МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Тобольский педагогический институт им. Д.И.Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДАЮ
Директор
_____ Шилов С.П

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

44.03.01 Педагогическое образование
Профиль Безопасность жизнедеятельности
Форма обучения заочная

1. Паспорт оценочных материалов по дисциплине

№ п/п	Темы дисциплины (модуля)/ разделы в ходе текущего контроля, вид промежуточной аттестации (зачет, экзамен, с указанием семестра)	Код и содержание контролируемой компетенции (или ее части)	Наименование оценочного средства (краткое описание с указанием количества вариантов, заданий и т.п.)
3 курс			
1	Информационная безопасность - основные понятия	УК-1 УК-8 ПК-2	Вопросы для обсуждения по теме 1. Конспект лекции
2	Основные угрозы информационной безопасности в информационной образовательной среде		Вопросы для обсуждения по теме 2. Практические задания по теме 2. Конспект лекции
3	Основные меры защиты информации в распределенных компьютерных системах		Вопросы для обсуждения по теме 3. Практические задания по теме 3. Конспект лекции
4	Взаимодействие в условиях недоверенной распределенной среде		Вопросы для обсуждения по теме 4. Практические задания по теме 4. Конспект лекции
5	Стандарты в области информационной безопасности в ИОС		Вопросы для обсуждения по теме 5. Практические задания по теме 5. Конспект лекции
6	Правовое обеспечение информационной безопасности		Вопросы для обсуждения по теме 6. Практические задания по теме 6. Практические задания по теме 6.
7	Организационное обеспечение информационной безопасности в ИОС		Вопросы для обсуждения по теме 7. Практические задания по теме 7. Конспект лекции
8	Лицензирование и сертификация в информационной среде		Вопросы для обсуждения по теме 8. Практические задания по теме 8. Конспект лекции
9	Международное законодательство в области защиты информации. Компьютерные правонарушения		Вопросы для обсуждения по теме 9. Практические задания по теме 9. Конспект лекции
	Раздел 1-9		Вопросы для подготовки к экзамену (1-30).

2. Виды и характеристика оценочных средств

2.1. Контрольные вопросы для обсуждения

Контрольные вопросы используются для проведения анализа материала, самостоятельного углубления знаний, а также для самопроверки знаний студентов по отдельным вопросам и/или темам дисциплины.

Балл	Критерий оценивания
зачтено	- показывает знание основных понятий темы, грамотно пользуется терминологией; - проявляет умение анализировать и обобщать информацию, навыки связного описания явлений и процессов; - демонстрирует умение излагать учебный материал в определенной логической последовательности; - показывает умение иллюстрировать теоретические положения конкретными примерами; - демонстрирует сформированность и устойчивость знаний, умений и навыков; - могут быть допущены одна–две неточности при освещении второстепенных вопросов.
не зачтено	- не раскрыто основное содержание учебного материала; - обнаружено незнание или непонимание большей или наиболее важной части учебного материала; - допущены ошибки в определении понятий, при использовании терминологии, в описании явлений и процессов, решении задач, которые не исправлены после нескольких наводящих вопросов; - не сформированы компетенции, отсутствуют соответствующие знания, умения и навыки.

2.2. Задания к практическим занятиям

Индивидуальные практические задания представляются в виде письменной работы или файла. Критерии оценки ответа (табл.) доводятся до сведения обучающихся в начале занятий. Оценка объявляется в конце занятия.

Балл	Критерий оценивания заданий
4-5	Свободно применяет полученные знания при выполнении практических заданий; Выполнил работу в полном объеме с соблюдением необходимой последовательности действий; В письменном отчете по работе правильно и аккуратно выполнены все записи; При ответах на контрольные вопросы правильно понимает их сущность, дает точное определение и истолкование основных понятий, использует специальную терминологию дисциплины, не затрудняется при ответах на видоизмененные вопросы, сопровождает ответ примерами.
2-3	Практическая работа выполнена не полностью, но объем выполненной части позволяет получить правильные результаты и выводы; В ходе выполнения работы студент продемонстрировал слабые практические навыки, были допущены ошибки; Студент умеет применять полученные знания при решении простых задач по готовому алгоритму; В письменном отчете по работе допущены ошибки; При ответах на контрольные вопросы правильно понимает их сущность, но в ответе имеются отдельные пробелы и при самостоятельном воспроизведении материала требует дополнительных и уточняющих вопросов преподавателя.
0-1	Практическая работа выполнена не полностью и объем выполненной работы не позволяет сделать правильных выводов, у студента имеются лишь отдельные представления об изученном материале, большая часть материала не усвоена; В письменном отчете по работе допущены грубые ошибки, либо он вообще отсутствует; На контрольные вопросы студент не может дать ответов, так как не овладел основными знаниями и умениями в соответствии с требованиями программы.

2.3. Экзамен в форме собеседования по вопросам

Процедура итогового контроля может производится в форме устного ответа на вопросы по дисциплине. Все обучающиеся допускаются к прохождению промежуточной аттестации независимо от итогов текущего контроля.

При выставлении оценки следует придерживаться следующих критериев:

Оценка «отлично»:

- полно раскрыл содержание материала в объеме, предусмотренном программой;
- изложил материал грамотным языком в определенной логической последовательности, точно используя специализированную терминологию и символику;
- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов.

Оценка «хорошо»:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- нет определенной логической последовательности, неточно используется специализированная терминология и символика;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию или вопросу преподавателя.

Оценка «удовлетворительно»:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, блок-схем и листингах, исправленные после нескольких наводящих вопросов преподавателя;
- студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме,
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка «неудовлетворительно»:

- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала,
- допущены ошибки в определении понятий, при использовании терминологии, в блок-схемах и листингах программ, которые не исправлены после нескольких наводящих вопросов преподавателя.

2.4. Посещение занятий

Посещение учебных занятий является обязательным. Лекция направляет и ориентирует студента в изучаемом материале. На лекции студенты должны конспектировать основное содержание лекции. На занятиях студент должен включаться в совместную деятельность с преподавателем и другими студентами, участвовать в групповых видах работы, в учебной дискуссии.

3. Оценочные средства

3.1. Контрольные вопросы для обсуждения

На практических занятиях проводится собеседование по вопросам и представления результатов исследовательской работы по заданной тематике. Выполнения практических заданий

1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты информации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?
7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
9. Каковы правовые понятия в области защиты информации?
10. Что такое защита информации? Информационная безопасность?
11. Охарактеризуйте понятия, связанные с организацией защиты информации.
12. Каковы основные принципы построения систем защиты информации?
13. Что такое комплексный подход к обеспечению информационной безопасности?
14. Каковы основные задачи защиты информации?
15. Докажите, что приведенное множество функций защиты является полным.
16. Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?
17. Каковы основные средства реализации комплексной системы защиты информации?
18. Что такое морально-этические средства защиты информации?
19. Докажите необходимость сочетания различных средств защиты информации.
20. Приведите примеры формальных и неформальных средств защиты?
21. Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?
22. Что такое информация и каковы уровни ее представления?
23. Перечислите основные носители информации, особенности их использования и защиты.
24. Какими свойствами определяется ценность информации?
25. Какие критерии оценки ценности информации Вы можете предложить?
26. Приведите примеры различной зависимости ценности информации от времени.
27. Что понимается под информационными ресурсами?
28. Что не разрешается относить к информации ограниченного доступа?
29. Что понимается под конфиденциальной информацией?
30. Какие существуют виды тайны?
31. Какое назначение имеет перечень конфиденциальных сведений предприятия?
32. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
33. Сформулируйте основные положения Доктрины информационной безопасности РФ.
34. Каковы основные цели защиты информации?
35. Каковы основные задачи в области информационной безопасности?
36. Какова структура государственной системы защиты информации?
37. Кто несет ответственность за нарушение режима защиты информации?
38. Каковы функции руководителей предприятий при организации защиты информации?
39. Каковы основные функции ФСТЭК?

40. Покажите роль различных министерств и ведомств в вопросах защиты информации.
41. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
42. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
43. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
44. В каких системах на первом месте стоит обеспечение доступности информации?
45. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
46. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
47. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
48. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
49. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
50. В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?
51. Что понимается под утечкой информации?
52. Каким образом классифицируются каналы утечки информации?
53. Каким образом следует выбирать меры защиты конфиденциальности информации?
54. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
55. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
56. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
57. Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
58. Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
59. Дайте определение шифра и сформулируйте основные требования к нему.
60. Поясните, что понимается под совершенным шифром.
61. Почему большинство современных шифрограмм могут быть однозначно дешифрованы?
62. Каким образом государство регулирует использование средств крипозащиты?
63. Каковы способы контроля целостности потока сообщений?
64. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
65. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
66. Как организован обмен документами, заверенными цифровой подписью?
67. В чем отличие и сходство обычной и цифровой подписей?
68. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
69. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
70. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
71. Как обеспечить целостность данных при их хранении?
72. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
73. Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.
74. Как защитить программное обеспечение от изучения логики его работы?
75. Предложите меры по обеспечению более надежной работы ЛВС университета.
76. Как изменяется надежность аппаратуры с течением времени?

77. Каковы способы повышения надежности аппаратуры и линий связи?
78. Что такое политика безопасности, кто ее разрабатывает и где она применяется?
79. Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
80. Каковы основные достоинства и недостатки дискреционных моделей?
81. Приведите примеры использования дискреционных моделей разграничения доступа.
82. Составьте матрицу доступа и граф доступа для организации документооборота факультета (объекты доступа: экзаменационные ведомости, персональные данные студентов, рабочие программы дисциплин; субъекты доступа: студенты, преподаватели, декан).
83. Что такое монитор безопасности и какие требования к нему предъявляются?
84. Цели применения стандартов информационной безопасности.
85. Охарактеризуйте основные положения Оранжевой книги.
86. Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
87. Каковы основные положения Европейских критериев безопасности информационных технологий?
88. Чем отличаются «информационная система» и «продукт информационных технологий»?
89. Для чего вводятся критерии адекватности?
90. Что такое Профиль защиты?
91. В чем особенности Канадских критериев безопасности компьютерных систем?
92. Опишите структуру Общих критериев безопасности информационных технологий.
93. Опишите технологию применения Общих критериев безопасности информационных технологий.
94. Каковы тенденции развития международной нормативной базы в области информационной безопасности?

3.2. Задания к практическим занятиям

1. Подготовка терминологического словаря основных понятий темы
2. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов:

Задача: Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс". Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения. Интервью с Ивановым была опубликована и стала общедоступной, и научным руководством Института "Прогресс". Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса. Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну. Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?

Задача: Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией. Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

Задача: Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта. В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылалась на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены. Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за 1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешитъ этот спор с позиции норм информационного права?

Задача: Организация «Новые технологии», занимающаяся формированием информационных ресурсов, начала разработку новой программы для государственных информационных систем. Для обеспечения защиты информационных ресурсов в этой системе был использован криптографический алгоритм «Криптт» компании «Джомолунгма» . Правомерно ли использование этого криптоалгоритма в разрабатываемой программе? Если да, то при каких условиях?

Задача: ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «Microsoft Windows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft». Вышеуказанные экземпляры ЭВМ являются контрафактными по следующими признакам: отсутствуют документы, подтверждающие приобретение копии программы «Microsoft Windows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (СОА) с наименованием и уникальным буквенно-цифровым ключом программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «Microsoft Windows XP Professional». Представитель ООО «Холдинг-М» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется. Оцените ситуацию с точки зрения авторского права.

Задача: Оператор ПК Абдуллин, согласно своим должностным обязанностям, приеме электронных носителей с материалами обязан был проверять их на наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении. В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию. Оцените действия Абдуллина с точки зрения действующего законодательства.

Задача: Разработчик программного обеспечения Стив несколько лет работал в акционерном обществе "Галатея". В трудовом договоре не было указано на явно имущественные права на созданные программы в процессе трудовой деятельности программиста. Во время работы Стив разработал эффективную систему автоматизации учета товаров на предприятии. Увидев, что его программа дает значительный экономический эффект, Стив потребовал от руководства доплату к ежемесячному окладу. Руководство рассмотрело вопрос по оплате и отказалось осуществлять доплату, вместо этого они приняли на работу еще одного программиста. Стив, в надежде, что он не сможет прийти к соглашению с компаниями, модифицировал свою программу, в результате чего она перестала функционировать. Оцените

сложившуюся ситуацию с точки зрения действующего законодательства. Как квалифицировать действия Стива?

3. Сопоставить предложенный перечень понятий с определениями, приведенными ниже. Результат сопоставления оформить в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение

Часть 1

Вирус (компьютерный, программный)
Информационная система общего пользования
Документированная информация
Аутентификация отправителя данных
Государственная тайна
Информационная система
Автоматизированная обработка персональных данных
Блокирование персональных данных
Автоматизированная система
Информация
Гриф секретности
Вредоносная программа
Доступ к информации
Информационно-телекоммуникационная сеть
Вспомогательные технические средства и системы
Защищаемая информация.
Безопасность персональных данных

Часть 2

I. программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

II. возможность получения информации и ее использования

III. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

IV. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

V. реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

VI. сведения (сообщения, данные) независимо от формы их представления

VII. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

VIII. зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

IX. подтверждение того, что отправитель полученных данных соответствует заявленному

X. состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

XI. технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных

XII. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной

деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

XIII. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

XIV. обработка персональных данных с помощью средств вычислительной техники

XV. система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

XVI. исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения

XVII. информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

4. Составить электронный конспект по основным правовым актам в области информационной безопасности

- ст. ст. 23, 24, 29, 42 Конституции РФ, ст. ст. 5,7,8,9 ФЗ "Об информации, информационных информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016);
- ст.ст. 3, 4 Закона РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016),
- ст. ст. 7, 8, 9, 11 ФЗ "О персональных данных" от 27.07.2006 N 152-ФЗ (действующая редакция, 2016); сфера действия и принцип отнесения к гостайне ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне";
- ст. 2 ФЗ "Об электронной подписи" от 06.04.2011 N 63-ФЗ (действующая редакция, 2016);
- ст.272, 273, 274 УК РФ.

5. Составить аналитическую записку - обзор по предложенному перечню. Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу

6. Найти сайт образовательного учреждения. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий

7. Найти определения АС в соответствии с классификацией, принятой в действующей системе правовых актов и нормативно-методических документов. Вставить определения вместо пропусков. Отметить нормативные документы, регламентирующие функционирование конкретной АС в предлагаемом перечне нормативных документов. Проверить правильность выполнения заданий путем совместного обсуждения и проверки

3.3. Конспектирование

Конспект – краткое письменное изложение содержания статьи, книги, лекции, включающее в себя основные положения и их подтверждение фактами, примерами. Главная информация записывается полностью, без существенных сокращений. Основное содержание конспектирования составляет переработка второстепенной информации в целях ее обобщения и сокращения.

При конспектировании необходимо обязательно указать название конспекта, источник, по которому осуществлялось конспектирование. Желательно избрать текстуальный или цитатный виды конспекта, которые позволят более подробно представить содержание конспектируемого источника. Отсутствие лишнего материала, не имеющего отношение к работе.

3.4. Вопросы к экзамену

1. Понятие информационной безопасности
2. Аспекты безопасности
3. Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз

(антропогенные, техногенные, стихийные источники угроз).

4. Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «чѐрные» хакеры. Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации.
5. Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит.
6. Парольные системы аутентификации. Стойкость парольных систем аутентификации. Взаимная проверка подлинности пользователей информационной системы.
7. Биометрические системы аутентификации. Основные методы взлома биометрических систем аутентификации.
8. Основные модели разграничения прав доступа: дискреционная, мандатная и ролевая модели доступа.
9. Криптографическая защита информации: определение шифрования, расшифрования, дешифрования, криптографического ключа, хеширования информации.
10. Симметричное и асимметричное шифрование. Примеры симметричного и асимметричного шифрования: шифр Виженера, алгоритм RSA.
11. Электронно-цифровая подпись (ЭЦП): определение ЭЦП, схема ЭЦП, определение сертификата открытого ключа, удостоверяющего центра. Инфраструктура открытых ключей (PKI).
12. Кодирование информации как средство обеспечения целостности информации. Примеры алгоритмов кодирования.
13. Стеганография как один из способов обеспечения конфиденциальности и целостности информации.
14. Аспекты защиты интеллектуальной собственности. Проблемы «пиратства». Реверсивный инжиниринг (обратное проектирование): цели, задачи, основные методы.
15. Алгоритм оценки и анализа рисков безопасности ИС. Управление рисками безопасности ИС.
16. Технические каналы утечки информации: акустический и виброакустический каналы; оптический канал утечки; электромагнитный канал утечки информации, ПЭМИН; материальный канал утечки информации. Основные способы защиты от утечки.
17. Организационные, технические и режимные меры обеспечения информационной безопасности информационных систем.
18. Определение «вируса». Структура «вируса». Принцип работы антивирусных программ. Обфускация (запутывание программного кода) и деобфускация.
19. Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации.
20. Международные договоры и конвенции в сфере защиты информации.

Задания практического характера на экзамене аналогичны заданиям, рассматриваемым в ходе практических занятий.