

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

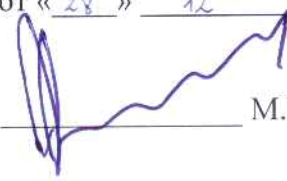
Институт информационных технологий и радиоэлектроники

Кафедра информатики и защиты информации

Основание: решение кафедры ИЗИ

от «28» 12 2016 года.

Зав. кафедрой ИЗИ


М.Ю. Монахов

Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении учебной дисциплины
«Методология информационной безопасности»

Направление подготовки: 10.04.01 «информационная безопасность»

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Владимир, 2016

1. Паспорт фонда оценочных средств

Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации при изучении учебной дисциплины «Методология информационной безопасности» разработан в соответствии с рабочей программой, входящей в ОПОП направления подготовки 10.04.01 «информационная безопасность».

№ п/п	Контролируемые разделы (темы) дисциплины	Се мес тр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение. Характеристика защищаемой информации	1	ОК-2, ПК-1	Контрольные вопросы и задания
2	Значение ИБ и ее место в системе национальной безопасности	1	ОК-2, ПК-1	Контрольные вопросы и задания
3	Основные понятия и определения в области информационной безопасности и защиты информации	1	ОК-2, ПК-1	Контрольные вопросы и задания
4	Категории защищаемой информации	1	ОК-2, ПК-1	Контрольные вопросы и задания
5	Концептуальная модель системы информационной безопасности	1	ОК-2, ПК-1	Контрольные вопросы и задания
6	Действия, приводящие к незаконному овладению конфиденциальной информацией	1	ОК-2, ПК-1	Контрольные вопросы и задания
7	Угрозы конфиденциальной информации	1	ОК-2, ПК-1	Контрольные вопросы и задания
8	Способы защиты информации	1	ОК-2, ПК-1	Контрольные вопросы и задания
9	Уровни информационной безопасности	1	ОК-2, ПК-1	Контрольные вопросы и задания
10	Законодательный уровень информационной безопасности	2	ОК-2, ПК-1	Контрольные вопросы и задания
11	Административный уровень информационной безопасности	2	ОК-2, ПК-1	Контрольные вопросы и задания
12	Процедурный уровень информационной безопасности	2	ОК-2, ПК-1	Контрольные вопросы и задания
13	Программно-технический уровень информационной безопасности	2	ОК-2, ПК-1	Контрольные вопросы и задания
14	Сервисы безопасности программно-технического уровня	2	ОК-2, ПК-1	Контрольные вопросы и задания
15	Сущность комплексной системы защиты информации	2	ОК-2, ПК-1	Контрольные вопросы и задания
16	Формирование облика нарушителя	2	ОК-2, ПК-1	Контрольные вопросы и задания
17	Алгоритм проведения анализа информационного риска на предприятии	2	ОК-2, ПК-1	Контрольные вопросы и задания
18	Управление информационной безопасностью	2	ОК-2, ПК-1	Контрольные вопросы и задания

Комплект оценочных средств по дисциплине «Методология информационной безопасности» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Методология информационной безопасности», для оценивания результатов обучения: знаний, умений, навыков и уровня приобретенных компетенций.

Комплект оценочных средств по дисциплине «Методология информационной безопасности» включает:

1 семестр

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении заданий по СРС, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме: контрольные вопросы для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2 семестр

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении заданий по СРС, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме: контрольные вопросы для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Методология информационной безопасности» при освоении образовательной программы по направлению подготовки 10.04.01 «информационная безопасность»

Перечень компетенций содержится в разделе 3 Рабочей программы дисциплины «Компетенции обучающегося, формируемые в результате освоения дисциплины»:

ОК-2 – способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

Знать	Уметь	Владеть
-------	-------	---------

<p>базовый понятийный аппарат в области ИБ; - виды и состав угроз информационной безопасности; - принципы и общие методы обеспечения информационной безопасности; - основные положения государственной политики обеспечения информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой; - виды носителей защищаемой информации; - виды тайн конфиденциальной информации; - виды уязвимости защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; - каналы и методы несанкционированного доступа к конфиденциальной информации; - классификацию видов, методов и средств защиты информации</p>	<p>выявлять угрозы информационной безопасности применительно к объектам защиты; - определять состав конфиденциальной информации применительно к видам тайны; - выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; - выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; - определять направления и виды защиты информации с учетом характера информации и задач по ее защите; - организовывать системное обеспечение защиты информации</p>	<p>основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; о современных и перспективных системах автоматизации информационно-аналитической работы информации</p>
--	---	---

ПК-1 – способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты.

Знать	Уметь	Владеть
<p>базовый понятийный аппарат в области ИБ; - виды и состав угроз информационной безопасности; - принципы и общие методы обеспечения информационной безопасности; - основные положения государственной политики обеспечения информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой; - виды носителей защищаемой информации; - виды тайн конфиденциальной информации; - виды уязвимости защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; - каналы и методы несанкционированного доступа к конфиденциальной информации; - классификацию видов, методов и средств защиты информации</p>	<p>выявлять угрозы информационной безопасности применительно к объектам защиты; - определять состав конфиденциальной информации применительно к видам тайны; - выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; - выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; - определять направления и виды защиты информации с учетом характера информации и задач по ее защите; - организовывать системное обеспечение защиты информации</p>	<p>основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы информации</p>

Оценка по дисциплине выставляется с учетом среднего балла освоения компетенций, формируемых дисциплиной, при условии сформированности каждой компетенции не ниже порогового уровня.

3. Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Методология информационной безопасности»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Методология информационной безопасности» предполагает письменный рейтинг-контроль, выполнение и защиту лабораторных, а также выполнение самостоятельных работ. В случае использования при изучении дисциплины дистанционных образовательных технологий проводится компьютерное тестирование.

Регламент проведения письменного рейтинг-контроля

№	Вид работы	Продолжительность
1	Предел длительности рейтинг-контроля	35-40 мин.
2	Внесение исправлений	до 5 мин.
	Итого	до 45 мин.

Критерии оценки письменного рейтинг-контроля (1,2 семестр)

Результаты каждого письменного рейтинга оцениваются в баллах. Максимальная сумма, набираемая студентом на каждом письменном рейтинге, составляет 10 баллов.

Критерии оценки для письменного рейтинга:

- 9-10 баллов выставляется обучающемуся, если соблюдаются критерии: полное раскрытие темы, вопроса, указание точных названий и определений, правильная формулировка понятий и категорий, приведение формул и (в необходимых случаях) их вывода, приведение статистики, самостоятельность ответа, использование дополнительной литературы;

- 7-8 баллов выставляется обучающемуся, если соблюдаются критерии: недостаточно полное раскрытие темы, несущественные ошибки в определении понятий и категорий, формулах, выводе формул, статистических данных, кардинально не меняющих суть изложения, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы;

- 5-6 баллов выставляется обучающемуся, если соблюдаются критерии: отражение лишь общего направления изложения лекционного материала и материала современных учебников, наличие достаточно количества несущественных или одной-двух существенных ошибок в определении понятий и категорий, формулах, их выводе, статистических данных, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы, неспособность осветить проблематику дисциплины;

- 1-4 балла выставляется обучающемуся, если соблюдаются критерии: нераскрытые темы; большое количество существенных ошибок, наличие грамматических и стилистических ошибок, отсутствие необходимых умений и навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методология информационной безопасности» (письменный рейтинг-контроль)

1 семестр:

Перечень вопросов для текущего контроля (письменный рейтинг №1):

1. Что такое признаковая структура объекта?
2. Что понимают под полученной объектом информацией?
3. Какая информация является предметом защиты?

4. Что такое признаковая информация?
5. Почему семантическая информация по отношению к признаковой является вторичной?
6. Какие признаки объектов являются демаскирующими?
7. Приведите классификацию демаскирующих признаков объектов защиты.
8. Опишите опознавательные демаскирующие признаки объектов защиты.
9. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
10. Что такое информативность демаскирующего признака?
11. Перечислите основные свойства информации как предмета защиты.
12. Почему информацию можно рассматривать как товар?
13. Изменяется ли цена информации во времени? Если да, то аргументируйте свой ответ.
14. Какой аналитической зависимостью можно аппроксимировать характер старения информации?
15. Что понимается под временем жизни информации?
16. Что такое количество информации?
17. Что такое тезаурус?
18. Почему информация способна случайным образом «растекаться» в пространстве?
19. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
20. Перечислите основные носители признаковой информации.
21. Что такое «источник конфиденциальной информации»?
22. Перечислите основные источники конфиденциальной информации.
23. В чем отличие прямых источников семантической информации от косвенных?
24. Охарактеризуйте людей (сотрудники, обслуживающий персонал, продавцы, клиенты и др.) в качестве источника конфиденциальной информации.
25. Охарактеризуйте документы как источники конфиденциальной информации.
26. В чем специфика публикаций, докладов, статей, интервью, проспектов, книг и т.д. в качестве источников конфиденциальной информации?
27. Охарактеризуйте технические носители информации и документов как источники конфиденциальной информации.
28. Охарактеризуйте технические средства обработки информации - автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи в качестве источника конфиденциальной информации.
29. Охарактеризуйте выпускаемую продукцию как источник конфиденциальной информации.
30. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации
31. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
32. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
33. Дайте определение информационной безопасности, прокомментируйте его составляющие.
34. Что такое защита информации?
35. Перечислите основные категории информационной безопасности и дайте им определения.
36. Охарактеризуйте понятие доступности.
37. Охарактеризуйте понятие целостности.
38. Охарактеризуйте понятие конфиденциальности.
39. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.

40. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
41. В чем заключаются национальные интересы России?
42. Чем обеспечиваются национальные интересы России?
43. В чем заключаются национальные интересы России в информационной сфере?
44. Что такое государственная информационная политика?
45. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
46. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
47. Что такое угроза к контексте ИБ России?
48. Классифицируйте угрозы ИБ РФ по общей направленности.
49. В чем состоят угрозы ИБ для личности?
50. В чем состоят угрозы ИБ для общества?
51. В чем состоят угрозы ИБ для государства?
52. Классифицируйте угрозы ИБ РФ по происхождению и прокомментируйте их.
53. Перечислите основные принципы ИБ России согласно Доктрине.
54. Каковы функции государственной системы по обеспечению ИБ?
55. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
56. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
57. В чем специфика деятельности Федеральной службой по техническому и экспортному контролю (ФСТЭК России)?
58. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
59. В чем специфика деятельности Федеральной службы безопасности?
60. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
61. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
62. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
63. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
64. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
65. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
66. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
67. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Перечень вопросов для текущего контроля (письменный рейтинг №2):

1. Какую информацию относят к защищаемой?
2. Дайте определение защищаемой информации.
3. Охарактеризуйте основные признаки защищаемой информации.
4. Перечислите и охарактеризуйте основных собственников защищаемой информации.
5. Что такое государственная тайна?
6. Приведите формальную модель определения государственных секретов
7. Перечислите сведения, которые могут быть отнесены к государственной тайне.
8. Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
9. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
10. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?

11. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
12. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
13. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
14. Перечислите основные объекты банковской тайны.
15. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
16. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
17. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
18. Перечислите основные объекты интеллектуальной собственности.
19. Что понимается под системой безопасности?
20. Перечислите основные компоненты концептуальной модели ИБ.
21. Что такое объекты угроз ИБ и в чем они выражаются?
22. Каковы основные источники угроз защищаемой информации?
23. Каковы цели угроз информации со стороны злоумышленников?
24. Перечислите основные источники конфиденциальной информации.
25. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
26. Перечислите базовые способы защиты информации.
27. Изобразите графически схему концептуальной модели системы ИБ.
28. Приведите возможный перечень способов получения информации.
29. Дайте определение способа несанкционированного доступа к источникам конфиденциальной информации.
30. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
31. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
32. Что такое утечка конфиденциальной информации?
33. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
34. Как осуществляется утечка конфиденциальной информации?

Перечень вопросов для текущего контроля (письменный рейтинг №3):

1. Дайте определение угрозы конфиденциальной информации.
2. Что такое атака?
3. Что такое окно опасности?
4. Что такое угрозы воздействия на источник информации?
5. Что такое угрозы утечки информации?
6. Какие угрозы называются преднамеренными, а какие случайными?
7. Что такое канал несанкционированного доступа?
8. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
9. Что такое наблюдение в теории информационной безопасности?
10. Что такое подслушивание в теории информационной безопасности?
11. Что такое перехват в теории информационной безопасности?
12. Что такое технический канал утечки информации?
13. Охарактеризуйте случайный и организованный канал утечки информации.

14. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
15. Какие организации формируют структуру разведывательного сообщества США?
16. Прокомментируйте наиболее распространенные угрозы доступности.
17. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
18. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
19. Охарактеризуйте программные атаки на доступность.
20. Что такое вредоносное программное обеспечение?
21. Дайте определение «бомбы», «червя», «вируса».
22. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
23. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
24. Перечислите основные угрозы конфиденциальности информации
25. Что в ИБ понимают под маскарардом?
26. Дайте определение способа защиты информации.
27. Охарактеризуйте способ предупреждения возможных угроз.
28. Прокомментируйте основные действия способа выявления угроз
29. Охарактеризуйте способ обнаружения угроз.
30. Охарактеризуйте способ пресечения или локализации угроз.
31. Прокомментируйте основные действия способа ликвидации последствий.
32. Перечислите основные защитные действия при реализации способов ЗИ,
33. Что такое защита от разглашения?
34. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
35. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
36. Назовите три группы мероприятий по технической защите информации.
37. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
38. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
39. Прокомментируйте основные технические мероприятия по технической защите информации.
40. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
41. В чем заключается специфика управления, как сервиса безопасности?

2 семестр

Перечень вопросов для текущего контроля (письменный рейтинг №1):

1. Когда принята Конституция РФ?
2. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
3. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
4. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
5. Когда принят Закон РФ «О государственной тайне»?
6. Дайте определение государственной тайны.
7. Когда принят Закон РФ "Об информации, информатизации и защите информации"?
8. Какие основные понятия рассматриваются в Закон РФ "Об информации, информатизации и защите информации"?
9. Дайте определение информации согласно Закону РФ "Об информации, информатизации и защите информации".
10. Дайте определение документа согласно Закону РФ "Об информации, информатизации и защите информации".

11. Дайте определение информационных процессов согласно Закону РФ "Об информации, информатизации и защите информации".
12. Дайте определение информационной системы согласно Закону РФ "Об информации, информатизации и защите информации".
13. Дайте определение информационных ресурсов согласно Закону РФ "Об информации, информатизации и защите информации".
14. Дайте определение конфиденциальной информации согласно Закону РФ "Об информации, информатизации и защите информации".
15. Что в Законе «Об информации ...» говорится о целях защиты информации?
16. В отношении каких видов информации устанавливается режим защиты согласно Закону РФ «Об информации ...»?
17. Почему лицензирование и сертификация выступают в качестве средства защиты информации (согласно Закону РФ «Об информации ...»)?
18. Что такое лицензия и лицензируемый вид деятельности (согласно Закону РФ "О лицензировании отдельных видов деятельности")?
19. Дайте определение лицензирования.
20. Кто такие лицензиат и лицензирующие органы?
21. Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии (согласно Закону РФ "О лицензировании отдельных видов деятельности").
22. Кто является основными лицензирующими органами в области защиты информации?
23. Какие вопросы, касающиеся информационной безопасности, рассматриваются в Законе РФ "Об участии в международном информационном обмене"?
24. Какова основная цель принятия Закона РФ "Об электронной цифровой подписи"?
25. Дайте определение электронной цифровой подписи согласно Закону РФ "Об электронной цифровой подписи".
26. Кто является владельцем сертификата ключа подписи (согласно Закону РФ "Об электронной цифровой подписи")?
27. Прокомментируйте понятие средств электронной цифровой подписи (согласно Закону РФ "Об электронной цифровой подписи")
28. Прокомментируйте понятие «сертификат средств электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
29. Прокомментируйте понятие «закрытый ключ электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
30. Прокомментируйте понятие «открытый ключ электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
31. Что такое сертификат ключа подписи и кто является его пользователем?
32. Какие сведения должен содержать сертификат ключа подписи?
33. Какие Вам известны американские законы, напрямую связанные с ИБ?
34. Охарактеризуйте специфику "Закона об информационной безопасности" (США).
35. Прокомментируйте американский законопроект "О совершенствовании информационной безопасности".
36. Что можно сказать о законодательстве ФРГ по вопросам ИБ?
37. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?
38. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне
39. Назовите главную цель мер административного уровня ИБ.
40. Что понимается под политикой безопасности?
41. Охарактеризуйте верхний уровень политики безопасности.
42. Приведите примерный список решений верхнего уровня политики безопасности.

43. Какие разделы политики безопасности рекомендованы Британским стандартом BS 7799:1995?
44. Охарактеризуйте средний уровень политики безопасности.
45. Какие аспекты ИБ характерны для среднего уровня политики безопасности?
46. Какие темы должна освещать политика безопасности среднего уровня для каждого аспекта ИБ?
47. Охарактеризуйте нижний уровень политики безопасности.
48. Что понимается под целями политики безопасности нижнего уровня?
49. Что такое программа безопасности?
50. Назовите главные цели программы безопасности верхнего уровня.
51. Кто отвечает за программу безопасности верхнего уровня?
52. Назовите главные цели программы безопасности нижнего уровня.
53. Кто отвечает за программу безопасности нижнего уровня?
54. Назовите этапы жизненного цикла информационного сервиса.
55. Прокомментируйте особенности этапов жизненного цикла информационного сервиса с точки зрения ИБ.
56. Что такое управление рисками?
57. Почему управление рисками рассматривается на административном уровне ИБ?
58. В чем заключается суть мероприятий по управлению рисками?
59. Какие возможны действия по отношению к выявленным рискам?
60. Назовите и охарактеризуйте этапы процесса управления рисками.
61. Как может осуществляться управление рисками на каждом из этапов *жизненного* цикла информационного сервиса?
62. Какие этапы управления рисками относятся к вспомогательным и почему?
63. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
64. Почему карта информационной системы способствует управлению рисками?
65. В чем суть методологии оценки рисков?
66. Что такое идентификация активов в процессе управления рисками?
67. Какие этапы управления рисками относятся к основным и почему?
68. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
69. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
70. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
71. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
72. Что такое оценка остаточного риска?
73. В чем заключается основная специфика процедурного уровня ИБ?
74. Перечислите основные классы мер процедурного уровня ИБ.
75. Охарактеризуйте управление персоналом, как важную меру процедурного уровня ИБ.
76. Прокомментируйте принцип разделения обязанностей в управлении персоналом, как меры процедурного уровня ИБ.
77. Прокомментируйте принцип минимизации привилегий в управлении персоналом, как меры процедурного уровня ИБ.
78. Охарактеризуйте физическую защиту ИС, принципиальную меру процедурного уровня ИБ.
79. Перечислите основные направления физической защиты.
80. Охарактеризуйте меры физического управления доступом.
81. Охарактеризуйте противопожарные меры физической защиты.
82. Что такое защита поддерживающей инфраструктуры и почему ей придается важность в ИБ?
83. В чем специфика защиты от перехвата данных?

84. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?
85. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
86. Охарактеризуйте процесс поддержки пользователей для обеспечения работоспособности ИС.
87. Охарактеризуйте процесс поддержки программного обеспечения для обеспечения работоспособности ИС.
88. Охарактеризуйте процесс конфигурационного управления для обеспечения работоспособности ИС.
89. Охарактеризуйте процесс резервного копирования для обеспечения работоспособности ИС.
90. Охарактеризуйте процесс управления носителями для обеспечения работоспособности ИС.
91. Охарактеризуйте процесс документирования для обеспечения работоспособности ИС.
92. Охарактеризуйте процесс регламентных работ для обеспечения работоспособности ИС.
93. Что такое реакция на нарушение режима безопасности?
94. Какие основные цели преследует реакция на нарушение режима безопасности?
95. В чем специфика планирования восстановительных работ на ИС?
96. Перечислите и прокомментируйте этапы планирования восстановительных работ.
Перечень вопросов для текущего контроля (письменный рейтинг №2):
 1. Перечислите основные причины важности программно-технического уровня ИБ.
 2. Назовите основные сервисы ИБ программно-технического уровня.
 3. Какие меры обеспечиваются сервисами безопасности
 4. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
 5. Перечислите принципы архитектурной безопасности ИС.
 6. Что такое идентификация?
 7. Дайте толкование понятия «аутентификация».
 8. Из-за каких причин затруднена надежная идентификация?
 9. Прокомментируйте парольную идентификацию.
 10. Какие меры позволяют повысить надежность парольной защиты?
 11. Назовите преимущества и недостатки одноразовых и многократных паролей.
 12. Прокомментируйте возможности биометрической идентификации (аутентификации).
 13. В чем заключается основная задача логического управления доступом?
 14. Что такое матрица доступа?
 15. Какая информация анализируется при принятии решения о предоставлении доступа?
 16. В чем суть ролевого управления доступом?
 17. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.
 18. В чем заключается основная задача аудита, как сервиса безопасности?
 19. Прокомментируйте основные цели, задачи и средства (компоненты) активного аудита.
 20. Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.
 21. Прокомментируйте возможности симметричного шифрования.
 22. Прокомментируйте возможности асимметричного шифрования.
 23. Приведите основные понятия криптографического контроля целостности.
 24. Что такое хэш-функция?
 25. Прокомментируйте понятия «удостоверяющий центр» и «цифровой сертификат».
 26. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС.
 27. Что такое firewall и как он функционирует?
 28. Для каких целей служит сервис анализа защищенности?
 29. Прокомментируйте понятие отказоустойчивости применительно к ИС.

30. Охарактеризуйте понятия «зона риска» и «зона нейтрализации».
 31. Перечислите основные меры обеспечения отказоустойчивости ИС.
 32. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
 33. В чем заключается специфика управления, как сервиса безопасности?
 34. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
 35. Сформулируйте основные концептуальные положения теории ЗИ.
 36. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
 37. Сформулируйте определение задачи защиты и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.
 38. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
 39. Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
 40. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?
 41. Раскройте кратко общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
 42. Как влияют показатели защищаемой информации на структуру и подходы к проектированию системы ЗИ?
 43. Прокомментируйте основные принципы обеспечения ИБ предприятия
 44. Какие должны быть условия успешности решения проблем ИБ?
 45. Сформулируйте общие требования к системе ИБ объекта
 46. Перечислите рекомендации создателям систем ИБ.
 47. Приведите принятую методику построения системы ИБ предприятия
- Перечень вопросов для текущего контроля (письменный рейтинг №3):*
1. Что включает в себя понятие «модель (облик) нарушителя»?
 2. Приведите возможную классификацию нарушителей.
 3. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
 4. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
 5. Что такое «таблица соответствия» анализа угроз со стороны каждой категории потенциальных злоумышленников?
 6. Приведите алгоритм учета факторов, определяющих облик нарушителя и позволяющий получить матрицу нарушений ИБ
 7. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
 8. Зачем необходим сценарий нарушения ИБ?
 9. Охарактеризуйте прямые и косвенные потери предприятия в результате информационного воздействия
 10. Перечислите 6 этапов анализа риска
 11. Приведите возможный вариант табличного представления результатов анализа риска
 12. Что понимают под управлением рисками? Охарактеризуйте общий подход.
 13. Каким образом уровень зрелости предприятия влияет на выбор подхода к оценке рисков в организации?

14. Охарактеризуйте процессный подход к оценке и управлению рисками по стандарту BS 7799
15. Приведите 7 факторов риска
16. Что такое «фазы оценки рисков»?
17. Охарактеризуйте основные методы оценки и управления рисками, реализованные в виде программного обеспечения.
18. Определите основную цель управления ИБ предприятия
19. Определите комплекс мероприятий по управлению ИБ предприятия
20. Приведите обобщенную схему процесса управления ИБ предприятия
21. Охарактеризуйте этапы логической последовательности принятия решения процесса управления ИБ
22. Охарактеризуйте информационно-расчетное обеспечение управления ИБ
23. Что понимают под системой управления ИБ?
24. Охарактеризуйте основные подсистемы СУИБ.
25. Назовите основные задачи службы ИБ
26. Определите основные подразделения службы ИБ.
27. Определите организационно-правовой статус СИБ
28. Охарактеризуйте основные направления деятельности администратора безопасности
29. Какие действия должен выполнять администратор безопасности в случае возникновения нарушения в компьютерной системе?

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Методология информационной безопасности» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

В ходе выполнения цикла лабораторных работ студенты знакомятся с актуальной, действующей на текущий момент нормативной базой в области информационной безопасности; рассматривают основные направления развития законодательства; обсуждают проблемы правоприменения действующих норм

Критерии оценки выполнения лабораторных работ (1, 2 семестр)

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 3 балла.

Критерии оценки для выполнения лабораторной работы:

- 2,5-3 балла выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствии с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 1,5-2,4 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствии с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на

контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 0,9-1,4 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствии с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,1-0,8 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствии с требованием преподавателя) не представлен или представлен неполный, отчет содержит описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 1,5 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методология информационной безопасности» (лабораторные работы)

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (1 семестр):

Лабораторная работа 1. Сбор исходных данных для аудита информационной безопасности объекта

1. Что такое аудит информационной безопасности объекта?
2. Что может выступать в качестве объекта аудита информационной безопасности объекта?
3. Где берутся данные для аудита информационной безопасности объекта?
4. Приведите перечень исходных данных, необходимых для аудита безопасности.
5. Назовите виды аудита безопасности.

Лабораторная работа 2. Выявление уязвимостей информационной системы

1. Что такое уязвимости информационной системы.
2. Что может выступать в качестве уязвимостей информационной системы.

3. Как можно выявить уязвимости информационной системы.
4. Приведите классификацию основных уязвимостей.
5. Назовите причины возникновения уязвимостей.

Лабораторная работа 3. Идентификация защитных механизмов

1. Что такое идентификация.
2. Что такое защитный механизм.
3. Приведите примеры защитных механизмов.
4. Назовите основные защитные механизмы, используемые в системах защиты информации.
5. Как происходит идентификация защитных механизмов.

Лабораторная работа 4. Идентификация нарушителей

1. Что такое идентификация.
2. Кто такие нарушители.
3. Приведите примеры нарушителей.
4. Как можно идентифицировать нарушителей?
5. Перечислите виды нарушителей.

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (2 семестр):

Лабораторная работа №1. Изучение показателей качества систем защиты информации предприятия

1. Что такое система защиты информации предприятия?
2. Что такое показатель качества систем защиты информации предприятия?
3. Приведите примеры систем защиты информации предприятия.
4. Приведите примеры показателей качества систем защиты информации предприятия.
5. Приведите классификацию показателей качества систем защиты информации предприятия.

Лабораторная работа №2. Проведение экспертизы защищенности ИС предприятия.

1. Что такое ИС предприятия?
2. Что подразумевается под защищённостью ИС предприятия?
3. Что такое экспертиза защищенности ИС предприятия?
4. Как проводится экспертиза защищенности ИС предприятия?

Лабораторная работа №3. Оценка качества СЗИ предприятия

1. Что такое СЗИ предприятия?
2. Что подразумевается под качеством СЗИ предприятия?
3. Какие существуют методы оценки качества СЗИ предприятия?
4. Что должна обеспечивать СЗИ предприятия?

Лабораторная работа №4. Расчет показателей качества системы защиты информации на примере коммерческого предприятия

1. Что такое коммерческое предприятие?
2. Что такое система защиты информации?
3. Какие бывают показатели качества системы защиты информации?
4. Как рассчитываются показатели качества системы защиты информации?

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Методология информационной безопасности» предполагается выполнение заданий СРС, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения самостоятельной работы (1, 2 семестр)

Результаты выполнения самостоятельной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение работы по каждой теме, составляет 1,5 балла.

Критерии оценки для выполнения работы:

- 1,2-1,5 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теме; полностью, самостоятельно и в определенный преподавателем срок выполнено задание;

- 0,8-1,1 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теме; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока;

- 0,5-0,7 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с отражением лишь общего направления изложения материала; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока, содержит незначительные ошибки;

- 0,1-0,4 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику темы; задание выполнено не полностью, не самостоятельно, с существенным нарушением определенного преподавателем срока, при выполнении задания продемонстрировал отсутствие необходимых умений и практических навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методология информационной безопасности» (самостоятельная работа)

1 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Введение. Характеристика защищаемой информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
2	Значение ИБ и ее место в системе национальной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
3	Основные понятия и определения в области информационной безопасности и защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
4	Категории защищаемой информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
5	Концептуальная модель системы информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
6	Действия, приводящие к незаконному овладению конфиденциальной информацией	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
7	Угрозы конфиденциальной информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
8	Способы защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
9	Уровни информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5

		Итого за семестр:	13,5
--	--	-------------------	------

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (1 семестр):

Раздел 1

1. Какие признаки объектов являются демаскирующими?
2. Приведите классификацию демаскирующих признаков объектов защиты.
3. Опишите опознавательные демаскирующие признаки объектов защиты.
4. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
5. Что такое информативность демаскирующего признака?
6. Что такое тезаурус?
7. Перечислите основные носители признаковой информации.
8. Перечислите основные источники конфиденциальной информации.
9. В чем отличие прямых источников семантической информации от косвенных?
10. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации

Раздел 2

1. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
2. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
3. В чем специфика деятельности Федеральной службы безопасности?
4. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
5. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
6. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
7. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
8. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
9. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
10. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
11. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Раздел 3

1. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
2. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
3. Дайте определение информационной безопасности, прокомментируйте его составляющие.
4. Что такое защита информации?
5. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.

Раздел 4

1. Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
2. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
3. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
4. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
5. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.

6. Какая информация не может быть отнесена к коммерческой тайне?
7. Перечислите основные объекты банковской тайны.
8. Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
9. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
10. Перечислите основные объекты интеллектуальной собственности.

Раздел 5

1. Что такое объекты угроз ИБ и в чем они выражаются?
2. Каковы основные источники угроз защищаемой информации?
3. Каковы цели угроз информации со стороны злоумышленников?
4. Перечислите основные источники конфиденциальной информации.
5. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
6. Перечислите базовые способы защиты информации.
7. Изобразите графически схему концептуальной модели системы ИБ.

Раздел 6

1. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
2. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
3. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
4. Как осуществляется утечка конфиденциальной информации?

Раздел 7

1. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
2. Что такое наблюдение в теории информационной безопасности?
3. Что такое подслушивание в теории информационной безопасности?
4. Что такое перехват в теории информационной безопасности?
5. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
6. Какие организации формируют структуру разведывательного сообщества США?
7. Охарактеризуйте *непреднамеренные ошибки в качестве угрозы доступности*.
8. Охарактеризуйте программные *атаки* на доступность.
9. Приведите примеры «бомбы», «червя», «вируса».
10. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
11. Что в ИБ понимают под маскарадом?

Раздел 8

1. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
2. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
3. Назовите три группы мероприятий по технической защите информации.
4. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
5. Прокомментируйте основные организационно-технические мероприятия поЗИ.
6. Прокомментируйте основные технические мероприятия по технической защите информации.
7. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
8. В чем заключается специфика управления, как сервиса безопасности?

2 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Законодательный уровень информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
2	Административный уровень информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
3	Процедурный уровень информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
4	Программно-технический уровень информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
5	Сервисы безопасности программно-технического уровня	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
6	Сущность комплексной системы защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
7	Формирование облика нарушителя	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
8	Алгоритм проведения анализа информационного риска на предприятии	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
9	Управление информационной безопасностью	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1,5
			Итого за семестр:	13,5

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (2 семестр):

Разделы 9. 10

1. Какова основная цель принятия Закона РФ "Об электронной цифровой подписи"?
2. Дайте определение электронной цифровой подписи согласно Закону РФ "Об электронной цифровой подписи".
3. Кто является владельцем сертификата ключа подписи (согласно Закону РФ "Об электронной цифровой подписи")?
4. Прокомментируйте понятие средств электронной цифровой подписи (согласно Закону РФ "Об электронной цифровой подписи")
5. Прокомментируйте понятие «сертификат средств электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
6. Прокомментируйте понятие «закрытый ключ электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
7. Прокомментируйте понятие «открытый ключ электронной цифровой подписи» (согласно Закону РФ "Об электронной цифровой подписи")
8. Что такое сертификат ключа подписи и кто является его пользователем?
9. Какие сведения должен содержать сертификат ключа подписи?
10. Какие Вам известны американские законы, напрямую связанные с ИБ?
11. Охарактеризуйте специфику "Закона об информационной безопасности" (США).
12. Прокомментируйте американский законопроект "О совершенствовании информационной безопасности".
13. Что можно сказать о законодательстве ФРГ по вопросам ИБ?
14. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?

Раздел 11

1. В чем заключается суть мероприятий по управлению рисками?
2. Какие возможны действия по отношению к выявленным рискам?
3. Назовите и охарактеризуйте этапы процесса управления рисками. Как может осуществляться управление рисками на каждом из этапов жизненного цикла информационного сервиса?
4. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
5. Почему карта информационной системы способствует управлению рисками?
6. В чем суть методологии оценки рисков?
7. Что такое идентификация активов в процессе управления рисками?
8. Какие этапы управления рисками относятся к основным и почему?
9. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
10. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
11. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
12. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
13. Что такое оценка остаточного риска?

Раздел 12

1. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
2. Охарактеризуйте процесс поддержки пользователей для обеспечения работоспособности ИС.
3. Охарактеризуйте процесс поддержки программного обеспечения для обеспечения работоспособности ИС.
4. Охарактеризуйте процесс конфигурационного управления для обеспечения работоспособности ИС.
5. Охарактеризуйте процесс резервного копирования для обеспечения работоспособности ИС.
6. Охарактеризуйте процесс управления носителями для обеспечения работоспособности ИС.
7. Охарактеризуйте процесс документирования для обеспечения работоспособности ИС.
8. Охарактеризуйте процесс регламентных работ для обеспечения работоспособности ИС.
9. Какие основные цели преследует реакция на нарушение режима безопасности?
10. Перечислите и прокомментируйте этапы планирования восстановительных работ.

Раздел 13

1. Какие меры обеспечиваются сервисами безопасности
2. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
3. Перечислите принципы архитектурной безопасности ИС.

Раздел 14

1. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.
2. В чем заключается основная задача аудита, как сервиса безопасности?
3. Прокомментируйте основные цели, задачи и средства (компоненты) активного аудита.
4. Прокомментируйте понятия «удостоверяющий центр» и «цифровой сертификат».
5. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС.
6. Что такое firewall и как он функционирует?
7. Для каких целей служит сервис анализа защищенности?
8. Прокомментируйте понятие отказоустойчивости применительно к ИС.
9. Охарактеризуйте понятия «зона риска» и «зона нейтрализации».
10. Перечислите основные меры обеспечения отказоустойчивости ИС.
11. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
12. В чем заключается специфика управления, как сервиса безопасности?

Раздел 15

1. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы?
2. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
3. Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
4. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?
5. Раскройте кратко общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
6. Как влияют показатели защищаемой информации на структуру и подходы к проектированию системы ЗИ?
7. Прокомментируйте основные принципы обеспечения ИБ предприятия
8. Какие должны быть условия успешности решения проблем ИБ?
9. Сформулируйте общие требования к системе ИБ объекта

Раздел 16

1. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
2. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
3. Что такое «таблица соответствия» анализа угроз со стороны каждой категории потенциальных злоумышленников?
4. Приведите алгоритм учета факторов, определяющих облик нарушителя и позволяющий получить матрицу нарушений ИБ
5. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
6. Зачем необходим сценарий нарушения ИБ?

Раздел 17

1. Каким образом уровень зрелости предприятия влияет на выбор подхода к оценке рисков в организации?
2. Охарактеризуйте процессный подход к оценке и управлению рисками по стандарту BS 7799
3. Приведите факторы риска
4. Что такое «фазы оценки рисков»?
5. Охарактеризуйте основные методы оценки и управления рисками, реализованные в виде программного обеспечения.

Раздел 18

1. Охарактеризуйте этапы логической последовательности принятия решения процесса управления ИБ
2. Охарактеризуйте информационно-расчетное обеспечение управления ИБ
3. Что понимают под системой управления ИБ?
4. Охарактеризуйте основные подсистемы СУИБ.
5. Назовите основные задачи службы ИБ
6. Определите основные подразделения службы ИБ.
7. Определите организационно-правовой статус СИБ
8. Охарактеризуйте основные направления деятельности администратора безопасности
9. Какие действия должен выполнять администратор безопасности в случае возникновения нарушения в компьютерной системе?

Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствии с Положением)

1 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	2,5
5	Дополнительные баллы (бонусы)	2
6	Лабораторные работы	12
7	Выполнение семестрового плана самостоятельной работы	13,5
8	Экзамен	40
9	Всего	100

2 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	2,5
5	Дополнительные баллы (бонусы)	2
6	Лабораторные работы	12
7	Выполнение семестрового плана самостоятельной работы	13,5
8	Экзамен	40
9	Всего	100

4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Методология информационной безопасности»

Регламент проведения промежуточного контроля (экзамена)

Промежуточная аттестация по итогам освоения дисциплины (экзамен) проводится в экзаменационную сессию. Экзамен проводится по билетам, содержащим три вопроса. Студент пишет ответы на вопросы экзаменационного билета на листах белой бумаги формата А4, на каждом из которых должны быть указаны: фамилия, имя отчество студента; шифр студенческой группы; дата проведения экзамена; номер экзаменационного билета. Листы должны быть подписаны и студентом и экзаменатором после получения студентом экзаменационного билета. Экзаменационные билеты должны быть оформлены в соответствии с утвержденным регламентом.

После подготовки студент устно отвечает на вопросы билета и уточняющие вопросы экзаменатора. Экзаменатор вправе задать студенту дополнительные вопросы и задания по материалам дисциплины для выявления степени усвоения студентом компетенций.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствии с Положением составляет 40 баллов.

Критерии оценивания компетенций на экзамене (1,2 семестр)

Оценка в баллах	Оценка за ответ на экзамене	Критерии оценивания компетенций
30 - 40	«Отлично»	Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует при ответе материалы из основной и дополнительной литературы по дисциплине, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных рабочей программой дисциплины.
20 - 29	«Хорошо»	Студент показывает твердое знание материала, грамотно и по существу излагает его, не допускает существенных неточностей при ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.
10 - 19	«Удовлетворительно»	Студент показывает знания только основного материала, но не усвоил его деталей; допускает неточности, недостаточно правильные формулировки, которые в целом не препятствуют усвоению последующего программного материала; допускает нарушения логической последовательности в изложении программного материала; испытывает затруднения при выполнении практических работ; подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины, на минимально допустимом уровне.
0 - 10	«Неудовлетворительно»	Студент не знает значительной части программного материала, имеет менее 50% правильно выполненных заданий от общего объема работы, допускает существенные ошибки при изложении материала, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.

Оценочные средства для промежуточной аттестации по учебной дисциплине «Методология информационной безопасности» (экзамен)

Перечень вопросов для промежуточного контроля (экзамена)

1 семестр:

1. Приведите классификацию демаскирующих признаков объектов защиты.
2. Опишите опознавательные демаскирующие признаки объектов защиты.
3. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
4. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
5. Перечислите основные носители признаков информации.
6. Что такое «источник конфиденциальной информации»?
7. Перечислите основные источники конфиденциальной информации.
8. В чем отличие прямых источников семантической информации от косвенных?
9. Перечислите основные категории информационной безопасности и дайте им определения.
10. Охарактеризуйте понятие доступности, целостности, конфиденциальности.
11. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
12. В чем заключаются и чем обеспечиваются национальные интересы России в информационной сфере?
13. Что такое государственная информационная политика?
14. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
15. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
16. Классифицируйте угрозы ИБ РФ по общей направленности.
17. В чем состоят угрозы ИБ для личности?
18. В чем состоят угрозы ИБ для общества?
19. В чем состоят угрозы ИБ для государства?
20. Перечислите основные принципы ИБ России согласно Доктрине.
21. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
22. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
23. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
24. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
25. Охарактеризуйте основные признаки защищаемой информации.
26. Перечислите и охарактеризуйте основных собственников защищаемой информации.
27. Что такое государственная тайна?
28. Перечислите сведения, которые могут быть отнесены к государственной тайне.
29. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
30. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
31. Перечислите основные объекты банковской тайны.
32. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
33. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).

34. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
35. Перечислите основные объекты интеллектуальной собственности.
36. Перечислите основные компоненты концептуальной модели ИБ.
37. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
38. Перечислите базовые способы защиты информации.
39. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
40. Что такое утечка конфиденциальной информации?
41. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
42. Как осуществляется утечка конфиденциальной информации?
43. Дайте определение угрозы конфиденциальной информации.
44. Какие угрозы называются преднамеренными, а какие случайными?
45. Что такое канал несанкционированного доступа?
46. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
47. Что такое наблюдение в теории информационной безопасности?
48. Что такое подслушивание в теории информационной безопасности?
49. Что такое перехват в теории информационной безопасности?
50. Что такое технический канал утечки информации?
51. Охарактеризуйте случайный и организованный канал утечки информации.
52. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
53. Прокомментируйте наиболее распространенные угрозы доступности.
54. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
55. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
56. Охарактеризуйте программные атаки на доступность.
57. Что такое вредоносное программное обеспечение?
58. Дайте определение способа защиты информации.
59. Охарактеризуйте способ предупреждения возможных угроз.
60. Прокомментируйте основные действия способа выявления угроз
61. Охарактеризуйте способ обнаружения угроз.
62. Охарактеризуйте способ пресечения или локализации угроз.
63. Прокомментируйте основные действия способа ликвидации последствий.
64. Перечислите основные защитные действия при реализации способов ЗИ,
65. Что такое защита от разглашения?
66. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
67. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
68. Назовите три группы мероприятий по технической защите информации.
69. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
70. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
71. Прокомментируйте основные технические мероприятия по технической защите информации.

Перечень вопросов для промежуточного контроля (экзамена)

2 семестр:

1. Какие вопросы, касающиеся ИБ, содержатся в Конституции РФ?

2. Какие вопросы, касающиеся ИБ, содержатся в Гражданском кодексе РФ?
3. Какие статьи Уголовного кодекса напрямую касаются ИБ?
4. Какие основные понятия рассматриваются в Закон РФ "Об информации, информатизации и защите информации"?
5. Что такое лицензия и лицензируемый вид деятельности (согласно Закону РФ "О лицензировании отдельных видов деятельности")?
6. Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии (согласно Закону РФ "О лицензировании отдельных видов деятельности").
7. Кто является основными лицензирующими органами в области защиты информации?
8. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?
9. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне
10. Назовите главную цель мер административного уровня ИБ.
11. Что понимается под политикой безопасности?
12. Охарактеризуйте верхний уровень политики безопасности.
13. Приведите примерный список решений верхнего уровня политики безопасности.
14. Какие аспекты ИБ характерны для среднего уровня политики безопасности?
15. Какие темы должна освещать политика безопасности среднего уровня для каждого аспекта ИБ?
16. Охарактеризуйте нижний уровень политики безопасности.
17. Что понимается под целями политики безопасности нижнего уровня?
18. Что такое программа безопасности?
19. Назовите главные цели программы безопасности верхнего уровня.
20. Кто отвечает за программу безопасности верхнего уровня?
21. Назовите главные цели программы безопасности нижнего уровня.
22. Кто отвечает за программу безопасности нижнего уровня?
23. В чем заключается основная специфика процедурного уровня ИБ?
24. Перечислите основные классы мер процедурного уровня ИБ.
25. Охарактеризуйте управление персоналом, как важную меру процедурного уровня ИБ.
26. Прокомментируйте принцип разделения обязанностей в управлении персоналом, как меры процедурного уровня ИБ.
27. Прокомментируйте принцип минимизации привилегий в управлении персоналом, как меры процедурного уровня ИБ.
28. Перечислите основные направления физической защиты.
29. Охарактеризуйте меры физического управления доступом.
30. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
31. Какие основные цели преследует реакция на нарушение режима безопасности?
32. В чем специфика планирования восстановительных работ на ИС?
33. Перечислите и прокомментируйте этапы планирования восстановительных работ.
34. Перечислите основные причины важности программно-технического уровня ИБ.
35. Назовите основные сервисы ИБ программно-технического уровня.
36. Какие меры обеспечиваются сервисами безопасности
37. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
38. Перечислите принципы архитектурной безопасности ИС.
39. Что такое идентификация?
40. Дайте толкование понятия «аутентификация».
41. Прокомментируйте парольную идентификацию.
42. Какие меры позволяют повысить надежность парольной защиты?
43. Назовите преимущества и недостатки одноразовых и многократных паролей.

44. Прокомментируйте возможности биометрической идентификации (аутентификации).
45. В чем заключается основная задача логического управления доступом?
46. Что такое матрица доступа?
47. Какая информация анализируется при принятии решения о предоставлении доступа?
48. В чем суть ролевого управления доступом?
49. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.
50. В чем заключается основная задача аудита, как сервиса безопасности?
51. Прокомментируйте основные цели, задачи и средства (компоненты) активного аудита.
52. Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.
53. Приведите основные понятия криптографического контроля целостности.
54. Что такое хэш-функция?
55. Прокомментируйте понятия «удостоверяющий центр» и «цифровой сертификат».
56. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС.
57. Что такое firewall и как он функционирует?
58. Для каких целей служит сервис анализа защищенности?
59. Прокомментируйте понятие отказоустойчивости применительно к ИС.
60. В чем заключается специфика управления, как сервиса безопасности?
61. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
62. Сформулируйте основные концептуальные положения теории ЗИ.
63. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
64. Сформулируйте определение задачи защиты и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.
65. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
66. Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
67. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?
68. Раскройте кратко общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
69. Как влияют показатели защищаемой информации на структуру и подходы к проектированию системы ЗИ?
70. Прокомментируйте основные принципы обеспечения ИБ предприятия
71. Сформулируйте общие требования к системе ИБ объекта
72. Перечислите рекомендации создателям систем ИБ.
73. Приведите принятую методику построения системы ИБ предприятия
74. Что включает в себя понятие «модель (облик) нарушителя»?
75. Приведите возможную классификацию нарушителей.
76. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
77. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ

78. Приведите алгоритм учета факторов, определяющих облик нарушителя и позволяющий получить матрицу нарушений ИБ
79. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
80. Перечислите 6 этапов анализа риска
81. Приведите возможный вариант табличного представления результатов анализа риска
82. Что такое «фазы оценки рисков»?
83. Охарактеризуйте основные методы оценки и управления рисками, реализованные в виде программного обеспечения.
84. Определите основную цель управления ИБ предприятия
85. Определите комплекс мероприятий по управлению ИБ предприятия
86. Приведите обобщенную схему процесса управления ИБ предприятия
87. Охарактеризуйте этапы логической последовательности принятия решения процесса управления ИБ
88. Назовите основные задачи службы ИБ
89. Определите основные подразделения службы ИБ.
90. Определите организационно-правовой статус СИБ
91. Охарактеризуйте основные направления деятельности администратора безопасности
92. Какие действия должен выполнять администратор безопасности в случае возникновения нарушения в компьютерной системе?