
7. администратор;
8. задание;
9. терминал;
10. порт;
11. файл данных;
12. программа;
13. регистр.

Задание №3
Какие из перечисленных ниже характеристик могут быть отнесены к основным характеристикам

устройств аутентификации?

1. габариты и вес;
2. среднее время наработки на отказ;
3. число обслуживаемых пользователей;
4. потребляемая мощность;
5. частота ошибочного отрицания законного пользователя;
6. частота ошибочного признания постороннего;
7. стоимость;
8. уровень защиты от атмосферных воздействий;
9. уровень защиты от несанкционированного доступа;
10. приемлемость со стороны пользователей;
11. объем циркулирующей информации между считывающим устройством и блоком сравнения.

Задание №4

Какие основные методы контроля доступа используются в современных автоматизированных системах?

1. на основе списковых схем разграничения доступа;
2. на основе принципа обоснованности доступа;
3. на основе аутентификации;
4. на основе мандатных схем разграничения доступа.

Задание №5

Защита информации в современных системах ее обработки – это обеспечение:

1. доступности информации для пользователей;
2. целостности информации при ее передаче, обработке и хранении;
3. конфиденциальности информации.

Задание №6

Что должна включать в себя информационная база монитора обращений для обеспечения реализации установленных правил разграничения доступа?

1. список паролей пользователей;
2. разрешенные виды доступа;
3. необходимые формы допуска;
4. идентификаторы пользователей;
5. уровни конфиденциальности объектов доступа.

Задание №7

Информационная безопасность – это:

1. состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних информационных угроз;
2. обеспечение защищенности жизненно важных интересов личности, общества и государства в информационной сфере;
3. состояние защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз;
4. обеспечение защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз.

Задание №8

Соблюдение принципа обоснованности доступа предполагает выполнение следующих условий:

1. пользователь должен иметь необходимую форму допуска, соответствующую уровню конфиденциальности запрашиваемой информации;
2. пользователь должен быть идентифицирован в системе;
3. пользователь должен быть аутентифицирован;
4. запрашиваемая пользователем конфиденциальная информация необходима ему для выполнения производственных обязанностей;
5. все действия пользователя должны быть зафиксированы в специальном журнале.

Задание №9

Реализация принципа персональной ответственности предполагает выполнение следующих условий:

1. пользователь должен иметь необходимую форму допуска, соответствующую уровню конфиденциальности запрашиваемой информации;
2. пользователь должен быть идентифицирован в системе;
3. пользователь должен быть аутентифицирован;
4. запрашиваемая пользователем конфиденциальная информация необходима ему для выполнения производственных обязанностей;
5. все действия пользователя должны быть зафиксированы в специальном журнале.

Задание №10

Какие из перечисленных методов аутентификации по своей сути отвечают принципу «пользователь есть»?

1. аутентификация по предъявленному паролю;
2. аутентификация по подписи;
3. аутентификация по PIN-коду;
4. аутентификация по голосу;
5. аутентификация по отпечаткам пальцев;
6. аутентификация по геометрии руки.

Задание №11

Какие из перечисленных методов могут быть использованы для повышения стойкости парольных систем аутентификации пользователей?

1. метод взаимной аутентификации по принципу «запрос-ответ»;
2. хранение паролей в зашифрованном виде;
3. использование паролей однократного применения.

Задание №12

В каких из перечисленных ниже случаев используется симметричный алгоритм шифрования?

1. используется централизованная схема распространения ключей шифрования, каждый абонент имеет два ключа – ключ связи с центром и ключ шифрования данных;
2. используется децентрализованная схема распространения ключей шифрования, каждый абонент имеет два ключа – ключ шифрования ключей и ключ шифрования данных;
3. используется открытая информационная сеть, каждый абонент имеет два ключа – общедоступный ключ и **секретный ключ.**

Задание №13

Основными требованиями, предъявляемыми к криптосистеме, являются:

1. наличие очень большого числа возможных ключей шифрования;

2. вероятности генерации любых возможных значений ключа должны быть одинаковыми;
3. не должны вырабатываться «слабые» ключи, известные для конкретного алгоритма шифрования.

Задание №14

Какие из перечисленных ниже методов криптографической защиты информации реализуются с помощью процедуры шифрования?

1. замена;
2. перестановка;
3. сжатие;
4. разнесение;
5. гаммирование.

Задание №15

В целях предотвращения заражения компьютерными вирусами рекомендуется:

1. вводить в ЭВМ минимальное число новых программ;
2. копировать новые программы прежде, чем они будут запущены в работу;
3. использовать криптографические методы защиты.

Задание №16

Какие из перечисленных ниже факторов приводят к возрастанию уязвимости современных автоматизированных систем для компьютерных вирусов?

1. расширение применения распределенной цифровой обработки информации;
2. использование перепрограммируемых встроенных ЭВМ и сетей связи;
3. стандартизация ЭВМ, программного обеспечения, форматов сообщений, каналов и процедур передачи данных.

Задания типа КО (задания с коротким ответом)

Задание №1

Рассмотрите возможность несанкционированного получения информации в следующем случае:
в рассматриваемой автоматизированной системе возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего систему;
в качестве компонента, являющегося объектом несанкционированных действий, рассматриваются магнитные носители информации (дискеты);
каналом несанкционированного получения информации является непосредственное хищение носителей.
Определите вероятности несанкционированного получения информации для каждого из нарушителей (P1 и P2), используя следующие обозначения:
P11 – вероятность проникновения нарушителя на территорию объекта;
P12 – вероятность проникновения нарушителя в здание;
P13 – вероятность проникновения нарушителя в помещение, где расположена система;
P14 – вероятность доступа внешнего нарушителя к ресурсам системы;
P15 – вероятность доступа внешнего нарушителя к базам данных;
P21 – вероятность доступа внутреннего нарушителя к ресурсам системы;
P22 – вероятность доступа внутреннего нарушителя к базам данных;
P1 – вероятность несанкционированного получения информации внешним нарушителем;

P2 – вероятность несанкционированного получения информации внутренним нарушителем.

Задание №2

Рассмотрите возможность несанкционированного получения информации в следующем случае:
в рассматриваемой автоматизированной системе возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего систему;
в качестве канала несанкционированного получения информации выступает ее распечатка с помощью принтера.
Определите вероятности несанкционированного получения информации для каждого из нарушителей (P1 и P2), используя следующие обозначения:
P11 – вероятность проникновения нарушителя на территорию объекта;
P12 – вероятность проникновения нарушителя в здание;
P13 – вероятность проникновения нарушителя в помещение, где расположена система;
P14 – вероятность доступа внешнего нарушителя к ресурсам системы;
P15 – вероятность доступа внешнего нарушителя к базам данных;
P21 – вероятность доступа внутреннего нарушителя к ресурсам системы;
P22 – вероятность доступа внутреннего нарушителя к базам данных;
P1 – вероятность несанкционированного получения информации внешним нарушителем;
P2 – вероятность несанкционированного получения информации внутренним нарушителем.

Задание №3

Зашифруйте с помощью метода перестановки фразу «передайте привет Максу». Используйте ключ 2576413 и символ «@» для обозначения пробелов.

Задание №4

Расшифруйте, используя ключ 58137462, фразу «шеунп@енчденвеоо@о@иеасл», зашифрованную с помощью метода перестановки. Для обозначения пробелов использован символ «@».

Критерии оценки

В критерии оценки успеваемости обучающихся входят:
- уровень теоретических знаний;
- умение использовать теоретические знания при решении задач.

Минимальный балл, при котором раздел аттестуется - 15, максимальный – 25.

Балл	Требования к знаниям
23 ÷ 25	**Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.**
18 ÷ 22	**Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.**
15 ÷ 17	**Оценка «удовлетворительно» выставляется студенту,**

	если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
менее 15	**Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.**

Раздел 2 Второй раздел

2.1 Контроль по итогам (КИ) - 12 Неделя

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ
для оценки уровня знаний студентов по дисциплинам
«Информационная безопасность»,

Контроль проводится письменно во время аудиторного занятия. При проведении экспресс опросов студент получает лист с индивидуальным заданием, включающим 5 вопросов, выбранных преподавателем произвольным образом из приведенного ниже перечня. Перечень включает задания трех видов: ВО (выбор одного правильного ответа), МВ (выбор нескольких правильных ответов), КО (задания с кратким ответом – число, формула). Для ответа студенту отводится 20 минут.

Критерии оценки результатов применения тестов текущего контроля (каждый тест состоит из пяти заданий)

Число правильных ответов	Процент освоения материала	Результат выполнения
0	менее 20%	0 (неуспешно)
1	от 20% до 30%	5 (неуспешно)
2	от 30% до 50%	10 (неуспешно)
3	от 50% до 60%	15 (успешно)
4	от 60% до 75%	20 (успешно)
5	более 75%	25 (успешно)

ЗАДАНИЯ ДЛЯ ТЕСТОВ

Задания типа ВО (выбор одного правильного ответа)

Задание №51
Какая задача предотвращения утечки информации по техническим каналам решается при проведении специальных исследований систем обработки конфиденциальной информации?

1. обнаружение съема информации;
2. предотвращение съема информации.

Задание №52
Какая задача предотвращения утечки информации по техническим каналам решается при постоянном или периодическом контроле загрузки радиодиапазона (радиомониторинге)?

1. обнаружение съема информации;
2. предотвращение съема информации.

Задание №53
Какие из перечисленных ниже устройств могут быть использованы для пассивного обнаружения электронного контроля речи?

1. генераторы аудиопомех;
2. электронные стетоскопы;
3. нелинейные локаторы;
4. лазерные детекторы.

Задание №54
Какой из перечисленных ниже методов не применяется для защиты конфиденциальной информации в каналах связи?

1. использование нелинейных локаторов;
2. использование аналогового скремблирования;
3. использование дискретизации с последующим шифрованием.

Задание №55
Активная защита от утечки информации по каналу ПЭМИН – это:

1. размещение всего оборудования в экранирующей радиоизлучения среде;
2. экранирование отдельных компонентов защищаемых систем, а также применение в линиях связи и питания различных фильтров, устройств подавления сигналов и развязки;
3. сокрытие информационных сигналов за счет шумовой или заградительной помехи с помощью специальных генераторов шума.

Задание №56
Пассивная защита от утечки информации по каналу ПЭМИН – это:

1. изменение вероятностной структуры сигнала, который может быть принят злоумышленником;
2. сокрытие информационных сигналов за счет шумовой или заградительной помехи с помощью специальных генераторов шума;
3. применение в линиях связи и питания различных фильтров, устройств подавления сигналов и развязки.

Задание №57
В законодательстве какой из приведенных стран впервые была установлена ответственность за нарушение порядка обработки и использования персональных данных?

1. Соединенные Штаты Америки;
2. Российская Федерация;
3. Великобритания;
4. Франция.

Задание №58
В законодательстве какой из приведенных стран компьютерные преступления впервые стали рассматриваться как преступления, представляющие особую опасность для граждан, общества и государства?

1. Соединенные Штаты Америки;
2. Великобритания;
3. Российская Федерация;
4. Франция;
5. Германия.

Задание №59
В законодательстве каких стран как преступления рассматриваются действия, создающие угрозу нанесения ущерба, например, попытка проникновения в систему, внедрение программы вируса и т.п.?

1. только Соединенные Штаты Америки;
2. только Российская Федерация;
3. большинство стран мира.

Задание №60

К какому периоду относятся первые попытки правового регулирования процесса информатизации в СССР и России?

1. 60-е годы XX века;
2. 70-е годы XX века;
3. 80-е годы XX века;
4. 90-е годы XX века.

Задание №61

К какому периоду относятся первые попытки правового регулирования процесса информатизации в США?

1. 60-е годы XX века;
2. 70-е годы XX века;
3. 80-е годы XX века.

Задание №62

Впервые проблема законодательного регулирования информатизации начала обсуждаться в США:

1. в связи с предложением создать общенациональный банк данных;
2. в связи с необходимостью защиты прав личности на частную жизнь;
3. в связи с необходимостью защиты предпринимательской и финансовой деятельности.

Задание №63

Вопрос о правовом обеспечении информатизации был поставлен в СССР в 70-х годах XX века:

1. в связи с развитием автоматизированных систем управления различных уровней;
2. в связи с закреплением общего права граждан на информацию;
3. в связи с созданием общего информационного пространства в международном аспекте.

Задание №64

Закон «Об информации, информационных технологиях и защите информации» предусматривает деление информации на классы:

1. общедоступная информация и конфиденциальная информация;
2. общедоступная информация и информация, составляющая государственную тайну;
3. общедоступная информация и информация с ограниченным доступом;
4. общедоступная информация, информация, составляющая государственную тайну, и информация, составляющая коммерческую тайну;
5. общедоступная информация, конфиденциальная информация и информация, представляющая персональные данные.

Задание №65

Ответственность за нарушение законодательства в области обеспечения информационной безопасности устанавливается законодательством об ответственности, которое включает в себя:

1. Уголовный кодекс;
2. Кодекс об административных правонарушениях;
3. Уголовный кодекс и Кодекс об административных правонарушениях;
4. Кодекс об административных правонарушениях и Трудовой кодекс;
5. Уголовный кодекс и Трудовой кодекс;
6. Уголовный кодекс, Кодекс об административных правонарушениях и Трудовой кодекс.

Задание №66

Какое из приведенных ниже компьютерных правонарушений наиболее часто встречается на практике?

1. несанкционированный доступ к информации, хранящейся в компьютере;
2. ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;
3. разработка и злонамеренное распространение компьютерных вирусов;
4. преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям;
5. подделка компьютерной информации;
6. хищение компьютерной информации.

Задание №67

В области обеспечения безопасности информации в мировой практике применяется значительное число специальных стандартов, предусматривающих деление автоматизированных систем на ряд классов по уровню их защищенности. Какие критерии лежат в основе такого деления на классы?

1. наличие в автоматизированной системе информации различного уровня конфиденциальности, использование различных технологий обработки информации (автоматической или интерактивной), использование различных режимов обработки информации (коллективного или индивидуального);
2. наличие в автоматизированной системе информации различного уровня конфиденциальности, наличие различных уровней полномочий субъектов доступа на доступ к конфиденциальной информации, использование различных режимов обработки информации (коллективного или индивидуального);
3. наличие в автоматизированной системе информации различного уровня конфиденциальности, наличие различных уровней полномочий субъектов доступа на доступ к конфиденциальной информации, использование различных технологий обработки информации (автоматической или интерактивной).

Задание №68

На какой из органов государственного управления Российской Федерации возложена координация работ в области криптографической защиты информации?

1. Федеральная служба по техническому и экспортному контролю;
2. Федеральная служба безопасности;
3. Федеральное агентство по информационным технологиям.

Задание №69

На какой из органов государственного управления Российской Федерации возложена координация работ в области технической защиты информации?

1. Федеральная служба по техническому и экспортному контролю;
2. Федеральная служба безопасности;
3. Федеральное агентство по информационным технологиям.

Задание №70

Какие из перечисленных ниже вопросов входят в компетенцию Федеральной службы по техническому и экспортному контролю?

1. контроль за работой средств массовой информации;
2. контроль и организация работ по защите информации в каналах правительственной связи;
3. контроль и координация работ по технической защите информации;

4. организация работ и выдача лицензий на защиту информации криптографическими методами.

Задание №71

Современная постановка задачи комплексной защиты информации предусматривает:

1. обеспечение конфиденциальности информации с помощью комплексного использования всех известных средств защиты;
2. обеспечение целостности информации при ее обработке с использованием современных информационных технологий;
3. обеспечение в комплексе доступности, целостности и конфиденциальности информации.

Задание №72

Какая из перечисленных ниже функций не входит в перечень полного множества функций защиты информации?

1. предупреждение возникновения условий, благоприятствующих порождению (возникновению) дестабилизирующих факторов;
2. предупреждение непосредственного проявления дестабилизирующих факторов;
3. предупреждение косвенного проявления дестабилизирующих факторов;
4. обнаружение проявившихся дестабилизирующих факторов;
5. предупреждение воздействия на защищаемую информацию проявившихся и обнаруженных дестабилизирующих факторов;
6. предупреждение воздействия на защищаемую информацию проявившихся, но необнаруженных дестабилизирующих факторов;
7. обнаружение воздействия дестабилизирующих факторов на защищаемую информацию;
8. локализация (ограничение) обнаруженного воздействия дестабилизирующих факторов на информацию;
9. локализация необнаруженного воздействия дестабилизирующих факторов на информацию;
10. ликвидация последствий локализованного обнаруженного воздействия дестабилизирующих факторов на информацию;
11. ликвидация последствий локализованного необнаруженного воздействия дестабилизирующих факторов на информацию.

Задание №73

Технические средства защиты информации – это:

a) механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов;
b) различные электронные, электронно-механические и тому подобные устройства, встраиваемые в аппаратуру автоматизированной системы или сопрягаемые с ней специально для решения задач защиты информации.

Какое из этих определений является верным?

1. определение «a»;
2. определение «b»;
3. оба определения.

Задание №74

Система защиты информации – это:

1. организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в автоматизированной системе, для решения в ней выбранных задач защиты;

2. совокупность всех ресурсов, выделяемых для защиты информации.

Задание №75
Одним из основных требований, предъявляемых к системе защиты информации, являются функциональные требования, сущностью которых является:

1. обеспечение решения требуемой совокупности задач защиты, удовлетворение всем требованиям защиты;
2. комплексное использование средств защиты, оптимизация архитектуры;
3. структурированность всех компонентов, простота эксплуатации.

Задание №76
К какому из макропроцессов управления системой защиты информации относится сбор и предварительная обработка информации о действительном уровне защищенности, обеспечиваемом системой?

1. планирование;
2. оперативно-диспетчерское управление;
3. календарно-плановое руководство;
4. обеспечение повседневной деятельности системы управления.

Задание №77
К какому из макропроцессов управления системой защиты информации относится принятие решения о корректировке программного обеспечения антивирусной защиты?

1. планирование;
2. оперативно-диспетчерское управление;
3. календарно-плановое руководство;
4. обеспечение повседневной деятельности системы управления.

Задания типа МВ (выбор нескольких правильных ответов)

Задание №17
Каков механизм внедрения компьютерного вируса при его воздействии на подсистему электропитания автоматизированной системы?

1. внедрение через основную среду, используемую подавляемой системой;
2. внедрение через другие среды, используемые подавляемой системой;
3. прямое внедрение в подавляемую систему;
4. косвенное внедрение в подавляемую систему.

Задание №18
Какие из перечисленных ниже мер составляют комплексную стратегию предотвращения вирусного подавления?

1. запрет доступа (препятствие проникновению вирусных программ в систему);
2. обнаружение (обнаружение присутствия в системе вирусной программы);
3. сдерживание (изоляция пораженной части системы от непораженной);
4. ликвидация (уничтожение вирусов до того, как они произведут свое разрушительное действие);
5. восстановление нормального функционирования (восстановление разрушенных файлов с использованием резервных файлов);
6. альтернативные меры (меры, не допускающие вывода системы из строя даже в случае поражения особо сложными и оригинальными вирусными программами).

Задание №19

Какие из перечисленных ниже средств относятся к основным техническим средствам автоматизированной системы?

1. персональные ЭВМ с периферийным оборудованием;
2. сети ЭВМ;
3. радиоаппаратура;
4. радиотрансляционный громкоговоритель;
5. телефонные аппараты городской АТС;
6. телефонные аппараты местной АТС;
7. датчики охранной и пожарной сигнализации;
8. радиотелефоны и сотовые телефоны;
9. телефакс;
10. табельное электрооборудование помещений;
11. телетайп;
12. средства размножения документов;
13. кондиционеры.

Задание №20

Какие из перечисленных ниже средств относятся к вспомогательным техническим средствам автоматизированной системы?

1. персональные ЭВМ с периферийным оборудованием;
2. сети ЭВМ;
3. радиоаппаратура;
4. радиотрансляционный громкоговоритель;
5. телефонные аппараты городской АТС;
6. телефонные аппараты местной АТС;
7. датчики охранной и пожарной сигнализации;
8. радиотелефоны и сотовые телефоны;
9. телефакс;
10. табельное электрооборудование помещений;
11. телетайп;
12. средства размножения документов;
13. кондиционеры.

Задание №21

Необходимость организационно-правового обеспечения безопасности информации вытекает из факта:

1. признания за информацией статуса товара;
2. признания за информацией статуса продукта общественного производства;
3. установления в законодательном порядке права собственности на информацию.

Задание №22

Какие из перечисленных ниже мер составляют организационно-правовую основу защиты информации в автоматизированной системе?

1. определение подразделений и лиц, ответственных за организацию защиты информации;
2. фиксация на документе персональных идентификаторов («подписей») лиц, изготовивших документ и (или) несущих ответственность за него;
3. узаконивание технико-математических решений вопросов организационно-правового обеспечения защиты информации;

4. нормативно-правовые, руководящие и методические материалы (документы) по защите информации;
5. меры ответственности за нарушение правил защиты информации;
6. фиксация факта любого (как несанкционированного, так и санкционированного) копирования защищаемой информации;
7. порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Задание №23

Какие из перечисленных ниже законодательных актов Российской Федерации имеют отношение к обеспечению информационной безопасности?

1. Закон РФ «О безопасности»;
2. Закон РФ «Об информации, информационных технологиях и защите информации»;
3. Закон РФ «О государственной тайне»;
4. Закон РФ «О правовой охране программ для ЭВМ и баз данных»;
5. Уголовный кодекс РФ;
6. Кодекс РФ об административных правонарушениях.

Задание №24

Каким из перечисленных ниже требований должна удовлетворять концепция комплексной защиты информации?

1. должны быть разработаны и доведены до уровня регулярного использования все необходимые механизмы гарантированного обеспечения требуемого уровня защищенности информации;
2. должны существовать механизмы практической реализации требуемого уровня защищенности информации;
3. необходимо располагать средствами рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники;
4. должны быть разработаны способы оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации.

Задание №25

Из приведенного ниже списка задач защиты информации выберите задачи, которые образуют репрезентативное множество. Под репрезентативностью понимается достаточность их для обеспечения требуемого уровня и эффективности осуществления всех функций защиты.

1. введение избыточности элементов системы;
2. резервирование элементов системы;
3. регулирование доступа к элементам системы;
4. регулирование использования элементов системы;
5. маскировка информации;
6. контроль элементов системы;
7.
8. регистрация сведений;
9. уничтожение информации;
10. сигнализация;
11. реагирование.

Задания типа КО (задания с коротким ответом)

Задание №5

Зашифруйте с помощью метода замены фразу «ваше донесение получено», используя в качестве ключа сдвиг алфавита на 5 символов вправо.

Задание №6

Расшифруйте, используя в качестве ключа сдвиг алфавита на 5 символов влево, фразу «фкхкйеочк фхнзкч сепцш», зашифрованную с помощью метода замены.

Критерии оценки

В критерии оценки успеваемости обучающихся входят:
- уровень теоретических знаний;
- умение использовать теоретические знания при решении задач.

Минимальный балл, при котором раздел аттестуется - 15, максимальный – 25.

Балл	Требования к знаниям
23 ÷ 25	**Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.**
18 ÷ 22	**Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.**
15 ÷ 17	**Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.**
менее 15	**Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.**

9 Семестр

Зачет

Вопросы к зачету по дисциплинам

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
4. Рассмотрите возможности несанкционированного получения информации в следующем случае:
   - в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;
   - в качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;
   - каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача ее на печать.

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

5. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?
6. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
7. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.
8. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

9. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

10. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

11. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

12. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

13. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

14. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

15. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

16. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

17. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

18. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

19. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

20. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.

21. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

22. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

23. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.

24. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

25. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.

26. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

27. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

28. Объясните, что представляет собой стеганография?

29. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.

30. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

31. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?

32. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

33. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

34. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

35. Каковы основные особенности криптосистем с общедоступным ключом?

36. Раскройте основное содержание алгоритма электронной цифровой подписи.

37. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.

38. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.

39. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?

40. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

41. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

42. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

43. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

44. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

45. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

46. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

47. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

48. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

49. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

50. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

51. Дайте классификацию источников утечки информации по техническим каналам.

52. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

53. Назовите известные вам методы и средства контроля акустической информации.

54. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

55. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

56. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

57. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

58. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

59. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

60. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

61. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.

62. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.

63. Что вы знаете из истории развития организационно-правового обеспечения зашиты информации в СССР и Российской Федерации? Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.

64. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

65. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

66. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

67. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

68. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

69. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

70. Сформулируйте основные концептуальные положения теории защиты информации.

71. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

72. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.

73. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

74. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

75. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

Методика оценки результатов

Критерии оценки знаний устанавливаются в соответствии с требованиями к профессиональной подготовке, исходя из действующих учебных планов и программ, с учётом характера будущей практической деятельности выпускника.

«Зачтено» (45-50 баллов) - студент владеет знаниями предмета в соответствии с рабочей программой, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на вопрос билета, четко формулирует ответ.

«Зачтено» (35-44 баллов) - студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах); самостоятельно и отчасти при наводящих вопросах дает полноценный ответ на вопрос билета.
«Зачтено» (30-34 баллов) - студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов.
«Не зачтено (ниже 30 баллов) - студент не освоил обязательного минимума знаний предмета; не способен ответить на вопрос билета даже при дополнительных наводящих вопросах экзаменатора.

Итоговая оценка представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля и выставляется в соответствии с Положением о кредитно-модульной системе. Максимальная оценка-100 баллов.

Оценка	Сумма баллов за разделы	Оценка ECTS
3 – «зачтено»	90-100	A
3 – «зачтено»	85-89	B
	75-84	C
	70-74	D
3 – «зачтено»	65-69	
	60-64	E
2 – «не зачтено»	Ниже 60	F